
GOVERNMENT COMMUNICATIONS SECURITY BUREAU

TE TIRA TIAKI

# NZISM

## New Zealand Information Security Manual

## February 2020 – Part 2

Chapters 14 - 23

www.gcsb.govt.nz

New Zealand Government

# Table of Contents

# 14. Software security

## 14.1. Standard Operating Environments

### Objective

14.1.1. Standard Operating Environments (SOE) are hardened in order to minimise attacks and compromise through known vulnerabilities and attack vectors.

### Context

#### Scope

14.1.2. This section covers information on the hardening of software used on workstations and servers on systems within agency control.

#### Characterisation

14.1.3. Characterisation is a technique used to analyse and record a system's configuration. It is important as it can be used as a baseline to verify the system's integrity at a later date. It is also important that the baseline has high levels of integrity and assurance to avoid reinfecting systems or reintroducing compromises when restoring from baselines.

14.1.4. In virtual environments a baseline is usually a "snapshot" or image take at a point in time. If the image or snapshot is infected, then restoring from that image can result in further compromise. See also Section 22.2 – Virtualisation and 22.3 – Virtual Local Area Networks.

14.1.5. Methods of characterising files and directories include:

- performing a cryptographic checksum on the files/directories when they are known to be virus/contaminant free;
- documenting the name, type, size and attributes of legitimate files and directories, along with any changes to this information expected under normal operating conditions; or
- for a Windows system, taking a system difference snapshot.

## References

14.1.6. Further references can be found at:

| Title | Publisher | Source |
|---|---|---|
| **ISO/IEC 27001:2013, A.12.4.1**<br>**Control of Operational Software** | ISO / IEC<br>Standards NZ | http://www.iso27001security.com/html/27001.html<br>http://www.standards.co.nz |
| **ISO/IEC 27001:2013, A.12.6.1**<br>**Control of Technical Vulnerabilities** | ISO / IEC<br>Standards NZ | http://www.iso27001security.com/html/27001.html<br>http://www.standards.co.nz |
| **Independent testing of different antivirus software and their effectiveness** | AV Comparatives | http://www.av-comparatives.org/ |

## PSR references

14.1.7. Relevant PSR requirements can be found at:

| Reference | Title | Source |
|---|---|---|
| **PSR Mandatory Requirements** | GOV3, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2 | http://www.protectivesecurity.govt.nz |
| **PSR content protocols** | Management protocol for information security<br>Management protocol for physical security | http://www.protectivesecurity.govt.nz |
| **PSR requirements sections** | Handling requirements for protectively marked information and equipment<br>Analyse evolving threats and vulnerabilities | http://www.protectivesecurity.govt.nz |
| **Managing specific scenarios** | Transacting online with the public | http://www.protectivesecurity.govt.nz |

## Rationale & Controls

### 14.1.8. Developing hardened SOEs

**14.1.8.R.01. Rationale**

Antivirus and anti-malware software, while an important defensive measure, can be defeated by malicious code that has yet to be identified by antivirus vendors. This can include targeted attacks, where a new virus is engineered or an existing one modified to defeat the signature-based detection schemes.

**14.1.8.R.02. Rationale**

The use of antivirus and anti-malware software, while adding value to the defence of workstations, cannot be relied solely upon to protect the workstation. As such agencies still need to deploy appropriately hardened SOEs to assist with the protection of workstations against a broader range of security risks.

**14.1.8.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD develop a hardened SOE for workstations and servers, covering:

- removal of unneeded software and operating system components;
- removal or disabling of unneeded services, ports and BIOS settings;
- disabling of unused or undesired functionality in software and operating systems;
- implementation of access controls on relevant objects to limit system users and programs to the minimum access required;
- installation of antivirus and anti-malware software;
- installation of software-based firewalls limiting inbound and outbound network connections;
- configuration of either remote logging or the transfer of local event logs to a central server; and
- protection of audit and other logs through the use of a one way pipe to reduce likelihood of compromise key transaction records.

### 14.1.9. Maintaining hardened SOEs

**14.1.9.R.01. Rationale**

Whilst a SOE can be sufficiently hardened when it is deployed, its security will progressively degrade over time. Agencies can address the degradation of the security of a SOE by ensuring that patches are continually applied, system users are not able to disable or bypass security functionality and antivirus and other security software is appropriately maintained with the latest signatures and updates.

**14.1.9.R.02. Rationale**

End Point Agents monitor traffic and apply security policies on applications, storage interfaces and data in real-time. Administrators actively block or monitor and log policy breaches. The End Point Agent can also create forensic monitoring to facilitate incident investigation.

**14.1.9.R.03. Rationale**

End Point Agents can monitor user activity, such as the cut, copy, paste, print, print screen operations and copying data to external drives and other devices. The Agent can then apply policies to limit such activity.

**14.1.9.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that for all servers and workstations:

- a technical specification is agreed for each platform with specified controls;
- a standard configuration created and updated for each operating system type and version;
- system users do not have the ability to install or disable software without approval; and
- installed software and operating system patching is up to date.

**14.1.9.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that for all servers and workstations:

- malware detection heuristics are set to a high level;
- malware pattern signatures are checked for updates on at least a daily basis;
- malware pattern signatures are updated as soon as possible after vendors make them available;
- all disks and systems are regularly scanned for malicious code; and
- the use of End Point Agents is considered.

### 14.1.10. Default passwords and accounts

**14.1.10.R.01. Rationale**

Default passwords and accounts for operating systems are often exploited by attackers as they are well documented in product manuals and can be easily checked in an automated manner with little effort required.

**14.1.10.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST reduce potential vulnerabilities in their SOEs by:

- removing unused accounts;
- renaming or deleting default accounts; and
- replacing default passwords before or during the installation process.

**14.1.10.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD reduce potential vulnerabilities in their SOEs by:

- removing unused accounts;
- renaming or deleting default accounts; and
- replacing default passwords, before or during the installation process.

### 14.1.11. Server separation

**14.1.11.R.01. Rationale**

Servers with a high security risk can include Web, email, file, Internet Protocol Telephony (IPT) servers, Mobile Device Manager (MDM) servers and gateway components. It is important to clearly identify all services and connections to design a complete and secure server separation architecture. Refer also to Chapter 19 – Gateway Security.

**14.1.11.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Where servers with a high security risk have connectivity to unsecure public networks, agencies SHOULD:

- use appropriately designed and configured gateways;
- consider the use of cross-domain solutions;
- segment networks;
- maintain effective functional segregation between servers allowing them to operate independently;
- minimise communications between servers at both the network and file system level as appropriate; and
- limit system users and programs to the minimum access needed to perform their duties.

### 14.1.12. Characterisation

#### 14.1.12.R.01. Rationale

There are known techniques for defeating basic characterisations, therefore other methods of intrusion detection are also needed, particularly in situations where it is impractical to use a trusted environment for the generation of the characterisation data. Characterisation is very useful in post-intrusion forensic investigations where an infected disk can be compared to stored characterisation data in order to determine what files have been changed or introduced.

#### 14.1.12.R.02. Rationale

Characterisation is also directly related to business continuity and disaster recovery and is influenced by Business Impact Analyses and Risk Assessments. Grouping elements by business applications and setting priority and criticality of the elements to the business may assist in determining the most appropriate and useful characterisations.

#### 14.1.12.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD:

- characterise all servers whose functions are critical to the agency, and those identified as being at a high security risk of compromise;
- store the characterisation information securely off the server in a manner that maintains integrity;
- update the characterisation information after every legitimate change to a system as part of the change control process;
- as part of the agency's ongoing audit schedule, compare the stored characterisation information against current characterisation information to determine whether a compromise, or a legitimate but incorrectly completed system modification, has occurred;
- perform the characterisation from a trusted environment rather than the standard operating system wherever possible; and
- resolve any detected changes in accordance with the agency's information security incident management procedures.

#### 14.1.12.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use an Approved Cryptographic Algorithm to perform cryptographic checksums for characterisation purposes.

#### 14.1.12.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider characterisations in the context of a BCP or DRP and any related Business Impact Analyses and Risk Assessments.

### 14.1.13. Automated outbound connections by software

**14.1.13.R.01. Rationale**

Applications that include beaconing functionality include those that initiate a connection to the vendor site over the Internet and inbound remote management.

**14.1.13.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD review all software applications to determine whether they attempt to establish any unauthorised or unplanned external connections.

**14.1.13.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

If automated outbound connection functionality is included, agencies SHOULD make a business decision to determine whether to permit or deny these connections, including an assessment of the security risks involved in doing so.

**14.1.13.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

If automated outbound connection functionality is included, agencies SHOULD consider the implementation of Data Loss Prevention (DLP) technologies.

### 14.1.14. Knowledge of software used on systems

**14.1.14.R.01. Rationale**

Information about installed software, that could be disclosed outside the agency, can include:

- user agent on Web requests disclosing the Web browser type;
- network and email client information in email headers; and
- email server software headers.

This information could provide a malicious entity with knowledge of how to tailor attacks to exploit vulnerabilities in the agency's systems.

**14.1.14.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD limit information that could be disclosed outside the agency about what software, and software versions are installed on their systems.

# 14.2. Application Whitelisting

## Objective

14.2.1. Only approved applications are used on agency controlled systems.

## Context

### Scope

14.2.2. This section covers information on the use of technical controls to restrict the specific applications that can be accessed by a user or group of users.

## References

14.2.3. Further information on application whitelisting as implemented by Microsoft can be found at:

| Title | Publisher | Source |
|---|---|---|
| **Using Software Restriction Policies to Protect Against Unauthorized Software** | Microsoft | http://technet.microsoft.com/en-us/library/bb457006.aspx |
| **APPLOCKER** | Microsoft | https://docs.microsoft.com/en-nz/windows/security/threat-protection/applocker/applocker-overview |
| **Implementing Application Whitelisting January2018** | ASD | http://www.asd.gov.au/publications/protect/Application_Whitelisting.pdf |
| **NIST Special Publication 800-167 - Guide to Application Whitelisting** | NIST | http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf |
| **Application Whitelisting Using Microsoft AppLocker** | NSA | https://www.iad.gov/iad/library/ia-guidance/tech-briefs/application-whitelisting-using-microsoft-applocker.cfm |
| **Application Whitelisting Explained** | CSE | https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsb95-eng_0.pdf |
| **Guidelines for Application Whitelisting in Industrial Control Systems** | DHS - The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) | https://ics-cert.us-cert.gov/sites/default/files/documents/Guidelines%20for%20Application%20Whitelisting%20in%20Industrial%20Control%20Systems_S508C.pdf |

## Rationale & Controls

### 14.2.4. Application whitelisting

**14.2.4.R.01. Rationale**

Application whitelisting can be an effective mechanism to prevent the successful compromise of an agency system resulting from the exploitation of a vulnerability in an application or the execution of malicious code.

**14.2.4.R.02. Rationale**

Defining a list of trusted executables, a whitelist, is a practical and secure method of securing a system rather than relying on a list of bad executables (black list) to be prevented from running.

**14.2.4.R.03. Rationale**

Application whitelisting is considered only one part of a defence-in-depth strategy in order to prevent a successful attack, or to help mitigate consequences arising from an attack.

**14.2.4.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD implement application whitelisting as part of the SOE for workstations, servers and any other network device.

### 14.2.5. System user permissions

**14.2.5.R.01. Rationale**

An average system user requires access to only a few applications, or groups of applications, in order to conduct their work. Restricting the system user's permissions to execute code to this limited set of applications reduces the attack surface of the system.

**14.2.5.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that a system user cannot disable the application whitelisting mechanism.

**14.2.5.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD prevent a system user from running arbitrary executables.

**14.2.5.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD restrict a system user's rights in order to permit them to only execute a specific set of predefined executables as required for them to complete their duties.

**14.2.5.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that application whitelisting does not replace the antivirus and anti-malware software within a system.

### 14.2.6. System administrator permissions

**14.2.6.R.01. Rationale**

Since the consequences of running malicious code as a privileged user are much more severe than an unprivileged user, an application whitelisting implementation should be strictly enforced for system administrators.

**14.2.6.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that system administrators are not automatically exempt from application whitelisting policy.

### 14.2.7. Application whitelisting configuration

**14.2.7.R.01. Rationale**

A decision to execute a routine, application, or other programme should be made based on a validated cryptographic hash as it is more secure than a decision based on the executable's signature, path or parent folder.

**14.2.7.R.02. Rationale**

In order for application whitelisting to be effective an agency MUST initially gather information on necessary executables and applications in order to ensure that the implementation is fully effective.

**14.2.7.R.03. Rationale**

Different application whitelisting controls, such as restricting execution based on cryptographic hash, filename, pathname or folder, have various advantages and disadvantages. Agencies need to be aware of this when implementing application whitelisting.

**14.2.7.R.04. Rationale**

Application whitelisting based on parent folder or executable path is futile if access control list permissions allow a system user to write to the folders or overwrite permitted executables.

**14.2.7.R.05. Rationale**

Executables may create multiple processes in the course of execution. These may be identified through examination of programme specifications, testing in a "sandboxed" environment before development and logs of any processes spawned or created.

**14.2.7.R.06. Rationale**

Spawned processes may behave in ways that can compromise system security, change security settings and modify access permissions. Clearly this can be undesirable behaviour.

**14.2.7.R.07. Rationale**

Adequate logging information can allow system administrators to further refine the application whitelisting implementation and detect a pattern of deny decisions for a system user.

**14.2.7.R.08. Rationale**

An example of relevant information that could be included in logs for application whitelisting implementations would be decisions to deny execution incorporating information that would present a reviewer with evidence of misuse.

**14.2.7.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that the default policy is to deny the execution of software.

**14.2.7.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that application whitelisting is used in addition to a strong access control list model and the use of limited privilege accounts.

**14.2.7.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD plan and test application whitelisting mechanisms and processes thoroughly prior to implementation.

**14.2.7.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD restrict the decision whether to run an executable based on the following, in the order of preference shown:

1. validates cryptographic hash;
2. executable absolute path;
3. digital signature; and
4. parent folder.

**14.2.7.C.05. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD restrict the process creation permissions of any executables which are permitted to run by the application whitelisting controls.

**14.2.7.C.06. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD validate executable behaviour, in particular process creation, permission changes, and access control modifications through examination, testing, monitoring and restriction of the permissions.

**14.2.7.C.07. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Logs from the application whitelisting implementation SHOULD include all relevant information.

# 14.3. Web Applications

## Objective

14.3.1. Access to Web content is implemented in a secure and accountable manner.

## Context

### Scope

14.3.2. This section covers information on Web browsers, plug-ins and active content including the development and implementation of appropriate use policies. The requirements in this section apply equally to the Web accessed via the Internet as well as websites accessed on an agency intranet.

## References

14.3.3. A Web whitelisting software application that allows for the management of whitelists can be obtained from:

| Title | Publisher | Source |
|---|---|---|
| **Dynamic Web Whitelisting for Squid** | SourceForge | http://whitetrash.sourceforge.net/ |

14.3.4. Examples of client-side JavaScript controls are available at:

| Title | Publisher | Source |
|---|---|---|
| **NoScript Firefox extension** | Inform Action | http://noscript.net |

## Rationale & Controls

### 14.3.5. Web usage policy

**14.3.5.R.01. Rationale**

If agencies allow system users to access the Web they will need to define the extent of Web access that is granted. This can be achieved through the development, and awareness raising amongst system users, of a Web usage policy.

**14.3.5.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop and implement a policy governing appropriate Web usage.

### 14.3.6. Web proxy

**14.3.6.R.01. Rationale**

Web proxies provide valuable information in determining if malicious code is performing regular interactions over Web traffic. Web proxies also provide usable information if system users are violating agency Web usage policies.

**14.3.6.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use a Web proxy for all Web browsing activities.

**14.3.6.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

An agency's Web proxy SHOULD authenticate system users and provide logging that includes at least the following details about websites accessed:

- address (uniform resource locator);
- time/date;
- system user;
- internal IP address; and
- external IP address.

**14.3.6.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT permit downloading of executable files from external websites unless there is a demonstrable and approved business requirement.

### 14.3.7. Applications and plug-ins

**14.3.7.R.01. Rationale**

Web browsers can be configured to allow the automatic launching of downloaded files. This can occur with or without the system user's knowledge thus making the workstation vulnerable to attack.

**14.3.7.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD disable the automatic launching of files downloaded from external websites.

### 14.3.8. Inspection of TSL

**14.3.8.R.01. Rationale**

As TLS encrypted Web traffic travelling over HTTPS connections can deliver content without any filtering, agencies can reduce this security risk by using TLS inspection so that the Web traffic can be filtered.

**14.3.8.R.02. Rationale**

An alternative of using a whitelist for HTTPS websites can allow websites that have a low security risk of delivering malicious code and have a high privacy requirement like Web banking, to continue to have end-to-end encryption.

**14.3.8.R.03. Rationale**

It is however, important to note that there are many recorded cases of websites generally considered to be a low security risk that have been compromised.

**14.3.8.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies permitting TLS through their gateways SHOULD implement:

- a solution that decrypts and inspects the TLS traffic as per content filtering requirements; or
- a whitelist specifying the addresses (uniform resource locators) to which encrypted connections are permitted, with all other addresses blocked.

### 14.3.9. Legal Advice on the inspection of TLS traffic

**14.3.9.R.01. Rationale**

Encrypted TLS traffic may contain personally identifiable information. Agencies should seek legal advice on whether inspecting such traffic is in breach of the Privacy Act or other legislation. User policies should incorporate an explanation of the security drivers and acknowledgement from users on the policy contents and requirements. Refer to Chapter 9 – Personnel Security and Chapter 15 – Email Security.

**14.3.9.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD seek legal advice regarding the inspection of encrypted TLS traffic by their gateways.

### 14.3.10. Whitelisting / Blacklisting websites

**14.3.10.R.01. Rationale**

Defining a whitelist of permitted websites and blocking all unlisted websites limits one of the most common data delivery and exfiltration techniques used by malicious code. However, if agency personnel have a legitimate requirement to access a numerous and rapidly changing list of websites, agencies will need to consider the practicality and costs of such an implementation. In such cases blacklisting is a limited but none-the-less effective measure.

**14.3.10.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD implement whitelisting for all HTTP traffic being communicated through their gateways.

**14.3.10.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies using a whitelist on their gateways to specify the external addresses, to which encrypted connections are permitted, SHOULD specify whitelist addresses by domain name or IP address.

**14.3.10.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

If agencies do not whitelist websites they SHOULD blacklist websites to prevent access to known malicious websites.

**14.3.10.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies blacklisting websites SHOULD update the blacklist on a frequent basis to ensure that it remains effective.

### 14.3.11. Client-side active content

**14.3.11.R.01. Rationale**

Software that runs on agency systems SHOULD be controlled by the agency. Active content delivered though websites should be constrained so that it cannot arbitrarily access system users' files or deliver malicious code. Unfortunately the implementations of Web browsers regularly contain flaws that permit such activity.

**14.3.11.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD block client-side active content, such as Java and ActiveX, which are assessed as having a limited business impact.

**14.3.11.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD:

- use client-side controls that allow JavaScript on a per website basis; and
- add JavaScript functions used only for malicious purposes to the agency Web content filter or IDS/IPS.

### 14.3.12. Web content filter

#### 14.3.12.R.01. Rationale

Using a Web proxy provides agencies with an opportunity to filter potentially harmful information to system users and their workstations.

#### 14.3.12.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use the Web proxy to filter content that is potentially harmful to system users and their workstations.

### 14.3.13. Website Passwords

#### 14.3.13.R.01. Rationale

Some websites require the use of a userID and password as the authentication mechanism. The management of passwords on these websites is often insecure and there are numerous examples of compromises where tens of thousands, and sometimes millions of passwords are compromised in a single incident. Where the same password is used on multiple websites, an incident can potentially compromise the user's account on *every* website using that password. It is important to treat these websites as insecure and manage passwords appropriately.

#### 14.3.13.C.01. Control: System Classification(s): All Classifications; Compliance: MUST NOT

Users MUST NOT use agency userid and login passwords as credentials for external websites.

#### 14.3.13.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD NOT

Users SHOULD NOT store web site authentication credentials (userID and password) on workstations, remote access devices (such as laptops) or BYO devices.

#### 14.3.13.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD NOT

Users SHOULD NOT use the same password for multiple websites.

# 14.4.Software Application Development

## Objective

14.4.1. Secure programming methods and testing are used for application development in order to minimise the number of coding errors and introduction of security vulnerabilities.

## Context

### Scope

14.4.2. This section covers information relating to the development, upgrade and maintenance of application software used on agency systems.

## References

14.4.3. Additional information relating to software development is contained in:

| Title | Publisher | Source |
|---|---|---|
| **ISO/IEC 27001:2013, A.12.5, Security in Development and Support Processes** | ISO / IEC<br><br>Standards NZ | http://www.iso27001security.com/html/27001.html<br><br>http://www.standards.co.nz |
| **OWASP Secure Coding Practices - Quick Reference Guide** | OWASP | https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide |
| **Secure Code Review** | MITRE Corporation | https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/secure-code-review |
| **Build Security In** | DHS – US-CERT | https://www.us-cert.gov/bsi |
| **Application Security - Application Security & Development A To Z** | US Defense Information Security Agency (DISA) | http://iase.disa.mil/stigs/app-security/app-security/Pages/index.aspx |
| **Writing Secure Code - Michael Howard and David LeBlanc** | Microsoft Press | ISBN Book 978-0-7356-1722-3<br>ISBN eBook 978-0-7356-9146-9 |

## Rationale & Controls

### 14.4.4. Software development environments

#### 14.4.4.R.01. Rationale

Recognised good practice segregates development, testing and production environments to limit the spread of malicious code and minimise the likelihood of faulty code being put into production.

Limiting access to development and testing environments will reduce the information that can be gained by an attacker.

#### 14.4.4.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that software development environments are configured such that:

- there are at least three separate environments covering:
  - development;
  - testing; and
  - production.
- information flow between the environments is strictly limited according to a defined and documented change policy, with access granted only to system users with a clear business requirement;
- new development and modifications only take place in the development environment; and
- write access to the authoritative source for the software (source libraries & production environment) is disabled.

### 14.4.5. Secure programming

#### 14.4.5.R.01. Rationale

Designing software to use the lowest privilege level needed to achieve its task will limit the privileges an attacker could gain in the event they subvert the software security.

#### 14.4.5.R.02. Rationale

Validating all inputs will ensure that the input is within expected ranges, reducing the chance that malicious or erroneous input causes unexpected results.

**14.4.5.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that software developers use secure programming practices when writing code, including:

- designing software to use the lowest privilege level needed to achieve its task;
- denying access by default;
- checking return values of all system calls; and
- validating all inputs.

### 14.4.6. Software testing

**14.4.6.R.01. Rationale**

Software reviewing and testing will reduce the possibility of introducing vulnerabilities into a production environment.

**14.4.6.R.02. Rationale**

Using an independent party for software testing will limit any bias that can occur when a developer tests their own software.

**14.4.6.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Software SHOULD be reviewed or tested for vulnerabilities before it is used in a production environment.

**14.4.6.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Software SHOULD be reviewed or tested by an independent party as well as the developer.

**14.4.6.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Software development SHOULD follow secure coding practices and agency development standards.

# 14.5. Web Application Development

## Objective

14.5.1. Security mechanisms are incorporated into all Web applications by design and implementation.

## Context

### Scope

14.5.2. This section covers the deployment of agency Web applications and websites.

### Protecting Web servers

14.5.3. Even though Web servers may contain only information authorised for release into the public domain, there still remains a need to protect the integrity and availability of the information. As such, Web servers are to be treated in accordance with the requirements of the classification of the system they are connected to.

### Web application components

14.5.4. Web application components at a high level consist of a Web server for presentation, a Web application for processing and a database for content storage. There can be more or fewer components, however in general there is a presentation layer, application layer and database layer.

## References

14.5.5. Further information on Web application security is available from the Open Web Application Security Project at:

| Title | Publisher | Source |
|---|---|---|
| **The Open Web Application Security Project (OWASP) - Reference** | OWASP | http://www.owasp.org |
| **NZ Government Web Toolkit** | DIA | https://webtoolkit.govt.nz/guidance/security-and-privacy-management/designing-for-security-and-privacy/security-and-privacy-assurance/ |
| **Web Design and Applications** | W3C | http://www.w3.org/standards/webdesign/ |
| **Web Development – Patterns and Practices** | Microsoft | https://msdn.microsoft.com/en-us/library/ff921348.aspx |

## Rationale & Controls

### 14.5.6. Agency website content

**14.5.6.R.01. Rationale**

Reviewing active content on agency Web servers will assist in identifying and mitigating information security issues.

**14.5.6.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD review all active content on their Web servers for known information security issues.

### 14.5.7. Segregation of Web application components

**14.5.7.R.01. Rationale**

Web applications are typically very exposed services that provide complex interactions with system users. This greatly increases the security risk of being compromised. By segregating components, the impact of potential application flaws or attacks is limited.

**14.5.7.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD minimise connectivity and access between each Web application component.

### 14.5.8. Web applications

**14.5.8.R.01. Rationale**

The Open Web Application Security Project guide provides a comprehensive resource to consult when developing Web applications.

**14.5.8.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD follow the documentation provided in the Open Web Application Security Project guide to building secure Web applications and Web services.

# 15. Email security

## 15.1. Email Applications

### Objective

Email messages have appropriate protective markings to facilitate the application of handling instructions.

### Context

#### Scope

This section covers information on email policy and usage as it applies to content and protective markings. Information on email infrastructure is located in Section 15.2 - Email Infrastructure.

#### Automatically generated emails

The requirements for emails within this section equally apply to automatically and manually generated emails.

#### Exceptions for receiving unmarked email messages

Where an agency receives unmarked non-government emails as part of its business practice the application of protective markings can be automated.

## References

Further references can be found at:

| Title | Publisher | Source |
|---|---|---|
| **NIST publication SP 800-45 v2, Guidelines on Electronic Mail Security** | NIST | http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf |
| **Detecting socially engineered emails August 2012** | ASD | http://www.asd.gov.au/publications/csocprotect/Socially_Engineered_Email.pdf |

## PSR references

Relevant PSR requirements can be found at:

| Reference | Title | Source |
|---|---|---|
| **PSR Mandatory Requirements** | GOV2, GOV3, GOV4, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2 | http://www.protectivesecurity.govt.nz |
| **PSR content protocols** | Management protocol for information security<br>Management protocol for physical security | http://www.protectivesecurity.govt.nz |
| **PSR requirements sections** | Handling requirements for protectively marked information and equipment<br>Build security awareness<br>Overview of security classifications | http://www.protectivesecurity.govt.nz |
| **Resource centre** | Email fraud: an INFOSEC case study<br>How do I protectively mark or classify a document | http://www.protectivesecurity.govt.nz |

## Rationale & Controls

### Email usage policy

**15.1.7.R.01. Rationale**

There are many security risks associated with the unsecure nature of email that are often overlooked. Documenting them will inform information owners about these security risks and how they might affect business operations.

**15.1.7.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop and implement a policy governing the use of email.

### Email distribution

**15.1.8.R.01. Rationale**

Often the membership, clearance level and nationality of members of email distribution lists is unknown. As such, personnel sending sensitive emails with NZEO or other nationality releasability marked information could be accidentally causing an information security incident by sending such information to distribution lists.

**15.1.8.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that emails containing NZEO or other nationality releasability marked information are sent only to named recipients.

**15.1.8.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT transmit emails or other documents, containing NZEO or other nationality releasability marks, to groups or distribution lists unless the nationality of all members of the distribution lists can be confirmed.

### Protective marking standard

**15.1.9.R.01. Rationale**

Applying markings that reflect the protective requirements of an email informs the recipient on how to appropriately handle the email and any related documents.

**15.1.9.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD comply with the national classification system for the application of protective markings.

### Marking tools

**15.1.10.R.01. Rationale**

Requiring system user intervention in the marking of system user-generated emails assures a conscious decision by the system user, lessening the chance of incorrectly marked emails.

**15.1.10.R.02. Rationale**

Limiting the protective markings a system user is allowed to choose, to those for which the system is accredited lessens the chance that a system user inadvertently over-classifies an email and reminds them of the maximum classification of information that is permitted on the system.

**15.1.10.R.03. Rationale**

Gateway filters usually check only the most recent protective marking. Care MUST be taken when changing protective markings to a classification lower than that of the original email as this can result in emails being forwarded to systems or individuals NOT authorised and cleared to receive them. The instructions in the classification system on changing classifications MUST be observed to avoid a security breach.

**15.1.10.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT allow system users to select protective markings that the system has not been accredited to process, store or communicate.

**15.1.10.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT allow a protective marking to be inserted into system user generated emails without their intervention.

**15.1.10.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT permit system users replying to or forwarding an email to select a protective marking that indicates that the classification of the email is lower than a previous classification used for the email.

### Marking classified and unclassified emails

**15.1.11.R.01. Rationale**

As with paper-based information, all electronic-based information should be marked with an appropriate protective marking in accordance with the classification system. This ensures that appropriate security measures are applied to the information and also assists in preventing the inadvertent release of information into the public domain.

**15.1.11.R.02. Rationale**

When a protective marking is applied to an email it is important that it reflects the highest classification in the body of the email and any attachments within the email.

**15.1.11.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

All classified and unclassified emails MUST have a protective marking.

**15.1.11.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Email protective markings MUST accurately reflect the highest classification of all elements in an email, including any attachments.

**15.1.11.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD include protective markings in the email subject line or header to facilitate early identification of the classification.

### Emails from outside the government

**15.1.12.R.01. Rationale**

If an email is received from outside government the system user has an obligation to determine the appropriate protective measures for the email if it is to be responded to, forwarded or printed.

**15.1.12.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Where an unmarked email has originated outside the government, the agency MUST assess the information and determine how it is to be handled in accordance with the classification system.

### Marking personal emails

**15.1.13.R.01. Rationale**

Applying protective markings to personal emails may create system overheads and will be misleading.

**15.1.13.R.02. Rationale**

Personal emails can be marked as "PERSONAL" or "UNOFFICIAL" to avoid confusion with Official or Classified information.

**15.1.13.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Where an email is of a personal nature and does not contain government information, protective markings SHOULD NOT be used.

### Receiving unmarked emails

**15.1.14.R.01. Rationale**

If an email is received from a New Zealand or overseas government agency without a protective marking the system user has an obligation to contact the originator to seek clarification on the appropriate protection measures for the email or follow established protocols and policy for protective markings.

**15.1.14.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Where an unmarked email has originated from a New Zealand or overseas government agency, personnel SHOULD contact the originator to determine how it is to be handled.

### Receiving emails with unknown protective markings

**15.1.15.R.01. Rationale**

If an email is received with a protective marking that the system user is not familiar with they have an obligation to contact the originator to seek clarification on the protective marking and the appropriate protection measures for the email.

**15.1.15.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Where an email is received with an unknown protective marking from a New Zealand or overseas government agency, personnel SHOULD contact the originator to determine appropriate protection measures.

### Printing

**15.1.16.R.01. Rationale**

The PSR requires that paper-based information have the classification of the information placed at the top and bottom of each piece of paper, in CAPITALS and appearing as the first and last item on each page.

**15.1.16.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD configure systems so that the protective markings appear at the top and bottom of every page when the email is printed, in CAPITALS and appearing as the first and last item on each page.

### Active Web addresses within emails

**15.1.17.R.01. Rationale**

Spoofed emails often contain an active Web address directing personnel to a malicious website to either elicit information or infect their workstation with malicious code. In order to reduce the success rate of such attacks agencies can choose to educate their personnel to neither send emails with active Web addresses or to click on Web addresses in emails that they receive.

**15.1.17.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Personnel SHOULD NOT send emails that contain active Web addresses or click on active Web addresses within emails they receive.

### Awareness of email usage policies

**15.1.18.R.01. Rationale**

In order to protect information and systems, system users will need to be familiar with email usage policies.

**15.1.18.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST make their system users aware of the agency's email usage policies.

### Monitoring email usage

**15.1.19.R.01. Rationale**

Agencies may choose to monitor compliance with aspects of email usage policies such as attempts to send prohibited file types or executables, attempts to send excessive sized attachments or attempts to send classified information without appropriate protective markings.

**15.1.19.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD implement measures to monitor their personnel's compliance with email usage policies.

**15.1.19.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD enforce the use of approved government email systems such as SEEMAIL.

### Public Web-based email services

**15.1.20.R.01. Rationale**

Using public Web-based email services may allow personnel to bypass security measures that agencies will have put in place to protect against malicious code or phishing attempts distributed via email. Web based email services may also by-pass agency context filtering mechanisms.

**15.1.20.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT allow personnel to use public Web-based email services, for processing, receiving or sending emails or attachments for official business.

# 15.2. Email Infrastructure

## Objective

15.2.1. Email infrastructure is hardened, email is secured and protective marking of email messages is enforced.

## Context

### Scope

15.2.2. This section covers information on email infrastructure security. Information on using email applications can be found in Section 15.1 - Email Applications and Section 9.3 - Using the Internet.

### Anti-spoofing controls

15.2.3. Phishing and malware distribution attacks are common internet security threats. To avoid agency domains being used fraudulently (e.g. for spam or spear-phishing), the following should be implemented:

- Sender Policy Framework (SPF)
- DomainKeys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting & Conformance (DMARC) records

15.2.4. Correct configuration of these features will help other mail servers authenticate the email they receive from your domains. It is important to note that DMARC is designed to protect against direct domain spoofing only. DMARC does not eliminate the need for additional forms of protection and analysis. It does, however, provide a way for participating senders and receivers to coordinate protective activities and streamline security processes.

15.2.5. It is also important to note that not all mail service providers enable DMARC, substituting the registration of a free email account as a validation of the user's email account instead. In this case the benefits and reporting associated with DMARC are not available.

## Domain-based Message Authentication, Reporting and Conformance (DMARC)

### Vocabulary

15.2.6. The terms "none", "reject" and "quarantine" are used to describe DMARC actions based on policy modes. In this usage:

- "none" means no action on the transmission or receipt of the email but continue to collect data and send reports;
- By default, email under a "reject" policy setting is not delivered. "Reject" either:
  - refuses to accept non-compliant email, or
  - initially accepts the non-compliant email but prevents an email reaching the user. The acceptance process can generate a Delivery Status Notification (block/"bounce") or simply delete/drop the email (block/delete);
- "quarantine" prevents an email from reaching the user but safely storing it so it can be accessed if required (a potentially suspicious email and/or attachment subject to additional scrutiny). Quarantined items can be released following a review and release process.

### What is DMARC

15.2.7. Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email authentication policy and reporting protocol that:

- complements and unifies the existing validation checks performed by SPF and DKIM;
- checks the stated origin of inbound emails using a combination of Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM);
- establishes a recipient email response for emails that fail the check;
- requests recipient email services to report email sources and origins;
- provides visibility over potentially illegitimate or fraudulent email.

15.2.8. DMARC builds on SPF and DKIM protocols, adding links to the author ("From:") domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, in order to improve and monitor protection of the recipient domain from fraudulent email.

15.2.9. Most email services will check your DMARC record and send aggregated reports including details of all email the service received from the agency, and its origin. This assists in identifying if an individual within the agency is sending email inappropriately or if the agency domain is being spoofed.

### Background, Reference and Implementation Guidance Sources

15.2.10. The IETF published RFC 7489, "Domain-based Message Authentication, Reporting, and Conformance (DMARC)" March 18th, 2015. RFC 7489. This is the principal standards guidance on the implementation and use of DMARC. Further guidance is available from The Global Cyber Alliance (GCA) - see References below.

### Using DMARC

15.2.11. By establishing DMARC, SPF, and DKIM records in DNS, it's possible to advise email service providers which servers should be legitimately sending email from the agency's domain, and what action to take with mail received from any other domains.

15.2.12. In support of DMARC agencies must publish an SPF and a DKIM record. Agencies must also ensure emails agencies send (including those from third party services that send on behalf of the agency) have a DKIM signature that matches the signature in the DKIM record.

15.2.13. Agencies can choose to quarantine or reject messages that fail checks. More specifically:

- Sender Policy Framework (SPF) is used to specify legitimate locations of servers which can send email for your domain;
- DomainKeys Identified Mail (DKIM) isn't supported by all mail servers, but if it is, it can be used to cryptographically sign outgoing mail sent by your servers to give email service providers further confidence that it's legitimate;
- DMARC is used to inform email service providers what action they should take if SPF or DKIM (or both) validation fails;
- One important aspect of DMARC is the action you ask email service providers to take when SPF or DKIM validation fails:
    - a policy of p=none means that they should allow non-compliant emails to be delivered but report the failure to the agency;
    - a policy of p=quarantine requests that they mark the email as spam;
    - a policy of p=reject requests the email service provider to refuse to deliver the email.

15.2.14. Many organisations start with a policy of **p=none**, then modify the configuration to **p=reject** as confidence is gained in the accuracy of the configuration and in systems performance.

15.2.15. To notify other organisations of the use of DMARC agencies may publish a text record in their DNS similar to the following:

- v=DMARC1;
- p=quarantine;
- pct=100;
- rua=mailto:dmarc@agency.govt.nz (where agency is the name of the respective agency).

15.2.16. This informs email recipients that:

- you have a DMARC policy (v=DMARC1)
- any messages that fail DMARC checks should be treated as spam (p=quarantine)
- they should treat 100% of your messages this way (pct=100)
- they should send reports of email received back to you (rua=mailto:dmarc@agency.govt.nz)

15.2.17. It is not unusual to experience minor errors in syntax or other elements of DMARC configuration when first implementing DMARC. Some discussion on common problems, issues and solutions can be found on the DMARC website (see the References table below).

15.2.18. It is unwise for an agency to attempt to move to full implementation of DMARC until there is certainty that the configuration and implementation are stable and operating as intended. The following implementation outline is recommended by the GCA/DMARC organisation (see References below):

- Deploy DKIM & SPF;
- Ensure mailers are correctly aligning the appropriate identifiers;
- Publish a DMARC record with the "none" flag set for the policies, which requests data reports;
- Analyse the data and modify mail streams as appropriate; and
- Modify DMARC policy flags from "none" to "quarantine" to "reject" as experience dictates.

**DMARC Reporting**

15.2.19. DMARC reporting provides information to assist an agency's IT system and email administrators. It can also provide an email asset inventory as well as providing data on spam, phishing and other email exploitation techniques.

15.2.20. DMARC can be configured to produce an aggregate report and a forensic report. In some cases agencies may also send reports to an external organisation such as a DMARC reporting service or a third-party IT service provider. Discretion should be used when providing such information to third parties in order to maintain security and privacy.

## References

15.2.21. Further information on email security is available from the following sources:

| Title | Publisher | Source |
|---|---|---|
| **RFC 3207, SMTP Service Extension for Secure SMTP over Transport Layer Security** | IETF | http://www.ietf.org/rfc/rfc3207.txt |
| **RFC 4408, Sender Policy Framework** | IETF | http://www.ietf.org/rfc/rfc4408.txt |
| **RFC 4686, Analysis of Threats Motivating DomainKeys Identified Mail** | IETF | http://www.ietf.org/rfc/rfc4686.txt |
| **RFC 4871, DomainKeys Identified Mail Signatures** | IETF | http://www.ietf.org/rfc/rfc4871.txt |
| **RFC 5617, DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)** | IETF | http://tools.ietf.org/html/rfc5617 |
| **NIST publication SP 800-45 v2, Guidelines on Electronic Mail Security** | NIST | http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf |
| **CPA Security Characteristic Desktop Email Encryption Version 1.0** | NCSC UK | https://www.ncsc.gov.uk/content/files/protected_files/document_files/CPA%20SC%20Desktop%20Email%20Encryption%20v1-0.pdf |
| **Sender Policy Framework Project** | | www.openspf.org |
| **Measuring The Impact of DMARC's Part in Preventing Business Email Compromise** | Global Cyber Alliance | https://www.globalcyberalliance.org |
| **DMARC** | DMARC | https://dmarc.org/ |
| **Common Problems with DMARC Records** | DMARC | https://dmarc.org/2016/07/common-problems-with-dmarc-records/ |
| **DMARC Reporting: Key Benefits and Takeaways** | Global Cyber Alliance | https://dmarc.globalcyberalliance.org/resource/dmarc-reporting-key-benefits-takeaways/ |
| **Use DMARC to validate email in Office 365** | Microsoft | https://docs.microsoft.com/en-us/office365/securitycompliance/use-dmarc-to-validate-email |
| **Using Multiple signing Algorithms with the ARC (Authenticated Received Chain) Protocol draft-ietf-dmarc-arc-multi-02** | IETF | file:///E:/Background/Standards/IETF/draft-ietf-dmarc-arc-multi-02.pdf |
| **RFC 6376, DomainKeys Identified Mail (DKIM) Signatures** | IETF | https://tools.ietf.org/pdf/rfc6376.pdf |
| **RFC 7208 Sender Policy Framework (SPF) for Authorising Use of Domains in Email, Version 1** | IETF | https://tools.ietf.org/pdf/rfc7208.pdf |
| **RFC 7489, Domain-based Message Authentication, Reporting and Conformance (DMARC)** | IETF | https://tools.ietf.org/html/rfc7489 |

| Title | Publisher | Source |
|---|---|---|
| **RFC 7960 Interoperability Issues between Domain-based Message Authentication, Reporting and Conformance (DMARC) and Indirect Email Flows** | IETF | https://tools.ietf.org/pdf/rfc7960.pdf |
| **RFC 8463 A New Cryptographic Signature Method for DomainKeys Identified Mail (DKIM)** | IETF | https://tools.ietf.org/pdf/rfc8463.pdf |
| **NIST Special Publication SP 800-117** | NIST | https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-177.pdf |
| **NIST Technical Note 1945 – Email Authentication Mechanisms: DMARC, SPF and DKIM, February 16, 2017** | NIST | https://www.nist.gov/publications/email-authentication-mechanisms-dmarc-spf-and-dkim |
| **Email Security and Anti-Spoofing** | NCSC UK | https://www.ncsc.gov.uk/guidance/email-security-and-anti-spoofing |
| **Phishing Attacks** | NCSC UK | https://www.cpni.gov.uk/system/files/documents/4d/9c/Phishing_Attacks_Defending_Your_Organisation_infographic.pdf |
| **Domain-based Message Authentication, Reporting and Conformance (DMARC)** | NCSC UK | https://www.gov.uk/government/publications/email-security-standards/domain-based-message-authentication-reporting-and-conformance-dmarc |
| **Binding Operational Directive BOD-18-01** | DHS | https://cyber.dhs.gov/assets/report/bod-18-01.pdf |
| **Malicious Email Mitigation Strategies** | ACSC | https://acsc.gov.au/publications/protect/malicious_email_mitigation.htm |
| **Mitigating spoofed emails – Sender Policy Framework explained** | ACSC | https://www.acsc.gov.au/publications/protect/spoof_email_sender_policy_framework.htm |

## Rationale & Controls

### 15.2.22. Domain-based Message Authentication, Reporting and Conformance (DMARC)

#### 15.2.22.R.01. Rationale

Phishing and malware distribution attacks are common internet security threats. To limit the possibility of agency domains being used fraudulently (e.g. for spam or spear-phishing), agencies should implement:

- Sender Policy Framework (SPF);
- DomainKeys Identified Mail (DKIM); and
- Domain-based Message Authentication, Reporting & Conformance (DMARC) records.

#### 15.2.22.R.02. Rationale

It is important to note that DMARC depends on the proper implementation of SPF and DKIM.

#### 15.2.22.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Before implementing DMARC agencies SHOULD:

- Create a DMARC policy;
- List all domains used for the sending email;
- Review the configuration of SPF and DKIM for all active domains; and
- Establish one or more monitored inboxes to receive reports.

#### 15.2.22.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD enable DMARC for all email originating from or received by their domain(s), including:

- sending domain owners SHOULD publish a DMARC record advising mail receivers the characteristics of messages purporting to originate from the sender's domain;
- received messages SHOULD be managed in accordance with the agency's published DMARC policy; and
- agencies SHOULD produce failure reports and aggregate reports according to the agency's DMARC policies.

#### 15.2.22.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD review DMARC reports on a regular basis and address any identified anomalies or security issues.

### 15.2.23. Filtering suspicious emails and attachments

**15.2.23.R.01. Rationale**

The intent of blocking specific types of emails is to reduce the likelihood of phishing emails and emails or attachments containing malicious code entering the agency's networks.

**15.2.23.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD configure the following gateway filters:

- inbound and outbound email, including any attachments, that contain:
  - malicious code;
  - content in conflict with the agency's email policy;
  - content that cannot be identified;
  - blacklisted or unauthorised filetypes; and
- encrypted content, when that content cannot be inspected for malicious code or authenticated as originating from a trusted source;
- emails addressed to internal email aliases with source addresses located from outside the domain; and
- all emails arriving via an external connection where the source address uses an internal agency domain name.

### 15.2.24. Active web addresses (URL) embedded in emails

**15.2.24.R.01. Rationale**

Spoofed emails often contain an active (embedded) email address directing users to a malicious website in order to infect the workstation or agency systems with malicious code.

**15.2.24.R.02. Rationale**

An effective defence is to strip and replace active addresses and hyperlinks with text only versions.

**15.2.24.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Email servers SHOULD be configured to strip active addresses and URL's and replace them with text only versions.

### 15.2.25. Preventing unmarked or inappropriately marked emails

**15.2.25.R.01. Rationale**

Unmarked or inappropriately marked emails can be blocked at two points, the workstation or the email server. The email server is often the preferred location to block emails as it is a single location under the control of system administrators that can enforce the requirement for the entire network. In addition email servers can apply controls for emails generated by applications.

**15.2.25.R.02. Rationale**

Whilst blocking at the email server is considered the most appropriate control there is an advantage in also blocking at the workstation. This approach adds an extra layer of security and will also reduce the likelihood of a data spill occurring on the email server.

**15.2.25.R.03. Rationale**

For classified systems is it important to note that all emails containing classified information MUST be protectively marked. This requirement is outlined in Section 15.1 - Email Applications.

**15.2.25.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST prevent unmarked and inappropriately marked emails being sent to intended recipients by blocking the email at the email server, originating workstation or both.

**15.2.25.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST enforce protective marking of emails so that checking and filtering can take place.

**15.2.25.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD enforce protective marking of emails so that checking and filtering can take place.

### 15.2.26. Blocking of outbound emails

**15.2.26.R.01. Rationale**

Blocking an outbound email with a valid protective marking or endorsement (e.g. NZEO) that indicates the email exceeds the classification of the communication path, stops data spills.

**15.2.26.R.02. Rationale**

Agencies may remove protective markings from emails destined for private citizens and businesses once they have been approved for release from the agency's gateways.

**15.2.26.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST configure systems to block any outbound emails with a protective marking or endorsement indicating that the content of the email exceeds the classification of the communication path.

**15.2.26.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD configure systems to log every occurrence of a blocked email.

### 15.2.27. Blocking of inbound emails

**15.2.27.R.01. Rationale**

Blocking an inbound email with a valid protective marking that indicates the email or its attachment exceeds the classification the receiving system is accredited to process will prevent a data spill from occurring on the receiving system.

**15.2.27.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST configure email systems to reject, log and report inbound emails with protective markings indicating that the content of the email exceeds the accreditation of the receiving system.

**15.2.27.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD notify the intended recipient of any blocked emails.

### 15.2.28. Undeliverable messages

**15.2.28.R.01. Rationale**

Undeliverable or "bounce" emails are commonly sent by email servers to the original sender when the email cannot be delivered, often because the destination address is invalid. Because of the common spamming practice of spoofing sender addresses, this can result in a large amount of bounce emails being sent to an innocent third party. Sending bounces only to senders that can be verified via the Sender Policy Framework (SPF) or other trusted means avoids contributing to this problem and allows other government agencies and trusted parties to receive legitimate bounce messages. See also 15.2.15 Sender Policy Framework (SPF).

**15.2.28.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD send notification of undeliverable, bounced or blocked emails to senders that can be verified via SPF or other trusted means.

### 15.2.29. Automatic forwarding of emails

**15.2.29.R.01. Rationale**

Unsecured automatic forwarding of emails can pose a serious risk to the unauthorised disclosure of classified information, for example, a system user may set up a server-side rule to automatically forward all emails to a personal email account. This can result in classified emails being forwarded to the personal email account.

**15.2.29.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that the requirements for blocking unmarked and outbound emails are also applied to automatically forwarded emails.

### 15.2.30. Open relay email servers

**15.2.30.R.01. Rationale**

An open relay email server (or open mail relay) is a server that is configured to allow anyone on the Internet to send emails through the server. Such configurations are highly undesirable as they allow spammers and worms to exploit this functionality to send emails through the server.

**15.2.30.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD disable open email relaying so that email servers will only relay messages destined for the agency's domain(s) and those originating from within that domain.

### 15.2.31. Email server maintenance activities

**15.2.31.R.01. Rationale**

Email servers perform a critical business function for many agencies; as such it is important that agencies perform regular email server auditing, security reviews and vulnerability analysis activities.

**15.2.31.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD perform regular email server auditing, security reviews and vulnerability analysis activities.

### 15.2.32. Centralised email gateways

**15.2.32.R.01. Rationale**

Without a centralised email gateway it is exceptionally difficult to deploy Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and outbound email protective markings verification.

Attackers will almost invariably avoid using the primary email server when sending malicious emails. This is because the backup or alternative gateways are often poorly maintained with out-of-date blacklists and content filtering.

**15.2.32.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Where an agency has system users that send email from outside the agency's network, an authenticated and encrypted channel MUST be configured to allow email to be sent via the centralised email gateway.

**15.2.32.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD route email through a centralised email gateway.

**15.2.32.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Where backup or alternative email gateways are in place, additional email gateways SHOULD be maintained at the same standard as the primary email gateway.

### 15.2.33. Transport Layer Security (TLS)

**15.2.33.R.01. Rationale**

Email can be intercepted anywhere between the originating email server and the destination email server. Email transport between organisations and agencies is usually over the internet or other unsecured public infrastructure so it is important that email interception is carefully managed and suitable controls applied. One effective measure is to use TLS to encrypt the email traffic **between email servers**.

**15.2.33.R.02. Rationale**

Enabling TLS on the originating and accepting email server will defeat passive attacks on the network, with the exception of cryptanalysis against email traffic. TLS encryption **between email servers** will not interfere with email content filtering schemes. Email servers will remain compatible with other email servers as IETF's RFC 3207 specifies the encryption as opportunistic.

**15.2.33.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST enable opportunistic TLS encryption as defined in IETF's RFC 3207 on email servers that make incoming or outgoing email connections over public infrastructure.

**15.2.33.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD implement TLS between email servers where significant volumes of classified information are passed via email to other agencies.

## 15.2.34. Sender Policy Framework (SPF)

**15.2.34.R.01. Rationale**

The Sender Policy Framework (SPF) is an open standard specifying a technical method to prevent sender address forgery.

An SPF-protected domain is less attractive to spammers and phishers because the forged e-mails are more likely to be caught in spam filters which check the SPF record. Because an SPF-protected domain is less attractive as a spoofed address, it is less likely to be blacklisted by spam filters and so is less disruptive to email traffic.

**15.2.34.R.02. Rationale**

Having a proper Sender Policy Framework (SPF) record increases the chances people will get emails you send. Without one, your email has a greater chance of being marked as Spam.

**15.2.34.R.03. Rationale**

SPF and alternatives such as Sender ID aid in the detection of spoofed email server address domains. The SPF record specifies a list of IP addresses or domains that are allowed to send mail from a specific domain. If the email server that transmitted the email is not in the list, the verification fails (there are a number of different fail types available).

**15.2.34.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST:

- specify mail servers using SPF or Sender ID; and
- mark, block or identify incoming emails that fail SPF checks for notification to the email recipient.

**15.2.34.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD:

- use a hard fail SPF record when specifying email servers; and
- use SPF or Sender ID to verify the authenticity of incoming emails.

**15.2.34.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD refer to the SPF recommendations in IETF's RFC 4408.

### 15.2.35. DomainKeys Identified Mail (DKIM)

#### 15.2.35.R.01. Rationale

DKIM enables a method of determining spoofed email content. The DKIM record specifies a public key that will sign the content of the message. If the signed digest in the email header doesn't match the signed content of the email the verification fails.

#### 15.2.35.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD enable DKIM signing on all email originating from their domain.

#### 15.2.35.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use DKIM in conjunction with SPF.

#### 15.2.35.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD verify DKIM signatures on emails received, taking into account that email distribution list software typically invalidates DKIM signatures.

#### 15.2.35.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD

Where agencies operate email distribution list software used by external senders, agencies SHOULD configure the software so that it does not impair the validity of the sender's DKIM signature.

# 16. Access Control

## 16.1. Identification and Authentication

### Objective

16.1.1. Identification and authentication requirements are implemented in order to provide a secure means of access to information and systems.

### Context

**Scope**

16.1.2. This section covers information on the identification and authentication of all system users.

16.1.3. Access Control is any mechanism by which an individual, system or application grants or revokes the right to access some location, system, data, or perform some action. Access Control must be supported by an appropriate organisational policy.

16.1.4. In this context a user is a real person. Machine or device to device communication and interaction may also require authentication. It is important to note, however, that the usual mechanisms applied to real persons cannot always be used in device to device authentication, for example, biometrics.

16.1.5. In Information Technology, a user will usually register a person's identity supported by some evidence of identity (EoI). This will be accompanied by an authority or approval to access information, usually from a manager or other executive. The authentication system will then issue credentials, usually user ID and password, but may also include tokens or use biometrics. The credentials are the means by which a user (a person) accesses an information technology system and are verified each time a user logs onto a system.

16.1.6. Access Control systems manage access rights, including:

- Physical access to locations;
- File system permissions, including physical documents and files, such as create, read, edit or delete data;
- Program permissions, such as the right to execute a programme;
- Data rights, such as the right to retrieve, print or update information in a database.

### Methods for user identification and authentication

16.1.7. Authentication is the process by which a claimed identity is verified and access permissions are confirmed before access is granted.

16.1.8. User authentication can be achieved by various means, including biometrics, cryptographic tokens, software tokens, passphrases, passwords and smartcards. Where this manual refers to passwords it equally applies to passphrases.

16.1.9. Authentication mechanisms are invariably described in terms of factors of authentication as follows:

1. Something you have (preferably NOT the device itself but a SEPARATE authentication device such as a token, RFID card or smartcard). This is also known as the *possession* factor;

2. Something you know such as a PIN, One-Time Password (OTP), reusable password, pattern or other component of a standard authentication mechanism. This is also described as the *knowledge* factor;

3. Something you are (biometrics of various types). This is also described as the *inherence* factor.

16.1.10. Commonly used two factor authentication schemes are combinations of physical presence, a token and a PIN/Password. Biometrics are less commonly used on mobile or remote systems.

### Software Tokens

16.1.11. Software Tokens, Soft Tokens or "softokens" are typically applications that run on mobile devices such as smart phones, tablets, laptops other workstations. They are sometimes also known as "virtual tokens". When soft tokens are used the device itself then becomes the "possession factor". Functionality may include:

- Transfer between devices by the user.
- Use of Quick Response (QR) codes to facilitate deployment.
- Manages international time zones changes when travelling.

16.1.12. The soft token (secret) is vulnerable to any attacker that can gain full access to the device through theft, loss or download of malware. This is not as secure as a *separate* hardware token which is more resistant to attack and tampering.

### Passwords and Password storage

16.1.13. Password length and composition (character type) has been found to be a primary factor in characterizing password strength [Strength] [Composition]. Passwords that are too short yield to brute force attacks as well as to dictionary attacks using words and commonly chosen passwords.

16.1.14. The minimum password length that should be required depends to a large extent on the threat model being addressed. Online attacks where the attacker attempts to log in by guessing the password can be mitigated by limiting the rate of login attempts permitted. In order to prevent an attacker (or a persistent claimant with poor typing skills) from easily inflicting a denial-of-service attack on the subscriber by making many incorrect guesses, passwords need to be complex enough that rate limiting does not occur after a modest number of erroneous attempts, but does occur before there is a significant chance of a successful guess.

16.1.15. Offline attacks are sometimes possible when one or more hashed passwords are obtained by the attacker through a database breach. The ability of the attacker to determine one or more users' passwords depends on the way in which the password is stored. Commonly, passwords are salted with a random value and hashed, preferably using a computationally expensive algorithm. Even with such measures, the current ability of attackers to compute many billions of hashes per second with no rate limiting requires passwords intended to resist such attacks to be orders of magnitude more complex than those that are expected to resist only online attacks.

16.1.16. Users should be encouraged to make their passwords as lengthy as they want, within reason. A reasonable upper limit is 64 characters.

16.1.17. Since the size of a hashed password is independent of its length, there is no reason not to permit the use of lengthy passwords (or pass phrases) if the user wishes. Extremely long passwords (perhaps megabytes in length) could conceivably require excessive processing time to hash, so it is reasonable to have some limit.

### Password Character Set Limitations

16.1.18. Limitations set on credential or password length or on the use of special characters can facilitate brute-force attacks.

16.1.19. A brute-force attack is a trial-and-error method used to discover information such as a user password, a personal identification number (PIN), or to decrypt encrypted data. Automation can be used to generate a large number of consecutive guesses. Similar methods are used by security analysts to test an organisation's system security, often described as penetration testing.

16.1.20. Organisations should not permit the use of short or no-length passwords, restrict the use of character sets or apply encoding restrictions on entry of or storage of credentials.

16.1.21. Password length, character variation and use of symbols, numbers and special characters including emoticons will increase the resistance of hash values to attack. These practices will assist in limiting a variety of malicious attacks on IT systems.

### Hashing

16.1.22. Hashing is a one-way function where data is mapped to a fixed-length value. It also protects a password by producing ciphertext. Contrast hashing with encryption which is a two-way function where the data can be encrypted and decrypted.

16.1.23. In general, applications use secure hashing algorithms for:

- Password Protection;
- Integrity checking: e.g. a tamper-evident seal for a file (check-sum);
- Authentication: e.g. Digital signatures, Hashed Message Authentication Codes (HMAC) and pseudo-random number generation (PRNG).

16.1.24. Very large passwords can create system performance issues and choke points. Password hashing reduces all passwords to a fixed length, improving efficiency and reducing the volume of credential traffic.

16.1.25. Approved hash functions have the following characteristics:

- **One-way**: It is computationally infeasible to find any input that maps to any pre-specified output; and
- **Collision Resistant**: It is computationally infeasible to find any two distinct inputs that map to the same output.

Refer also to 17.4 – Transport Layer Security.

### Salting

16.1.26. Refer to 17.2.13 for discussion on the use of salts; and 17.2.25 for the related rationale and controls.

### Key Stretching

16.1.27. Key stretching is a technique of slowing the hash function as a means of discouraging attacks (making the time spent not worthwhile while increasing the length of the detection window). Typically this is achieved through a high iteration count in the hashing process, in some cases as high as 10,000 iterations. It is important to note the stretching of the key does not alter the entropy (randomness) of the key-space, rather it complicates the method of computing the stretched key.

16.1.28. However note the time versus security trade off here as key stretching comes at the cost of more time spent in validating user connection requests. This is particularly apparent for transactional or high user-volume websites and networks with large numbers of users.

## References

16.1.29. Additional information relating to Access Control and User Authentication can be found at:

| Title | Publisher | Source |
|---|---|---|
| **ISO/IEC 27002:2013, Section 11,**<br>**User Password Management**<br>**Password Use**<br>**User Identification and Authentication** | ISO / IEC<br><br>Standards NZ | http://www.iso27001security.com/html/27001.html<br>http://www.standards.co.nz |
| **RFC 8492 Secure Password Ciphersuites for Transport Layer Security (TLS) FEB 2019** | IETF | https://tools.ietf.org/html/rfc8492 |
| **Evidence of Identity** | DIA | http://www.dia.govt.nz/DIAWebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Standard-Index?OpenDocument |
| **The NZ Government Authentication Standard** | GCIO | http://ict.govt.nz/guidance-and-resources/standards-compliance/authentication-standards/ |
| **The NZ Government Authentication Standard Appendix A – Definitions** | GCIO | http://ict.govt.nz/guidance-and-resources/standards-compliance/authentication-standards/guide-authentication-standards-online-services/appendix-def |
| **Special Publication 800-63-2 – August 2013**<br>**Electronic Authentication Guideline** | NIST | http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf |
| **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** | IETF | https://tools.ietf.org/pdf/rfc2898.pdf |
| **RFC 8018 PKCS #5: Password-Based Cryptography Specification Version 2.1** | IETF | https://tools.ietf.org/pdf/rfc8018.pdf |
| **NIST Special Publication 800-63-3 series - Digital Identity Guidelines** | NIST | https://pages.nist.gov/800-63-3/ |
| **NIST Special Publication 800-106 Randomized Hashing for Digital Signatures** | NIST | https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-106.pdf |
| **NIST Special Publication 800-107 Revision 1 Recommendation for Applications Using Approved Hash Algorithms** | NIST | https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf |

| Title | Publisher | Source |
|---|---|---|
| **NIST Special Publication 800-132 Recommendation for Password-Based Key Derivation Part 1: Storage Application** | NIST | https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf |
| **The academic paper The Adoption of Single Sign-On and Multifactor Authentication in Organisations – A Critical Evaluation Using TOE Framework**<br>**Issues in Informing Science and Information Technology Volume 7, 2010** | Issues in Informing Science and Information Technology (IISIT) | http://iisit.org/Vol7/IISITv7p161-189DCosta788.pdf |
| **Multi-factor Authentication January 2012** | ASD | http://www.asd.gov.au/publications/csocprotect/Multi_Factor_Authentication.pdf |
| **Mitigating the use of stolen credentials to access agency information – August 2012** | ASD | http://www.asd.gov.au/publications/csocprotect/Stolen_Credentials.pdf |
| **NIST Special Publication 800-53, Revision 4 - Security and Privacy Controls for Federal Information Systems and Organizations** | NIST | http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf |
| **Establishing Security Best Practices in Access Control** | Security Research Labs | www.git-security.com/file/track/5743/1 |
| **Windows Server - Interactive logon: Do not display last user name** | Microsoft Technet | https://technet.microsoft.com/en-us/library/jj852247.aspx |
| **Windows Server: Network access: Do not allow storage of passwords and credentials for network authentication** | Microsoft Technet | https://technet.microsoft.com/en-us/library/jj852185.aspx |

## PSR references

16.1.30. Relevant PSR requirements can be found at:

| Reference | Title | Source |
|---|---|---|
| **PSR Mandatory Requirements** | GOV5, GOV6, GOV7, PERSEC1, PERSEC2, PERSEC3, PERSEC4, INFOSEC1, INFOSEC2, INFOSEC3 and INFOSEC4 | http://www.protectivesecurity.govt.nz |
| **PSR content protocols** | Management protocol for information security<br>Management protocol for physical security<br>Management protocol for personnel security | http://www.protectivesecurity.govt.nz |
| **PSR requirements sections** | Security zones<br>Handling requirements for protectively marked information and equipment<br>Supply chain security<br>Understanding the physical security lifecycle | http://www.protectivesecurity.govt.nz |
| **Managing specific scenarios** | Working away from the office<br>Mobile and remote working | http://www.protectivesecurity.govt.nz |

## Rationale & Controls

### 16.1.31. Policies and procedures

**16.1.31.R.01. Rationale**

Developing policies and procedures will ensure consistency in identification, authentication and authorisation, across agency systems and with relevant standards.

**16.1.31.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST:

- develop and maintain a set of policies and procedures covering system users':
  - identification;
  - authentication;
  - authorisation; and
- make their system users aware of the agency's policies and procedures.

### 16.1.32. System user identification

**16.1.32.R.01. Rationale**

Having uniquely identifiable system users ensures accountability.

**16.1.32.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that all system users are:

- uniquely identifiable; and
- authenticated on each occasion that access is granted to a system.

### 16.1.33. Shared accounts

**16.1.33.R.01. Rationale**

Sharing passwords and UserIDs (credentials) may be convenient but invariably hampers efforts to identify a specific user and attribute actions to a specific person or system. While agencies and users find convenience in sharing credentials, doing so is highly risky. Shared credentials can defeat accountability and the attribution and non-repudiation principles of access control. This is particularly important where administrative access to networks and servers or access to classified information is provided through shared credentials.

**16.1.33.C.01. Control:** System Classification(s): TS; Compliance: MUST NOT

Agencies MUST NOT use shared credentials to access accounts.

**16.1.33.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT use shared credentials to access accounts.

### 16.1.34. System user identification for shared accounts

**16.1.34.R.01. Rationale**

Agencies may have a compelling business reason for the use of shared accounts. These may include Anonymous, Guest and Temporary Employee (such relieving a receptionist) credentials. It may not be possible to attribute the use of such accounts to a specific person.

**16.1.34.R.02. Rationale**

As shared accounts are non user-specific, agencies will need to determine an appropriate method of attributing actions undertaken by such accounts to specific personnel. For example, a logbook may be used to document the date and time that a person takes responsibility for using a shared account and the actions logged against the account by the system.

**16.1.34.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

If agencies choose to allow shared, non user-specific accounts they MUST ensure that an independent means of determining the identification of the system user is implemented.

### 16.1.35. Methods for system user identification and authentication

**16.1.35.R.01. Rationale**

A personal identification number is typically short in length and employs a small character set, making it susceptible to brute force attacks.

**16.1.35.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT use a numerical password (or personal identification number) as the sole method of authenticating a system user to access a system.

**16.1.35.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that they combine the use of multiple methods when identifying and authenticating system users.

### 16.1.36. Protecting stored authentication information

**16.1.36.R.01. Rationale**

Limiting the storage of unprotected authentication information reduces the possibility of an attacker finding and using the information to access a system under the guise of a valid system user.

**16.1.36.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT allow storage of unprotected authentication information that grants system access, or decrypts an encrypted device, to be located on, or with the system or device, to which the authentication information grants access.

### 16.1.37. Protecting authentication data in transit

#### 16.1.37.R.01. Rationale

Secure transmission of authentication information will reduce the risk of interception and subsequent use of the authentication information by an attacker to access a system under the guise of a valid system user.

#### 16.1.37.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that system authentication data is protected when in transit on agency networks or All-of-Government systems.

### 16.1.38. Hashing

#### 16.1.38.R.01. Rationale

Hashing is a means of protecting stored passwords or other authentication data by cryptographically converting the password to fixed length ciphertext. This protects against incidents where an unsanctioned copy of the password or authentication database has been made, exported or the database otherwise compromised. Approved cryptographic protocols are discussed in Chapter 17. See also Section 17.2 for discussion on the use of salts to strengthen the cryptographic resistance of a hash.

#### 16.1.38.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Password and other authentication data SHOULD be hashed before storage using an approved cryptographic protocol and algorithm.

### 16.1.39. Identification of foreign nationals

#### 16.1.39.R.01. Rationale

Where systems contain NZEO or other nationalities releasability marked or protectively marked information, and foreign nationals have access to such systems, it is important that agencies implement appropriate security measures to assist in identifying users that are foreign nationals. Such measures will assist in preventing the release of sensitive information to those not authorised to access it.

#### 16.1.39.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Where systems contain NZEO or other nationalities releasability marked or protectively marked information, agencies MUST provide a mechanism that allows system users and processes to identify users who are foreign nationals, including seconded foreign nationals.

#### 16.1.39.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies using NZEO systems SHOULD ensure that identification includes specific nationality for all foreign nationals, including seconded foreign nationals.

## 16.1.40. Password selection policy

**16.1.40.R.01. Rationale**

Passwords are the primary authentication mechanism for almost all information systems and are fundamental part of access and authentication processes and mechanisms. While there are some limitations in the use of passwords, they remain the most cost effective means available with current technology.

**16.1.40.R.02. Rationale**

Passwords are subject to three principal groups of risks:

1. Intentional password sharing;
2. Password theft, loss or compromise; and
3. Password guessing and cracking.

**16.1.40.R.03. Rationale**

Associated with these risk groups are four principal methods of attacking passwords:

1. Interactive attempts including password guessing, brute force attacks or some knowledge of the user or agency.
2. Obtaining the password through social engineering or phishing.
3. Compromising the password through oversight, observation, use of keyloggers, cameras etc.
4. Cracking through network traffic interception, misconfiguration, malware, data capture etc. For example a simple eight-letter password can today be brute-forced in minutes by software freely available on the Internet.

**16.1.40.R.04. Rationale**

Password controls are designed to manage these risks and attack methods using the controls specified in this section. For example, passwords with at least ten characters utilising upper and lower case, numbers and special characters have a much greater resistance to brute force attacks. When use in combination with controls such as password history and regular password change, passwords can present high resistance to known attack methods.

**16.1.40.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST implement a password policy enforcing:

- a minimum password length of ten characters, consisting of at least three of the following character sets:
  - lowercase characters (a-z);
  - uppercase characters (A-Z);
  - digits (0-9); and
  - punctuation and special characters.

**16.1.40.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD implement a password policy enforcing either:

- a minimum password length of 16 characters with no complexity requirement; or
- a minimum password length of ten characters, consisting of at least three of the following character sets:
  - lowercase characters (a-z);
  - uppercase characters (A-Z);
  - digits (0-9); and
  - punctuation and special characters.

### 16.1.41. Password management

**16.1.41.R.01. Rationale**

Changing a password at least every 90 days will limit the time period in which a disclosed password could be used by an unauthorised system user.

**16.1.41.R.02. Rationale**

Preventing a system user from changing their password more than once a day will stop the system user from immediately changing their password back to their old password.

**16.1.41.R.03. Rationale**

Checking passwords for compliance with the password selection policy will allow system administrators to detect unsafe password selection and ensure that the system user changes it.

**16.1.41.R.04. Rationale**

Requiring a system user to change a password on account reset will ensure that the system user has a password known only to that user and is more easily remembered.

**16.1.41.R.05. Rationale**

Disallowing predictable reset passwords will reduce the security risk of brute force attacks and password guessing attacks.

**16.1.41.R.06. Rationale**

Using different passwords when resetting multiple accounts will prevent a system user whose account has been recently reset from logging into another such account.

**16.1.41.R.07. Rationale**

Disallowing passwords from being reused within eight changes will prevent a system user from cycling between a small subset of passwords.

**16.1.41.R.08. Rationale**

Disallowing sequential passwords will reduce the security risk of an attacker easily guessing a system user's next password based on their knowledge of the system user's previous password.

**16.1.41.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST:

- ensure that passwords are changed at least every 90 days;
- prevent system users from changing their password more than once a day;
- check passwords for compliance with their password selection policy where the system cannot be configured to enforce complexity requirements; and
- force the system user to change an expired password on initial logon or if reset.

**16.1.41.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST NOT

Agencies MUST NOT:

- allow predictable reset passwords;
- reuse passwords when resetting multiple accounts;
- store passwords in the clear on the system;
- allow passwords to be reused within eight password changes; and
- allow system users to use sequential passwords.

**16.1.41.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD:

- ensure that passwords are changed at least every 90 days;
- prevent system users from changing their password more than once a day;
- check passwords for compliance with their password selection policy where the system cannot be configured to enforce complexity requirements; and
- force the system user to change an expired password on initial logon or if the password is reset.

**16.1.41.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT:

- allow predictable reset passwords;
- reuse passwords when resetting multiple accounts;
- store passwords in the clear on the system;
- allow passwords to be reused within eight password changes; and
- allow system users to use sequential passwords.

### 16.1.42. Resetting passwords

**16.1.42.R.01. Rationale**

To reduce the likelihood of social engineering attacks aimed at service desks, agencies will need to ensure that system users provide sufficient evidence to verify their identity when requesting a password reset for their system account.

This evidence could be in the form of:

- the system user physically presenting themselves and their security pass to service desk personnel who then reset their password;
- physically presenting themselves to a known colleague who uses an approved online tool to reset their password; or
- establishing their identity by responding correctly to a number of questions before resetting their own password.

**16.1.42.R.02. Rationale**

Issuing complex reset passwords maintains the security of the user account during the reset process. This can also present an opportunity to demonstrate the selection of strong passwords.

**16.1.42.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure system users provide sufficient evidence to verify their identity when requesting a password reset for their system account.

### 16.1.43. Password authentication

**16.1.43.R.01. Rationale**

LAN Manager's authentication mechanism uses a very weak hashing algorithm known as the LAN Manager hash algorithm. Passwords hashed using the LAN Manager hash algorithm can easily be compromised using rainbow tables or brute force attacks.

**16.1.43.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD disable LAN Manager for password authentication on workstations and servers.

### 16.1.44. Session termination

**16.1.44.R.01. Rationale**

Developing a policy to automatically logout and shutdown workstations after an appropriate time of inactivity will assist in preventing the compromise of an unattended workstation that contains classified or sensitive information. Such a policy will also reduce the power consumption requirements of the agency during non-operational hours.

**16.1.44.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD develop and implement a policy to automatically logout and shutdown workstations after an appropriate time of inactivity.

### 16.1.45. Session and screen locking

**16.1.45.R.01. Rationale**

Screen and session locking will prevent access to an unattended workstation.

**16.1.45.R.02. Rationale**

Ensuring that the screen does not appear to be turned off while in the locked state will prevent system users from forgetting they are still logged in and will prevent other system users from mistakenly thinking there is a problem with a workstation and resetting it.

**16.1.45.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST:

- configure systems with a session or screen lock;
- configure the lock to activate:
  - after a maximum of 10 minutes of system user inactivity; or
  - if manually activated by the system user;
- configure the lock to completely conceal all information on the screen;
- ensure that the screen is not turned off or enters a power saving state before the screen or session lock is activated;
- have the system user reauthenticate to unlock the system; and
- deny system users the ability to disable the locking mechanism.

**16.1.45.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD:

- configure systems with a session or screen lock;
- configure the lock to activate:
  - after a maximum of 15 minutes of system user inactivity; or
  - if manually activated by the system user;
- configure the lock to completely conceal all information on the screen;
- ensure that the screen is not turned off or enters a power saving state before the screen or session lock is activated;
- have the system user reauthenticate to unlock the system; and
- deny system users the ability to disable the locking mechanism.

### 16.1.46. Suspension of access

**16.1.46.R.01. Rationale**

Locking a system user account after a specified number of failed logon attempts will reduce the risk of brute force attacks.

**16.1.46.R.02. Rationale**

Removing a system user account when it is no longer required will prevent personnel from accessing their old account and reduce the number of accounts that an attacker can target.

**16.1.46.R.03. Rationale**

Suspending inactive accounts after a specified number of days will reduce the number of accounts that an attacker can target.

**16.1.46.R.04. Rationale**

Investigating repeated account lockouts will reduce the security risk of any ongoing brute force logon attempts and allow security management to act accordingly.

**16.1.46.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST:

- Record all successful and failed logon attempts;
- lock system user accounts after three failed logon attempts;
- have a system administrator reset locked accounts;
- remove or suspend system user accounts as soon as possible when personnel no longer need access due to changing roles or leaving the agency; and
- remove or suspend inactive accounts after a specified number of days.

**16.1.46.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD:

- lock system user accounts after three failed logon attempts;
- have a system administrator reset locked accounts;
- remove or suspend system user accounts as soon as possible when personnel no longer need access due to changing roles or leaving the agency; and
- remove or suspend inactive accounts after a specified number of days.

### 16.1.47. Investigating repeated account lockouts

**16.1.47.R.01. Rationale**

Repeated account lockouts may be an indication of malicious activity being directed towards compromising a particular account.

**16.1.47.C.01. Control:** System Classification(s): C, S, TS; Compliance: SHOULD

Agencies SHOULD ensure that repeated account lockouts are investigated before reauthorising access.

### 16.1.48. Logon banner

**16.1.48.R.01. Rationale**

A logon banner for a system serves to remind system users of their responsibilities when using the system. It may also be described as a "Splash Screen" or "User Consent Screen".

**16.1.48.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD have a logon banner that requires a system user to acknowledge and accept their security responsibilities before access to the system is granted.

**16.1.48.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD seek legal advice on the exact wording of logon banners.

**16.1.48.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agency logon banners SHOULD cover issues such as:

- the system's classification;
- access only being permitted to authorised system users;
- the system user's agreement to abide by relevant security policies;
- the system user's awareness of the possibility that system usage is being monitored;
- the definition of acceptable use for the system; and
- legal ramifications of violating the relevant policies.

### 16.1.49. Displaying when a system user last logged in

**16.1.49.R.01. Rationale**

Displaying when a system user has last logged onto a system will assist system users in identifying any unauthorised use of their account. Accordingly, when any case of unauthorised use of an account is identified, it should be reported to an ITSM immediately for investigation.

**16.1.49.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD configure systems to display the date and time of the system user's previous login during the login process.

## 16.1.50. Display of Last User Logged on

### 16.1.50.R.01. Rationale

Agency systems that process or store sensitive information, have monitors displayed in unsecured locations, or are remotely accessed, revealing logged on user's full names or domain account names presents a number of risks. These include user spoofing (user name is now known), presentation of a target of opportunity for unsecured workstations and a potential privacy breach. These risks are higher on shared workstations, such as Internet access workstations.

### 16.1.50.R.02. Rationale

In Windows and some other systems it is possible that individuals with administrator access can identify last logged information through access to Local Group Policy. This level of access must be carefully controlled and monitored.

### 16.1.50.R.03. Rationale

Some systems may cache credentials on any workstation or other parts of the system. Caching is frequently found where workstations, laptops or mobile devices require domain credentials when disconnected from the domain. This practice can pose some risk and recommended practice is to disable credential caching except where specifically required.

### 16.1.50.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT permit the display of last logged on username, credentials or other identifying details.

### 16.1.50.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT permit the caching of credentials unless specifically required.

# 16.2.System Access

## Objective

16.2.1. Access to information on systems is controlled in accordance with agency policy and this manual.

## Context

### Scope

16.2.2. This section covers information on accessing systems for all system users. Additional information on privileged users can be found in Section 16.3 - Privileged Access and additional information on security clearance, briefing and authorisation requirements can be found in Section 9.2 - Authorisations, Security Clearances and Briefings.

## Rationale & Controls

### 16.2.3. Access from foreign controlled systems and facilities

**16.2.3.R.01. Rationale**

If a New Zealand system is to be accessed overseas it will need to be from at least a facility owned by a country that New Zealand has a multilateral or bilateral agreement with. NZEO systems can be accessed only from facilities under the sole control of the government of New Zealand and by New Zealand citizens.

**16.2.3.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT allow access to NZEO information from systems and facilities not under the sole control of the government of New Zealand and New Zealand citizens.

**16.2.3.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Unless a multilateral or bilateral security agreement is in place, agencies SHOULD NOT allow access to classified information from systems and facilities not under the sole control of the government of New Zealand and New Zealand citizens.

### 16.2.4. Enforcing authorisations on systems

**16.2.4.R.01. Rationale**

Enforcing authorisations of system users through the use of access controls on a system will assist in enforcing the need-to-know principle.

**16.2.4.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST have authorisation of system users enforced by access controls.

### 16.2.5. Protecting compartmented information on systems

**16.2.5.R.01. Rationale**

Compartmented information is particularly sensitive and as such extra measures need to be put in place on systems to restrict access to those with sufficient authorisation, briefings and a demonstrated need-to-know or need- to access.

**16.2.5.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST restrict access to compartmented information. Such restriction MUST be enforced by the system.

### 16.2.6. Developing an access control list

**16.2.6.R.01. Rationale**

A process is described for developing an access control list to assist agencies in the consistent development of access control lists for their systems.

**16.2.6.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD follow the process in the table below for developing an access control list.

| Stage | Description |
|---|---|
| **1** | Establish groups of all system resources based on similar security objectives. |
| **2** | Determine the information owner for each group of resources. |
| **3** | Obtain agreement from system owners. |
| **4** | Establish groups encompassing all system users based on similar functions or security objectives. |
| **5** | Determine the group owner or manager for each group of system users. |
| **6** | Determine the degree of access to the resource for each system user group. |
| **7** | Decide on the level of access for security administration, based on the internal security policy. |
| **8** | Identify any classification, protective markings and releasability indicators, (such as NZEO or compartmented information). |

# 16.3. Privileged Access

## Objective

16.3.1. Only trusted personnel are granted privileged access to systems.

## Context

### Scope

16.3.2. This section covers information relating specifically to personnel that are granted privileged access to systems.

### Privileged access

16.3.3. Within this section, privileged access is considered to be access which can give a system user:

- the ability to change key system configurations;
- the ability to change control parameters;
- access to audit and security monitoring information;
- the ability to circumvent security measures;
- access to all data, files and accounts used by other system users, including backups and media; or
- special access for troubleshooting the system.

## References

16.3.4. Additional information relating to privileged and system accounts, including monitoring, is contained in:

| Title | Publisher | Source |
|---|---|---|
| **ISO/IEC 27001:2013, A.11.2.2 Privilege Management** | ISO / IEC<br>Standards NZ | http://www.iso27001security.com/html/27001.html<br>http://www.standards.co.nz |
| **NZISM– Section 6.3 Change Management** | GCSB | NZISM –Section 6.3 Change Management |
| **Restricting administrative privileges** | ASD | http://www.asd.gov.au/publications/protect/Restricting_Admin_Privileges.pdf |
| **DNSSEC Practice Statement** | NZ Registry Services | http://www.nzrs.net.nz |

## Rationale & Controls

### 16.3.5. Use of privileged accounts

**16.3.5.R.01. Rationale**

Inappropriate use of any feature or facility of a system that enables a privileged user to override system or application controls can be a major contributory factor to failures, information security incidents, or system breaches.

**16.3.5.R.02. Rationale**

Privileged access rights allow for system wide changes to be made and as such an appropriate and effective mechanism to log privileged users and strong change management practices will provide greater accountability and auditing capability.

**16.3.5.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST:

- ensure strong change management practices are implemented;
- ensure that the use of privileged accounts is controlled and accountable;
- ensure that system administrators are assigned and consistently use, an individual account for the performance of their administration tasks;
- keep privileged accounts to a minimum; and
- allow the use of privileged accounts for administrative work only.

**16.3.5.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD:

- ensure strong change management practices are implemented;
- ensure that the use of privileged accounts is controlled and accountable;
- ensure that system administrators are assigned an individual account for the performance of their administration tasks;
- keep privileged accounts to a minimum; and
- allow the use of privileged accounts for administrative work only.

### 16.3.6. Privileged system access by foreign nationals

**16.3.6.R.01. Rationale**

As privileged users may have the ability to bypass controls on a system it is strongly encouraged that foreign nationals are not given privileged access to systems processing particularly sensitive information.

**16.3.6.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT allow foreign nationals, including seconded foreign nationals, to have privileged access to systems that process, store or communicate NZEO information.

**16.3.6.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT allow foreign nationals, including seconded foreign nationals, to have privileged access to systems that process, store or communicate classified information.

### 16.3.7. Security clearances for privileged users

**16.3.7.R.01. Rationale**

When frequent data transfers occur between systems of different classifications, having privileged users from the lesser system cleared to the classification of the higher system will assist in any actions that need to be taken resulting from any data spill.

**16.3.7.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies involved in frequent transfers of data from another system to their system with a lesser classification SHOULD clear at least one privileged user to the classification of the higher system.

# 16.4. Remote Access

## Objective

16.4.1. Remote access to systems is minimised, secure, controlled, authorised and authenticated.

## Context

### Scope

16.4.2. This section covers information relating to the methods used by personnel to access an agency system from a remote location.

### Remote access

16.4.3. Remote access is defined as user access to agency systems originating outside an agency network. It does not include web–based access to DMZ resources. Further information on working off–site can be found in Chapter 21 – Working Off-site. The requirements for using multi–factor authentication are described in the Identification and Authentication section of this chapter.

### Remote privileged access

16.4.4. Remote access by a privileged user to an agency system via a less trusted security domain (for example, the Internet) may present additional risks. Controls in this section are designed to prevent escalation of user privileges from a compromised remote access account.

16.4.5. Remote privileged access does **not** include privileged access across disparate physical sites that are within the same security domain or privileged access across remote sites that are connected via trusted infrastructure. Privileged access of this nature faces different threats to those discussed above. Ensuring robust processes and procedures are in place within an agency to monitor and detect the threat of a malicious insider are the most important measure for this scenario.

### Encryption

16.4.6. Cryptography is used to provide confidentiality and preserve integrity of data transmitted over networks where it may be intercepted or examined and is outside the control of the sender and recipient.

16.4.7. With the increases in speed and computing power and the cost reductions of modern computing, older cryptographic algorithms are increasingly vulnerable. It is vital that recommendations and controls in the NZISM are followed.

16.4.8. The use of approved cryptographic algorithms to encrypt authentication, session establishment and data for all remote access connections is considered good practice (See Chapter 17 - Cryptography and Chapter 21 - Working Off-Site).

## References

16.4.9. Further references can be found at:

| Title | Publisher | Source |
|---|---|---|
| **Virtual Private Network Capability Package Version 3.1 March 2015** | NSA | https://www.nsa.gov/resources/everyone/csfc/capability-packages/assets/files/vpn-cp.pdf |
| **NIST Special Publication 800-46 Revision 2**<br>**Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security** | NIST | http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf |
| **NIST Special Publication 800-114 Revision 1**<br>**User's Guide to Telework and Bring Your Own Device (BYOD) Security** | NIST | http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf |

## Rationale & Controls

### 16.4.10. Authentication

**16.4.10.R.01. Rationale**

Authenticating remote system users and devices ensures that only authorised system users and devices are allowed to connect to agency systems.

**16.4.10.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST authenticate each remote connection and user prior to permitting access to an agency system.

**16.4.10.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD authenticate both the remote system user and device during the authentication process.

### 16.4.11. Remote privileged access

**16.4.11.R.01. Rationale**

A compromise of remote access to a system can be limited by preventing the use of remote privileged access from an untrusted domain.

**16.4.11.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST NOT

Agencies MUST NOT allow the use of remote privileged access from an untrusted domain, including logging in as an unprivileged system user and then escalating privileges.

**16.4.11.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT allow the use of remote privileged access from an untrusted domain, including logging in as an unprivileged system user and then escalating privileges.

### 16.4.12. VPNs

**16.4.12.R.01. Rationale**

Virtual Private Networks (VPN's) use a tunnelling protocol to create a secure connection over an intermediate (public) network such as the internet. A VPN uses techniques such as encryption, authentication, authorisation and access control to achieve a secure connection. See Chapter 17 for details on cryptographic selection and implementation.

**16.4.12.R.02. Rationale**

A VPN can connect remote or mobile workers or remote locations to a private (agency) network.

**16.4.12.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD establish VPN connections for all remote access connections.

# 16.5. Event Logging and Auditing

## Objective

16.5.1. Information security related events are logged and audited for accountability, incident management, forensic and system monitoring purposes.

## Context

### Scope

16.5.2. This section covers information on the automatic logging of information relating to network activities. Information regarding manual logging of system management activities can be found in Section 16.3 - Privileged Access. See also Chapter7 - Information Security Incidents.

16.5.3. A security event is a change to normal or expected behaviour of a network, network component, system, device or user. Event logging helps improve the security posture of a system by increasing the accountability of all user actions, thereby improving the chances that malicious behaviour will be detected.

16.5.4. It is important that sufficient details are recorded in order for the logs to be useful when reviewed or when an investigation is in progress. Retention periods are also important to ensure sufficient log history is available. Conducting audits of event logs is an integral part of the security and maintenance of systems, since they will help detect and attribute any violations of information security policy, including cyber security incidents, breaches and intrusions.

## References

16.5.5. Additional information relating to event logging is contained in:

| Title | Publisher | Source |
|---|---|---|
| **ISO/IEC 27001:2013**<br>**Monitoring** | ISO / IEC<br>Standards NZ | http://www.iso27001security.com/html/27001.html<br>http://www.standards.co.nz |
| **Standard Time for a New Zealand Network** | Measurement Standards Laboratory | http://msl.irl.cri.nz/services/time-and-frequency/ntp-server-information |

## Rationale & Controls

### 16.5.6. Maintaining system management logs

**16.5.6.R.01. Rationale**

Having comprehensive information on the operations of a system can assist system administration, support information security and assist incident investigation and management. In some cases forensic investigations will rely on the integrity, continuity and coverage of system logs.

**16.5.6.R.02. Rationale**

It will be impractical and costly to store all system logs indefinitely. An agency retention policy may consider:

- Legislative and regulatory requirements;
- Ensure adequate retention for operational support and efficiency;
- Minimise costs and storage requirements; and
- An adequate historical archive is maintained.

Care should be taken to ensure that these considerations are properly balanced.

Some practices dictate retention periods, for example good DNSSEC practice requires log information is stored in log servers for 4 months, then archived and retained for at least 2 years.

**16.5.6.C.01. Control:** System Classification(s): TS; Compliance: MUST

Agencies MUST maintain system management logs for the life of a system.

**16.5.6.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD determine a policy for the retention of system management logs.

### 16.5.7. Content of system management logs

**16.5.7.R.01. Rationale**

Comprehensive system management logs will assist in logging key management activities conducted on systems.

**16.5.7.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

A system management log SHOULD record the following minimum information:

- all system start-up and shutdown;
- service, application, component or system failures;
- maintenance activities;
- backup and archival activities;
- system recovery activities; and
- special or out of hours activities.

### 16.5.8. Logging requirements

**16.5.8.R.01. Rationale**

Event logging can help raise the security posture of a system by increasing the accountability for all system user actions.

**16.5.8.R.02. Rationale**

Event logging can increase the chances that malicious behaviour will be detected by logging the actions of a malicious party.

**16.5.8.R.03. Rationale**

Well configured event logging allows for easier and more effective auditing and forensic examination if an information security incident occurs.

**16.5.8.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop and document logging requirements covering:

- the logging facility, including:
  - log server availability requirements; and
  - the reliable delivery of log information to the log server;
- the list of events associated with a system or software component to be logged; and
- event log protection and archival requirements.

### 16.5.9. Events to be logged

**16.5.9.R.01. Rationale**

The events to be logged are key elements in the monitoring of the security posture of systems and contributing to reviews, audits, investigations and incident management.

**16.5.9.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST log, at minimum, the following events for all software components:

- logons;
- failed logon attempts;
- logoffs;
- date and time;
- all privileged operations;
- failed attempts to elevate privileges;
- security related system alerts and failures;
- system user and group additions, deletions and modification to permissions; and
- unauthorised or failed access attempts to systems and files identified as critical to the agency.

### 16.5.10. Additional events to be logged

**16.5.10.R.01. Rationale**

The additional events to be logged can be useful for reviewing, auditing or investigating software components of systems.

**16.5.10.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD log the events listed in the table below for specific software components.

| Software component | Events to log |
|---|---|
| **Database** | System user access to the database. |
| | Attempted access that is denied. |
| | Changes to system user roles or database rights. |
| | Addition of new system users, especially privileged users. |
| | Modifications to the data. |
| | Modifications to the format or structure of the database. |
| **Network/operating system** | Successful and failed attempts to logon and logoff. |
| | Changes to system administrator and system user accounts. |
| | Failed attempts to access data and system resources. |
| | Attempts to use special privileges. |
| | Use of special privileges. |
| | System user or group management. |
| | Changes to the security policy. |
| | Service failures and restarts. |
| | System startup and shutdown. |
| | Changes to system configuration data. |
| | Access to sensitive data and processes. |
| | Data import/export operations. |
| **Web application** | System user access to the Web application. |
| | Attempted access that is denied. |
| | System user access to the Web documents. |
| | Search engine queries initiated by system users. |

**16.5.10.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD log, at minimum, the following events for all software components:

- user login;
- all privileged operations;
- failed attempts to elevate privileges;
- security related system alerts and failures;
- system user and group additions, deletions and modification to permissions; and
- unauthorised or failed access attempts to systems and files identified as critical to the agency.

### 16.5.11. Event log facility

**16.5.11.R.01. Rationale**

The act of logging events is not enough in itself. For each event logged, sufficient detail needs to be recorded in order for the logs to be useful when reviewed. An authoritative external time source, a local **Time Source Master Clock or server or** Co-ordinated Universal Time (UTC) is essential for the time-stamping of events and later inspection or forensic examination. The NZ Interoperability Framework (e-GIF) recognises the time standard for New Zealand as UTC (MSL), with Network Time Protocol (NTP) v.4 as the delivery method over the Internet.

**16.5.11.R.02. Rationale**

New Zealand standard time is maintained by the Measurement Standards Laboratory of New Zealand (MSL), a part of Industrial Research Limited (IRL). New Zealand standard time is based on UTC, a worldwide open standard used by all modern computer operating systems. UTC (MSL) is kept within 200 nanoseconds of the international atomic time scale maintained by the Bureau International des Poids et Mesures (BIPM) in Paris.

**16.5.11.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

For each event identified as needing to be logged, agencies MUST ensure that the log facility records at least the following details, where applicable:

- date and time of the event;
- relevant system user(s) or processes;
- event description;
- success or failure of the event;
- event source (e.g. application name); and
- IT equipment location/identification.

**16.5.11.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD establish an authoritative time source.

**16.5.11.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD synchronise all logging and audit trails with the time source to allow accurate time stamping of events.

### 16.5.12. Event log protection

**16.5.12.R.01. Rationale**

Effective log protection and storage (possibly involving the use of a dedicated event logging server) will help ensure the integrity and availability of the collected logs when they are audited.

**16.5.12.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Event logs MUST be protected from:

- modification and unauthorised access; and
- whole or partial loss within the defined retention period.

**16.5.12.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST configure systems to save event logs to separate secure servers as soon as possible after each event occurs.

**16.5.12.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that:

- systems are configured to save event logs to a separate secure log server; and
- event log data is archived in a manner that maintains its integrity.

### 16.5.13. Event log archives

**16.5.13.R.01. Rationale**

It is important that agencies determine the appropriate length of time to retain DNS, proxy, event systems and other operational logs. Logs are an important information source in reviews, audits and investigations ideally these should be retained for the life of the system or longer.

**16.5.13.R.02. Rationale**

The Archives, Culture, and Heritage Reform Act 2000, the Public Records Act 2005 and the Official Information Act 1982 may determine or influence the length of time that logs need to be retained and if they should be archived.

**16.5.13.C.01. Control**: System Classification(s): All Classifications; Compliance: MUST

Event logs MUST be archived and retained for an appropriate period as determined by the agency.

**16.5.13.C.02. Control**: System Classification(s): All Classifications; Compliance: MUST

Disposal or archiving of DNS, proxy, event, systems and other operational logs MUST be in accordance with the provisions of the relevant legislation.

**16.5.13.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD seek advice and determine if their logs are subject to legislation.

**16.5.13.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD retain DNS, proxy and event logs for at least 18 months.

### 16.5.14. Event log auditing

**16.5.14.R.01. Rationale**

Conducting audits of event logs is seen as an integral part of the maintenance of systems, as they will assist in the detection and attribution of any violations of agency security policy, including information security incidents, breaches and intrusions.

**16.5.14.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop and document event log audit requirements covering:

- the scope of audits;
- the audit schedule;
- action to be taken when violations are detected;
- reporting requirements; and
- roles and specific responsibilities.

# 17. Cryptography

## 17.1. Cryptographic Fundamentals

### Objective

17.1.1. Cryptographic products, algorithms and protocols are approved by the GCSB for suitability before being used and that cryptographic implementations by agencies are adequate for the protection of data and communications.

### Context

#### Scope

17.1.2. This section covers information on the fundamentals of cryptography including the use of encryption to protect data at rest and in transit. Detailed information on algorithms and protocols approved to protect classified information can be found in Section 17.2 - Approved Cryptographic Algorithms and Section 17.3 - Approved Cryptographic Protocols.

#### Purpose of cryptography

17.1.3. Encryption is primarily used to provide confidentiality protecting against the risk of information being exploited by an attacker. More broadly, cryptography can also provide authentication, non-repudiation and integrity. Cryptography is also used in the establishment of secure connectivity, such as IPSEC VPNs.

17.1.4. The use of approved encryption will generally reduce the likelihood of an unauthorised party gaining access to the information contained within the encrypted data.

17.1.5. Cryptography is an important control for data protection and the encryption selected will depend on the classification of the data. Note that classification, in itself, provides no protection but is merely indicative of the degree of protection and care in handling required for that level of classification.

17.1.6. Care needs to be taken with encryption systems that do not encrypt the entire media content to ensure that either all of the classified data is encrypted or that the media is handled in accordance with the highest classification of the unencrypted data.

17.1.7. With the increases in speed and computing power and the cost reductions of modern computing, older cryptographic algorithms are increasingly vulnerable. It is vital that recommendations and controls in the NZISM are followed.

#### Using encryption

17.1.8. Encryption of data at rest can be used to reduce the physical protection of storage and handling requirements of media or systems.

17.1.9. Encryption of data in transit can be used to provide protection for information being communicated over insecure mediums and hence reduce the security requirements of the communication process.

17.1.10. When agencies use encryption for data at rest or in transit, they are not reducing the classification of the information. When encryption is used the potential risk of disclosure of the information is reduced, and as such the protection requirements for a lower classification may be considered to be more appropriate to that information.

17.1.11. As the classification of the information does not change when encrypted, agencies cannot use lowered storage, physical transfer or security requirements as a baseline to further lower requirements with an additional cryptographic product.

17.1.12. In general terms, the level of assurance of specific encryption protocols and algorithms is defined in terms of Common Criteria, Protection Profiles or, in some cases, approved cryptographic evaluations. It is important to note that evaluations of cryptographic protocols and algorithms are NOT universally conducted when security products are evaluated, relying rather on previous approved evaluations of cryptographic protocols and algorithms.

**Risk Assessments**

17.1.13. Encryption algorithms create data transformations that are designed to be difficult to easily reverse by unauthorised users. Today's software will usually provide several algorithmic options, including some older algorithms provided for backward compatibility with older (legacy) systems. In many cases the older algorithms may be deprecated, are considered time-expired and are not fit for purpose in modern systems.

17.1.14. In all cases a comprehensive risk assessment should be undertaken before configurations are selected. Some general principles to be considered are:

- Long, complex passwords are stronger than short passwords;
- Long keys generally provide stronger encryption than short keys;
- Asymmetric encryption is slower than symmetric encryption;
- Symmetric encryption is generally recommended when the key is stored locally only;
- Asymmetric encryption is recommended when keys need to be shared across communication channels;
- If you are encrypting very large volumes of data, encrypting the data using a symmetric key, and encrypting the symmetric key with an asymmetric key may be more operationally effective;
- Normally encrypted data cannot be compressed, but compressed data can be encrypted. Data should be compressed before encryption.

17.1.15. It is important to note that the NZISM prescribes approved algorithms and protocols and users must select combinations from these lists.

### Transitioning Cryptographic Algorithms and Protocols

17.1.16. It is important to use algorithms that adequately protect sensitive information. It is also important to recognise that all cryptographic algorithms and protocols have a finite life. Challenges are posed by new cryptanalysis techniques and methods, the increasing power of classical computing technology, and the continuing work on the development of quantum computers. In addition, there is an active field of work that continuously seeks to compromise algorithms and protocols currently in use.

17.1.17. Planning for changes in the use of cryptography because of algorithm breaks, the availability of more powerful computing techniques or new technologies is an important consideration for agencies. Awareness of retirement or deprecation of algorithms and associated protocols is essential.

### Retiring RSA

17.1.18. RSA was announced in 1976 so it is now over 40 years old. Several flaws and attacks have been identified since creation, each of which required specific mitigations, careful implementation and management. Unfortunately there is ample evidence that implementers continue to have difficulties in securely implementing, using and managing RSA.

17.1.19. To counter identified threats from shorter RSA key lengths, longer key lengths have been specified in the NZISM since 2010. Subsequently it was specified in the NZISM that RSA was approved for use in legacy systems only.

17.1.20. This approach was selected to allow agencies to plan the retirement of legacy systems and ensure replacement systems were using only approved algorithms and protocols.

17.1.21. There are several indicators that RSA will be deprecated in the next few years. For example the TLS 1.3 Working Group has agreed to deprecate RSA in favour of elliptic curve cryptography. The most recent guidance from NIST is also indicative of impending deprecation of RSA.

17.1.22. It is, therefore essential that agencies are aware of these changes and plan the retirement of RSA from their systems as part of their ongoing operational management.

### Product specific cryptographic requirements

17.1.23. This section provides requirements for the use of cryptography to protect classified information. Requirements, additional to those in this Manual, can exist in consumer guides for products once they have completed an approved evaluation. Vendor specifications supplement this manual and where conflict in controls occurs the product specific requirements take precedence. Any policy or compliance conflicts are to be incorporated into the risk assessment.

### Exceptions for using cryptographic products

17.1.24. Where Agencies implement a product that uses an Approved Cryptographic Algorithm or Approved Cryptographic Protocol to provide protection of unclassified data at rest or in transit, that product does not require a separate, approved evaluation. Correct implementation of the cryptographic protocol is fundamental to the proper operation of the Approved Cryptographic Algorithm or Approved Cryptographic Protocol and is part of the checking conducted during system certification.

### Federal Information Processing Standard 140

17.1.25. The FIPS 140 is a United States standard for the validation of both hardware and software cryptographic modules.

17.1.26. FIPS 140 is in its second iteration and is formally referred to as FIPS 140-2. This section refers to the standard as FIPS 140 but applies to both FIPS 140-1 and FIPS 140-2. The third iteration, FIPS 140-3, has been released in draft and this section also applies to that iteration.

17.1.27. FIPS 140 is not a substitute for an approved evaluation of a product with cryptographic functionality. FIPS 140 is concerned solely with the cryptographic functionality of a module and does not consider any other security functionality.

17.1.28. Cryptographic evaluations of products will normally be conducted by an approved agency. Where a product's cryptographic functionality has been validated under FIPS 140, the GCSB can, at its discretion, and in consultation with the vendor, reduce the scope of a cryptographic evaluation.

17.1.29. The GCSB will review the FIPS 140 validation report to confirm compliance with New Zealand National Cryptographic Policy.

### New Zealand National Policy for High Grade Cryptographic Products, High Grade Cryptographic Equipment and Key Management

17.1.30. The New Zealand National Standard for High Grade Cryptographic Products (HGCP) & High Grade Cryptographic Equipment (HGCE) and related key management is contained in the New Zealand Communications Security Standard No. 300 – Control of COMSEC Material. This prescribes national doctrine for the control of COMSEC materials. Note this is a RESTRICTED document.

## References

17.1.31. Further references can be found at:

| Title | Publisher | Source |
|---|---|---|
| **New Zealand Communications Security Standard No. 300 – Control of COMSEC Material** | GCSB | Contact the GCSB<br>RESTRICTED document available on application to authorised personnel |
| **New Zealand Communications Security Standard No. 500 - Policy** | GCSB | Contact the GCSB<br>RESTRICTED document available on application to authorised personnel |
| **FIPS140-2** | NIST | http://www.csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf |
| **FIPS140-3 DRAFT** | NIST | http://www.csrc.nist.gov/publications/drafts/fips140-3/FIPS_140-3_sections_submitted_for_comments.pdf |
| **NIST Special Publication 800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths** | NIST | http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf |
| **NIST Special Publication 800-56B Revision 1 - Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, September 2014** | NIST | http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br1.pdf |
| **SP 800-57 Part 1, Recommendation for Key Management: Part 1: General (Revision4), Jan 2016** | NIST | http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4 |
| **SP 800-57 Part 2, Recommendation for Key Management: Part 2: Best Practices for Key Management Organization, Aug 2005** | NIST | http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf |
| **SP 800-57 Part 3, Recommendation for Key Management, Part 3 Application-Specific Key Management Guidance, Jan, 2015** | NIST | http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf |
| **FIPS PUB 186-4 Digital Signature Standard (DSS) July 2013** | NIST | http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf |
| **SP 800-131A Rev. 2 (DRAFT) Transitioning the Use of Cryptographic Algorithms and Key Lengths – July 2018** | NIST | https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/draft |
| **SP 800-56B Rev. 1 - Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography - September 2014** | NIST | https://csrc.nist.gov/publications/detail/sp/800-56b/rev-1/final |
| **Handling requirements for protectively marked information and equipment** | PSR | http://www.protectivesecurity.govt.nz |
| **Virtual Private Network Capability Package Version 3.1 March 2015** | NSA | https://www.nsa.gov/ia/_files/VPN_CP_3_1.pdf |

| Title | Publisher | Source |
|---|---|---|
| **Suite B Implementer's Guide to NIST SP 800-56A, July 28, 2009** | NSA | http://docplayer.net/204368-Suite-b-implementer-s-guide-to-nist-sp-800-56a-july-28-2009.html |
| **Guidelines on Cryptographic Algorithms Usage and Key Management - EPC342-08 Version 7.0 4 November 2017** | European Payments Council | https://www.europeanpaymentscouncil.eu/document-library/guidance-documents/guidelines-cryptographic-algorithms-usage-and-key-management |
| **Choose an Encryption Algorithm** | Microsoft | https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/choose-an-encryption-algorithm?view=sql-server-2017 |
| **Transport Layer Protection Cheat Sheet** | OWASP | https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet |
| **Guide to Cryptography** | OWASP | https://www.owasp.org/index.php/Guide_to_Cryptography |
| **New Directions in Cryptography - IEEE Transactions on Information Theory Vol IT22 November 1976** | Diffie, Hellman | https://ee.stanford.edu/~hellman/publications/24.pdf |
| **Transport Layer Security (tls)** | IETF | https://datatracker.ietf.org/wg/tls/documents/ |
| **TLS 1.3** | IETF | http://ietf.org/blog/tls13/ |
| **The Transport Layer Security (TLS) Protocol Version 1.3 March 2018** | IETF | https://tlswg.github.io/tls13-spec/draft-ietf-tls-tls13.html |

## Rationale & Controls

### 17.1.32. Using cryptographic products

**17.1.32.R.01. Rationale**

No real-world product can ever be guaranteed to be free of vulnerabilities. The best that can be done is to increase the level of assurance in a product to a point that represents satisfactory risk management.

**17.1.32.R.02. Rationale**

Refer to Chapter 12 – Product Security for a discussion on product evaluation and assurance.

**17.1.32.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies using cryptographic functionality within a product for the protection of classified information MUST ensure that the product has completed a cryptographic evaluation recognised by the GCSB.

### 17.1.33. Data recovery

**17.1.33.R.01. Rationale**

It is important for continuity and operational stability that cryptographic products provide a means of data recovery to allow for the recovery of data in circumstances such as where the encryption key is unavailable due to loss, damage or failure. This includes production, storage, backup and virtual systems. This is sometimes described as "key escrow".

**17.1.33.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Cryptographic products MUST provide a means of data recovery to allow for recovery of data in circumstances where the encryption key is unavailable due to loss, damage or failure.

**17.1.33.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Cryptographic products SHOULD provide a means of data recovery to allow for recovery of data in circumstances where the encryption key is unavailable due to loss, damage or failure.

### 17.1.34. Reducing storage and physical transfer requirements

**17.1.34.R.01. Rationale**

When encryption is applied to media or media residing within IT equipment it provides an additional layer of defence. Whilst such measures do not reduce or alter the classification of the information itself, physical storage, handling and transfer requirements may be reduced to those of a lesser classification for the media or equipment (but not the data itself).

**17.1.34.R.02. Rationale**

Approved Cryptographic Algorithms are discussed in section 17.2.

**17.1.34.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Encryption used to reduce storage or physical handling protection requirements MUST be an approved cryptographic algorithm in an EAL2 (or higher) encryption product.

**17.1.34.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST

If an agency wishes to reduce the storage or physical transfer requirements for IT equipment or media that contains classified information, they MUST encrypt the classified information using High Grade Cryptographic Equipment (HGCE). It is important to note that the classification of the information itself remains unchanged.

**17.1.34.C.03. Control:** System Classification(s): C, S, TS; Compliance: MUST

If an agency wishes to use encryption to reduce the storage, handling or physical transfer requirements for IT equipment or media that contains classified information, they MUST use:

- full disk encryption; or
- partial disk encryption where the access control will allow writing only to the encrypted partition holding the classified information.

**17.1.34.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD

If an agency wishes to use encryption to reduce the storage or physical transfer requirements for IT equipment or media that contains classified information, they SHOULD use:

- full disk encryption; or
- partial disk encryption where the access control will only allow writing to the encrypted partition holding the classified information.

### 17.1.35. Encrypting NZEO information at rest

**17.1.35.R.01. Rationale**

NZEO information is particularly sensitive and it requires additional protection in the form of encryption, when at rest. This includes production, storage, backup and virtual systems.

**17.1.35.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST use an Approved Cryptographic Algorithm to protect NZEO information when at rest on a system.

### 17.1.36. Information and Systems Protection

**17.1.36.R.01. Rationale**

When encryption is applied to information being communicated over networks, less assurance is required for the physical protection of the communications infrastructure. In some cases, no physical security can be applied to the communications infrastructure such as public infrastructure, the Internet or non-agency controlled infrastructure. In other cases no direct assurance can be obtained and reliance is placed on third party reviews and reporting. In such cases encryption of information is the only practical mechanism to provide sufficient assurance that the agency information systems are adequately protected.

**17.1.36.R.02. Rationale**

Data duplication for backups or data replication between data centres requires the same level of protection as other parts of the agency's infrastructure. This includes outsourced services.

**17.1.36.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST use HGCE if they wish to communicate or pass information over UNCLASSIFIED, insecure or unprotected networks.

**17.1.36.C.02. Control:** System Classification(s): **RESTRICTED/SENSITIVE**; Compliance: MUST

Information or systems classified RESTRICTED or SENSITIVE MUST be encrypted with an approved encryption algorithm and protocol if information is transmitted or systems are communicating over any insecure or unprotected network such as the Internet, public infrastructure or non-agency controlled networks.

**17.1.36.C.03. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST encrypt agency data using an approved algorithm and protocol when data is transmitted between data centres over insecure or unprotected networks such as the Internet, public infrastructure or non-agency controlled networks.

**17.1.36.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use an approved encryption product if they wish to communicate over insecure or unprotected networks such as the Internet, public networks or non-agency controlled networks.

### 17.1.37. IT equipment using Encryption

**17.1.37.R.01. Rationale**

In general terms, when IT equipment employing encryption functionality is turned on and authenticated all information becomes accessible to the system user. At such a time the IT equipment will need to be handled in accordance with the highest classification of information on the system. Special technology architectures and implementations exist where accessibility continues to be limited when first powered on. Agencies should consult the GCSB for further advice on special architectures and implementations.

**17.1.37.R.02. Rationale**

The classification of the equipment when powered off will depend on the equipment type, cryptographic algorithms and protocols used and whether cryptographic key has been removed. Agencies should consult the GCSB for further advice on treatment of specific software, systems and IT equipment.

**17.1.37.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

When IT equipment storing encrypted information is turned on and authenticated, it MUST be treated as per the original classification of the information.

**17.1.37.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agency MUST consult the GCSB for further advice on the powered off status and treatment of specific software, systems and IT equipment.

### 17.1.38. Encrypting NZEO information in transit

**17.1.38.R.01. Rationale**

NZEO information is particularly sensitive and requires additional protection. It must be encrypted when in transit.

**17.1.38.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

In addition to any encryption already in place for communication mediums, agencies MUST use an Approved Cryptographic Protocol and Algorithm to protect NZEO information when in transit.

### 17.1.39. Key Refresh and Retirement

#### 17.1.39.R.01. Rationale

All cryptographic keys have a limited useful life after which the key should be replaced or retired. Typically the useful life of the cryptographic key (cryptoperiod) is use, product and situation dependant. Product guidance is the best source of information on establishing cryptoperiods for individual products. A more practical control is the use of data, disk or volume encryption where key changes are more easily managed. Selection of cryptoperiods should be based on a risk assessment.

#### 17.1.39.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD establish cryptoperiods for all keys and cryptographic implementations in their systems and operations.

#### 17.1.39.C.02. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use risk assessment techniques and guidance to establish cryptoperiods.

#### 17.1.39.C.03. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST consult with the GCSB for the key management requirements for HGCE.

# 17.2. Approved Cryptographic Algorithms

## Objective

17.2.1. Information is protected by a properly implemented, Approved Cryptographic Algorithm.

## Context

### Scope

17.2.2. This section covers cryptographic algorithms that the GCSB recognises as being approved for use within government. Implementations of the algorithms in this section need to have successfully completed an approved cryptographic evaluation before they can be approved to protect information. Correct implementations of cryptographic protocols are checked during system certification.

17.2.3. High grade cryptographic algorithms are **not** covered in this section.

### Approved cryptographic algorithms

17.2.4. There is no guarantee or proof of security of an algorithm against presently unknown attacks. However, the algorithms listed in this section have been extensively scrutinised by government, industry and academic communities in a practical and theoretical setting and have not been found to be susceptible to any feasible attacks. There have been some cases where theoretically impressive vulnerabilities have been found, however these results are not considered to be feasible with current technologies and capabilities.

17.2.5. Where there is a range of possible key sizes for an algorithm, some of the smaller key sizes do not provide an adequate safety margin against attacks that might be found in the future. For example, future advances in number factorisation could render the use of smaller RSA moduli a security vulnerability.

17.2.6. The approved cryptographic algorithms fall into three categories: asymmetric/public key algorithms, hashing algorithms and symmetric encryption algorithms. Collectively these were known as SUITE B and were first promulgated in 2006.

17.2.7. Suite B was superseded by the Commercial National Security Algorithm Suite in August 2015 and later supplemented by the Commercial Solutions for Classified (CSFC) Programme.

17.2.8. The approved asymmetric/public key algorithms are:

- ECDH for agreeing on encryption session keys;
- ECDSA for digital signatures;
- DH for agreeing on encryption session keys for legacy systems only;
- DSA for digital signatures for legacy systems only;
- RSA for digital signatures and passing encryption session keys or similar keys for legacy systems only.

17.2.9. The approved hashing algorithms are:

- Secure Hashing Algorithm 2 (i.e. SHA-384 and SHA-512); and
- Secure Hashing Algorithm 1 (i.e. SHA-1) for legacy systems only.

17.2.10. The approved symmetric encryption algorithms are:

- AES using key lengths of 256 bits; and
- 3DES for legacy systems only.

17.2.11. SHA-1, 3DES, DH, DSA and RSA MUST NOT be used for new implementations but are approved only for current legacy systems already running these algorithms. It is important to note that the use of these older cryptographic algorithms has been deprecated in several countries including Australia and the US.

17.2.12. Summary Table

| Function | Cryptographic algorithm or protocol | Applicable standards | Minimum |
|---|---|---|---|
| **Encryption** | Advanced Encryption Standard (AES) | FIPS 197 | 256-bit key |
| **Hashing** | Secure Hash Algorithm (SHA) | FIPS 180-4 | SHA-384 |
| **Digital signature** | Elliptic Curve Digital Signature Algorithm (ECDSA) | FIPS 186-3<br>ANSI X9.62 | NIST P-384 |
| **Key exchange** | Elliptic Curve Diffie-Hellman (ECDH) | SP 800-56A<br>ANSI X9.63 | NIST P-384 |

**Salting**

17.2.13. Salting is a technique of further modifying a hash by adding a value or character string to the start or end of a password. This improves the resistance of the hash to brute force attacks. To further improve resistance the salt should be cryptographically strong and randomly generated as unique for each password.

17.2.14. The effectiveness of salts is reduced if implemented poorly. Common implementation errors are salts that are too short and the reuse of salts. To implement credential-specific salts the following principles should be followed:

- Generation of a unique salt when a stored credential is created;
- Generate salts as cryptographically strong random data;
- Use a 32 or 64 bit salt as storage and system constraints permit;
- Implement a security schema that is not dependent on hiding, splitting or otherwise obfuscating the salt; and
- Do NOT apply salts per user or on a system wide basis.

## References

17.2.15. The following references are provided for the approved asymmetric/public key algorithms, hashing algorithms and encryption algorithms. Note that Federal Information Processing Standards (FIPS) are standards and guidelines that are developed by the US National Institute of Standards and Technology (NIST) for US Federal computer systems.

| Topic | Publisher | Reference |
|---|---|---|
| **DH** | IEEE | W. Diffie and M. E. Hellman, 'New Directions in Cryptography', IEEE Transactions on Information Theory, vol. 22, is. 6, pp. 644-654, November 1976 |
| **RSA** | RSA Laboratories | Public Key Cryptography Standards #1 |
| **RFC 6944 Applicability Statement: DNS Security (DNSSEC) DNSKEY Algorithm Implementation Status** | Internet Engineering Task Force (IETF) | https://tools.ietf.org/pdf/rfc6944.pdf |
| **AES-CBC Algorithm** | IETF | See RFC 3602.<br>http://www.rfc-editor.org/rfc/rfc3602.txt |
| **AES in TLS** | IETF | See RFC 5288<br>http://www.rfc-editor.org/rfc/rfc5288.txt |
| **RFC 8492 Secure Password Ciphersuites for Transport Layer Security (TLS) FEB 2019** | IETF | https://tools.ietf.org/html/rfc8492 |
| **DSA**<br>**Digital Signature Algorithm** | NIST | FIPS 186-4 Digital Signature Standard (DSS)<br>http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf |
| **AES**<br>**Advanced Encryption Standard** | NIST | FIPS 197<br>http://www.nist.gov/customcf/get_pdf.cfm?pub_id=901427 |
| **NIST Special Publication 800-57 Part 1 Revision 4**<br>**Recommendation for Key Management - Part 1: General** | NIST | http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf |
| **NIST Special Publication 800-57**<br>**Recommendation for Key Management – Part 2: Best Practices for Key Management Organization** | NIST | http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p2.pdf |

| | | |
|---|---|---|
| **NIST Special Publication 800-57 Part 3 Revision 1**<br>**Recommendation for Key Management Part 3: Application-Specific Key Management Guidance** | NIST | http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf |
| **ECDH** | NIST | NIST Special Publication 800-56A (Revision 2), May 2013 - Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography<br>http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf<br>Also ANSI X9.63 and ANSI X9.42 |
| **SHA** | NIST<br><br>Standards Australia | FIPS PUB 180-4 - Secure Hash Standard (SHS)<br>http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf<br>Also Australian Standard AS 2805.13.3<br>http://infostore.saiglobal.com/store/ |
| **3DES** | NIST<br><br><br><br>ANSI<br>Standards Australia | NIST Special Publication 800-67 Revision 1 Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher<br>FIPS PUB 46-3 Data Encryption Standard (DES)(withdrawn)<br>ANSI X9.52-1998 Triple Data Encryption Algorithm Modes of Operation (withdrawn)<br>Also Australian Standard AS 2805.5.4<br>http://infostore.saiglobal.com/store/ |
| **Cryptography Management** | NIST | Recommendation for Key Derivation through Extraction then Expansion, September 2010.<br>http://csrc.nist.gov/publications/nistpubs/800-56C/SP-800-56C.pdf<br>FIPS 140-3 - Security Requirements for Cryptographic Modules. |
| **AES** | NIST | NIST Special Publication 800-38D – Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC |
| **AES** | NIST | The Galois/Counter Mode of Operation (GCM)<br>http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf |
| **AES** | NIST | NIST Advanced Encryption Standard Algorithm Validation List - http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html |
| **AES-CBC** | NIST | Cipher Block Chaining (CBC) see NIST Special Publication 800-38A, Recommendations for Block Cipher Modes of Operation – Methods and Techniques<br>http://csrc.nist.gov/publications/PubsSPs.html |
| **FIPS PUB 180-4, Secure Hash Standard, August 2015** | NIST | https://csrc.nist.gov/publications/detail/fips/180/4/final |

| | | |
|---|---|---|
| **RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0** | IETF | https://tools.ietf.org/pdf/rfc2898.pdf |
| **RFC 8018 PKCS #5: Password-Based Cryptography Specification Version 2.1** | IETF | https://tools.ietf.org/pdf/rfc8018.pdf |
| **NIST Special Publication 800-63-3 series - Digital Identity Guidelines** | NIST | https://pages.nist.gov/800-63-3/ |
| **NIST Special Publication 800-106 Randomized Hashing for Digital Signatures** | NIST | https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-106.pdf |
| **NIST Special Publication 800-107 Revision 1 Recommendation for Applications Using Approved Hash Algorithms** | NIST | https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-107r1.pdf |
| **NIST Special Publication 800-132 Recommendation for Password-Based Key Derivation Part 1: Storage Application** | NIST | https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf |
| **Commercial National Security Algorithm (CNSA) Suite, January 2016** | NSA | https://www.iad.gov/iad/programs/iad-initiatives/cnsa-suite.cfm |
| **Commercial National Security Algorithm (CNSA) Suite Factsheet** | NSA | https://www.iad.gov/iad/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/commercial-national-security-algorithm-suite-factsheet.cfm |
| **Commercial Solutions for Classified (CSfC) FAQ 2018** | NSA | https://www.nsa.gov/Portals/70/documents/resources/everyone/csfc/csfc-faqs.pdf |

## Rationale & Controls

### 17.2.16. Using Approved Cryptographic Algorithms

**17.2.16.R.01. Rationale**

Inappropriate configuration of a product using an Approved Cryptographic Algorithm can inadvertently select relatively weak implementations of the cryptographic algorithms. In combination with an assumed level of security confidence, this can represent a significant security risk.

**17.2.16.R.02. Rationale**

When configuring unevaluated products that implement an Approved Cryptographic Algorithm, agencies should disable any non-approved algorithms. A less effective control is to advise advising system users not to use them via a policy. Correct implementation of cryptographic protocols and disabling of unapproved algorithms is checked during system certification.

**17.2.16.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies using an unevaluated product that implements an Approved Cryptographic Algorithm MUST ensure that only Approved Cryptographic Algorithms can be used.

### 17.2.17. Approved asymmetric/public key algorithms

**17.2.17.R.01. Rationale**

Over the last decade DSA and DH cryptosystems have been subject to increasingly successful sub-exponential factorisation and index-calculus based attacks. ECDH and ECDSA offer more security per bit increase in key size than either DH or DSA and are considered more secure alternatives.

**17.2.17.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use ECDH and ECDSA for all new systems, version upgrades and major system modifications.

### 17.2.18. Using DH (Legacy systems ONLY)

**17.2.18.R.01. Rationale**

A modulus of at least 4096 bits for DH is now considered good practice by the cryptographic community.

**17.2.18.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies using DH, for the approved use of agreeing on encryption session keys, MUST use a modulus of at least 4096 bits.

### 17.2.19. Legacy Equipment using DH

**17.2.19.R.01. Rationale**

If a network device is NOT able to support the required cryptographic protocol, algorithm and key length, the system will be at risk of a cryptographic compromise. In such cases, the longest feasible key length must be implemented and the legacy device scheduled for replacement as a matter of urgency.

**17.2.19.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Legacy devices which are NOT capable of implementing required key lengths MUST be reconfigured with the longest feasible key length as a matter of urgency.

**17.2.19.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Legacy devices which are NOT capable of implementing required key lengths MUST be scheduled for replacement as a matter of urgency.

### 17.2.20. Using DSA (Legacy systems ONLY)

**17.2.20.R.01. Rationale**

A modulus of at least 1024 bits for DSA is considered good practice by the cryptographic community.

**17.2.20.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies using DSA, for the approved use of digital signatures, MUST use a modulus of at least 1024 bits.

### 17.2.21. Using ECDH

**17.2.21.R.01. Rationale**

A field/key size of at least 384 bits for ECDH is now considered good practice by the cryptographic community.

**17.2.21.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies using ECDH, for the approved use of agreeing on encryption session keys, MUST implement the curve P-384 (prime moduli).

**17.2.21.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

All VPN's using an ECDH key length less than 384 MUST replace all Pre-Shared Keys with keys of at least 384 bits, as soon as possible.

### 17.2.22. Using ECDSA

**17.2.22.R.01. Rationale**

A field/key size of at least 160 bits for ECDSA is considered good practice by the cryptographic community. Not all legacy systems support a modulus of this length, in which case significant risk is being carried.

**17.2.22.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies using ECDSA, for the approved use of digital signatures, MUST implement the curve P-384 (prime moduli).

### 17.2.23. Using RSA (Legacy systems ONLY)

**17.2.23.R.01. Rationale**

A modulus of at least 2048 bits for RSA is considered good practice by the cryptographic community.

**17.2.23.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies using RSA, for the approved use of digital signatures and passing encryption session keys or similar keys, MUST use a modulus of at least 2048 bits.

**17.2.23.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies using RSA, for the approved use of digital signatures and passing encryption session keys or similar keys, MUST ensure that the public keys used for passing encrypted session keys are different to the keys used for digital signatures.

### 17.2.24. Approved hashing algorithms

**17.2.24.R.01. Rationale**

Recent research conducted by cryptographic community suggests that SHA-1 may be susceptible to collision attacks. While no practical collision attacks have been published for SHA-1, they may become feasible in the near future.

**17.2.24.R.02. Rationale**

The use of SHA-1 is permitted ONLY in legacy systems where no other option exists.

**17.2.24.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST use the SHA-2 family before using SHA-1.

**17.2.24.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use a minimum of SHA-384.

### 17.2.25. Salts

**17.2.25.R.01. Rationale**

The use of salts strengthens the resistance of hash values to a variety of attacks, including brute force, rainbow table, dictionary and lookup table attacks.

**17.2.25.R.02. Rationale**

Key derivation functions use a password, a salt, then generate a password hash. Their purpose is to make password guessing by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive.

**17.2.25.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Memorised secrets such as passwords MUST be stored in a form that is resistant to offline attacks.

**17.2.25.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Memorised secrets such as passwords SHOULD be salted and hashed using a suitable one-way key derivation function.

**17.2.25.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

The salt SHOULD be at least 32 bits in length; be chosen arbitrarily; and each instance should be unique, so as to minimise salt value collisions among stored hashes.

### 17.2.26. Approved symmetric encryption algorithms

**17.2.26.R.01. Rationale**

The use of Electronic Code Book (ECB) mode in block ciphers allows repeated patterns in plaintext to appear as repeated patterns in the ciphertext. Most cleartext, including written language and formatted files, contains significant repeated patterns. An attacker can use this to deduce possible meanings of ciphertext by comparison with previously intercepted data. In other cases they might be able to determine information about the key by inferring certain contents of the cleartext. The use of other modes such as Cipher Block Chaining, Cipher Feedback, Output Feedback or Counter prevents such attacks.

**17.2.26.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies using AES or 3DES SHOULD NOT use Electronic Code Book (ECB) mode.

### 17.2.27. Using 3DES (Legacy systems ONLY)

**17.2.27.R.01. Rationale**

Using three distinct keys is the most secure option, while using two distinct keys in the order key 1, key 2, key 1 is also deemed secure for practical purposes. All other keying options are equivalent to single DES, which is not deemed secure for practical purposes.

**17.2.27.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

3DES MUST use either two distinct keys in the order key 1, key 2, key 1 or three distinct keys.

### 17.2.28. Using the Advanced Encryption Standard

**17.2.28.R.01. Rationale**

AES can operate in several modes. The Galois/Counter Mode (GCM) is the preferred AES mode, selected for its efficiency and performance.

**17.2.28.R.02. Rationale**

Galois/Counter Mode (GCM) is a block cipher mode of operation that uses universal hashing over a binary Galois field to provide authenticated encryption. It can be implemented in hardware to achieve high speeds with low cost and low latency. Software implementations of GCM can achieve excellent performance by using table-driven field operations. It uses mechanisms that are supported by a well-understood theoretical foundation with security is based on the security of the block cipher.

**17.2.28.R.03. Rationale**

The two functions that comprise AES/GCM are described as authenticated encryption and authenticated decryption. The authenticated encryption function encrypts the data and computes an authentication tag. The authenticated decryption function decrypts the data, contingent on the verification of the tag.

**17.2.28.R.04. Rationale**

Implementation of AES may restrict the data to be encrypted to the non-confidential data. This variant of GCM is called GMAC. For GMAC, the authenticated encryption and decryption functions become the functions for generating and verifying an authentication tag on the non-confidential data.

**17.2.28.R.05. Rationale**

Refer to NIST Special Publication 800-38D – Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC for detailed application independent information. RFC 4106 and RFC 6379 describe the use of GCM in IPsec Encapsulating Security Payload (ESP). RFC 5288 describes the use of GCM in Transport Layer Security (TLS).

#### 17.2.28.R.06. Rationale

The Cipher Block Chaining (CBC) mode is approved for use in IKEv2. NIST Special Publication 800-38A - *Recommendations for Block Cipher Modes of Operation – Methods and Techniques*, contains an application independent description of CBC. The AES-CBC cipher algorithm standard is defined in RFC 3602.

#### 17.2.28.R.07. Rationale

Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP) mode and Galois/Counter Mode Protocol (GCMP) are both approved for use in Wireless LAN Access Systems implementing the IEEE 802.11ac standard.

#### 17.2.28.C.01. Control: System Classification(s): All Classifications; Compliance: SHOULD

AES implementations for symmetric encryption of data SHOULD use the Galois/Counter Mode (GCM).

# 17.3. Approved Cryptographic Protocols

## Objective

17.3.1. Classified information in transit is protected by an Approved Cryptographic Protocol implementing an Approved Cryptographic Algorithm.

## Context

### Scope

17.3.2. This section covers information on the cryptographic protocols that the GCSB recognises as being approved for use within government. Implementations of the protocols in this section need to have successfully completed a GCSB recognised cryptographic evaluation before they can be approved for implementation.

17.3.3. High grade cryptographic protocols are **not** covered in this section.

### Approved cryptographic protocols

17.3.4. In general, the GCSB only recognises the use of cryptographic products that have passed a formal evaluation. However, the GCSB may approve the use of some commonly available cryptographic protocols even though their implementations within specific products have not been formally evaluated. This approval is limited to cases where they are used in accordance with the requirements in this manual.

17.3.5. The Approved Cryptographic Protocols are:

- TLS;
- SSH;
- S/MIME;
- OpenPGP Message Format; and
- IPSec.

## Rationale & Controls

### 17.3.6. Using Approved Cryptographic Protocols

**17.3.6.R.01. Rationale**

If a product implementing an Approved Cryptographic Protocol has been inappropriately configured, it is possible that relatively weak cryptographic algorithms or implementations could be inadvertently selected. In combination with an assumed level of security confidence, this can represent a significant level of security risk.

**17.3.6.R.02. Rationale**

When configuring unevaluated products that implement an Approved Cryptographic Protocol, agencies can ensure that only the Approved Cryptographic Algorithm can be used by disabling the unapproved algorithms within the products (which is preferred). Alternatively a policy can be put in place to advise system users not to use the non-approved algorithms.

**17.3.6.R.03. Rationale**

While many Approved Cryptographic Protocols support authentication, agencies should be aware that these authentication mechanisms are not foolproof. To be effective, these mechanisms MUST be securely implemented and protected.

This can be achieved by:

- providing an assurance of private key protection;
- ensuring the correct management of certificate authentication processes including certificate revocation checking; and
- using a legitimate identity registration scheme.

**17.3.8.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies using a product that implements an Approved Cryptographic Protocol MUST ensure that only Approved Cryptographic Protocols can be used.

# 17.4. Transport Layer Security

## Objective

17.4.1. Transport Layer Security is implemented correctly as an approved protocol.

## Context

### Scope

17.4.2. This section covers the conditions under which TLS can be used as an approved cryptographic protocol. Additionally, as File Transfer Protocol over SSL is built on SSL/TLS, it is also considered within the scope of this section.

17.4.3. When using a product that implements TLS, requirements for using approved cryptographic protocols will also need to be referenced in the Section 17.3 - Approved Cryptographic Protocols.

17.4.4. Further information on handling TLS traffic through gateways can be found in Section 14.3 - Web Applications.

### Background

17.4.5. **Transport Layer Security** (**TLS**) and Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communication security when using the Internet. They use X.509 certificates and asymmetric cryptography for authentication purposes. This generates a session key. This session key is then used to encrypt data between the parties.

17.4.6. Encryption with the session key provides data and message confidentiality, and message authentication codes for message integrity.

17.4.7. Several versions of the TLS and SSL protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging, and voice-over-IP (VoIP).

17.4.8. Although common usage has been to use the terms TLS and SSL interchangeably, they are distinct protocols.

17.4.9. TLS is an Internet Engineering Task Force (IETF) protocol, first defined in 1999, updated in RFC 5246 (August 2008) and RFC 6176 (March 2011). It is based on the earlier SSL specifications (1994, 1995, 1996) developed by Netscape Communications for adding the HTTPS protocol to their Navigator web browser. A draft of TLS 1.3 was released in October 2014.

17.4.10. Microsoft announced in October 2014 that that it will disable Secure Sockets Layer (SSL) 3.0 support in its Internet Explorer browser and in its Online Services, from Dec. 1, 2014.

### SSL 3.0 Vulnerability

17.4.11. A design vulnerability was found in the way SSL 3.0 handles block cipher mode padding. The Padding Oracle On Downgraded Legacy Encryption (POODLE) attack demonstrates how an attacker can exploit this vulnerability to decrypt and extract information from an encrypted transaction.

17.4.12. The POODLE attack demonstrates this vulnerability using web browsers and web servers, which is one of the most likely exploitation scenarios. All systems and applications utilizing the Secure Socket Layer (SSL) 3.0 with cipher-block chaining (CBC) mode ciphers may be vulnerable.

### SSL Superseded

17.4.13. SSL is now superseded by TLS, with the latest version being TLS 1.2 which was released in August 2008. The largely because of security flaws in the older SSL protocols.

17.4.14. Accordingly SSL is no longer an approved cryptographic protocol and it SHOULD be replaced by TLS.

## References

17.4.15. Further information on TLS and SSL can be found at:

| Title | Publisher | Source |
|---|---|---|
| **The SSL 3.0 specification** | IETF | https://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00 |
| **The TLS 1.2 specification** | IETF | http://tools.ietf.org/html/rfc5246 |
| **The SSL 2.0 prohibition** | IETF | http://tools.ietf.org/html/rfc6176 |
| **The Transport Layer Security (TLS) Protocol Version 1.3**<br>**draft-ietf-tls-tls13-03**<br>**October 2014** | IETF | http://datatracker.ietf.org/doc/draft-ietf-tls-tls13/ |
| **Vulnerability Summary for CVE-2014-3566** | NIST | http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566 |
| **Alert (TA14-290A) - SSL 3.0 Protocol Vulnerability and POODLE Attack** | US-CERT | https://www.us-cert.gov/ncas/alerts/TA14-290A |
| **This POODLE Bites: Exploiting The SSL 3.0 Fallback** | Google<br>September 2014 | http://www.openssl.org/~bodo/ssl-poodle.pdf |

## Rationale & Controls

### 17.4.16. Using TLS

**17.4.16.R.01. Rationale**

Whilst version 1.0 of SSL was never released, version 2.0 had significant security flaws leading to the development of SSL 3.0. SSL has since been superseded by TLS with the latest version being TLS 1.2 which was released in August 2008. SSL is no longer an approved cryptographic protocol.

**17.4.16.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use the current version of TLS (version 1.2).

**17.4.16.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT use any version of SSL.

# 17.5.Secure Shell

## Objective

17.5.1. Secure Shell (SSH) is implemented correctly as an Approved Cryptographic Protocol.

## Context

### Scope

17.5.2. SSH is software based on the Secure Shell protocol and enables a connection to a remote system.

17.5.3. This section covers information on the conditions under which commercial and open-source implementations of SSH can be used as an approved cryptographic protocol. Additionally, secure copy and Secure File Transfer Protocol use SSH and are therefore also covered by this section.

17.5.4. When using a product that implements SSH, requirements for using approved cryptographic protocols will also need to be referenced from the Section 17. 3 - Approved Cryptographic Protocols.

## References

17.5.5. Further references can be found at:

| Title | Publisher | Source |
|---|---|---|
| **Further information on SSH can be found in the SSH specification** | IETF | http://tools.ietf.org/html/rfc4252 |
| **Further information on Open SSH** | Open SSH | http://www.openssh.org |
| **OpenSSH 7.3** | Open SSH | http://www.openssh.com/txt/release-7.3 |

## Rationale & Controls

### 17.5.6. Using SSH

#### 17.5.6.R.01. Rationale

The configuration directives provided are based on the OpenSSH implementation of SSH. Agencies implementing SSH will need to adapt these settings to suit other SSH implementations.

#### 17.5.6.R.02. Rationale

SSH version 1 is known to have vulnerabilities. In particular, it is susceptible to a man-in-the-middle attack, where an attacker who can intercept the protocol in each direction can make each node believe they are talking to the other. SSH version 2 does not have this vulnerability.

#### 17.5.6.R.03. Rationale

SSH has the ability to forward connections and access privileges in a variety of ways. This means that an attacker who can exploit any of these features can gain unauthorised access to a potentially large amount of classified information.

#### 17.5.6.R.04. Rationale

Host-based authentication requires no credentials (password, public key etc.) to authenticate although in some cases a host key can be used. This renders SSH vulnerable to an IP spoofing attack.

#### 17.5.6.R.05. Rationale

An attacker who gains access to a system with system administrator privileges will have the ability to not only access classified information but to control that system completely. Given the clearly more serious consequences of this, system administrator login or administrator privilege escalation SHOULD NOT be permitted.

**17.5.6.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

The table below outlines the settings that SHOULD be implemented when using SSH.

| Configuration description | Configuration directive |
|---|---|
| **Disallow the use of SSH version 1** | Protocol 2 |
| **On machines with multiple interfaces, configure the SSH daemon to listen only on the required interfaces** | ListenAddress xxx.xxx.xxx.xxx |
| **Disable connection forwarding** | AllowTCPForwarding no |
| **Disable gateway ports** | Gatewayports no |
| **Disable the ability to login directly as root** | PermitRootLogin no |
| **Disable host-based authentication** | HostbasedAuthentication no |
| **Disable rhosts-based authentication** | RhostsAuthentication no |
| | IgnoreRhosts yes |
| **Do not allow empty passwords** | PermitEmptyPasswords no |
| **Configure a suitable login banner** | Banner/directory/filename |
| **Configure a login authentication timeout of no more than 60 seconds** | LoginGraceTime xx |
| **Disable X forwarding** | X11Forwarding no |

### 17.5.7. Authentication mechanisms

**17.5.7.R.01. Rationale**

Public key-based systems have greater potential for strong authentication, put simply, people are not able to remember particularly strong passwords. Password-based authentication schemes are also more susceptible to interception than public key-based authentication schemes.

**17.5.7.R.02. Rationale**

Passwords are more susceptible to guessing attacks, so if passwords are used in a system then countermeasures should be put into place to reduce the chance of a successful brute force attack.

**17.5.7.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use public key-based authentication before using password-based authentication.

**17.5.7.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies that allow password authentication SHOULD use techniques to block brute force attacks against the password.

### 17.5.8. Automated remote access

**17.5.8.R.01. Rationale**

If password-less authentication is enabled, allowing access from unknown IP addresses would allow untrusted parties to automatically authenticate to systems without needing to know the password.

**17.5.8.R.02. Rationale**

If port forwarding is not disabled or it is not configured securely, an attacker may be able to gain access to forwarded ports and thereby create a communication channel between the attacker and the host.

**17.5.8.R.03. Rationale**

If agent credential forwarding is enabled, an intruder could connect to the stored authentication credentials and then use them to connect to other trusted hosts or even intranet hosts, if port forwarding has been allowed as well.

**17.5.8.R.04. Rationale**

X11 is a computer software system and network protocol that provides a graphical user interface for networked computers. Failing to disable X11 display remoting could result in an attacker being able to gain control of the computer displays as well as keyboard and mouse control functions.

**17.5.8.R.05. Rationale**

Allowing console access permits every user who logs into the console to run programs that are normally restricted to the root user.

**17.5.8.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use parameter checking when using the 'forced command' option.

**17.5.8.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies that use logins without a password for automated purposes SHOULD disable:

- access from IP addresses that do not need access;
- port forwarding;
- agent credential forwarding;
- X11 display remoting; and
- console access.

**17.5.8.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies that use remote access without the use of a password SHOULD use the 'forced command' option to specify what command is executed.

### 17.5.9. SSH-agent

**17.5.9.R.01. Rationale**

SSH-agent or other similar key caching programs hold and manage private keys stored on workstations and respond to requests from remote systems to verify these keys. When an SSH-agent launches, it will request the user's password. This password is used to unlock the user's private key. Subsequent access to remote systems is performed by the agent and does not require the user to re-enter their password. Screenlocks and expiring key caches ensure that the user's private key is not left unlocked for long periods of time.

**17.5.9.R.02. Rationale**

Agent credential forwarding is required when multiple SSH connections are chained to allow each system in the chain to authenticate the user.

**17.5.9.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies that use SSH-agent or other similar key caching programs SHOULD:

- only use the software on workstation and servers with screenlocks;
- ensure that the key cache expires within four hours of inactivity; and
- ensure that agent credential forwarding is used when multiple SSH traversal is needed.

### 17.5.10. SSH-Versions

**17.5.10.R.01. Rationale**

Older versions contain known vulnerabilities which are regularly addressed or corrected by newer versions.

**17.5.10.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that the latest implementation of SSH software is being used. Older versions contain known vulnerabilities.

# 17.6.Secure Multipurpose Internet Mail Extension

## Objective

17.6.1. Secure Multipurpose Internal Mail Extension (S/MIME) is implemented correctly as an approved cryptographic protocol.

## Context

### Scope

17.6.2. This section covers information on the conditions under which S/MIME can be used as an approved cryptographic protocol.

17.6.3. When using a product that implements S/MIME, requirements for using approved cryptographic protocols will also need to be referenced from Section 17.3 - Approved Cryptographic Protocols.

17.6.4. Information relating to the development of password selection policies and password requirements can be found in Section 16.1 - Identification and Authentication.

## References

17.6.5. Further information on S/MIME can be found at:

| Title | Publisher | Source |
|---|---|---|
| **Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification** | IETF | https://tools.ietf.org/html/rfc5751<br><br>https://datatracker.ietf.org/wg/smime |
| **NIST SP800-57, Recommendations for Key Management** | NIST | http://csrc.nist.gov/publications/PubsSPs.html |

## Rationale & Controls

### 17.6.6. Decommissioning

**17.6.6.R.01. Rationale**

Decommissioning MUST ensure any remanent cryptographic data is destroyed or unrecoverable.

**17.6.6.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Decommissioning of faulty or redundant equipment MUST comply with media sanitisation requirements described in Chapter 12 – Product Security.

### 17.6.7. Using S/MIME

**17.6.7.R.01. Rationale**

S/MIME 2.0 used weaker cryptography (40-bit keys) than is approved for use by the government. Version 3.0 was the first version to become an Internet Engineering Taskforce (IETF) standard.

**17.6.7.R.02. Rationale**

Agencies choosing to implement S/MIME should be aware of the inability of many content filters to inspect encrypted messages and any attachments for inappropriate content, and for server-based antivirus software to scan for viruses and other malicious code.

**17.6.7.R.03. Rationale**

Improper decommissioning and sanitisation presents opportunities for harvesting Private Keys. Products that hosted multiple Private Keys for the management of multiple identities should be considered points of aggregation with an increased "target value". Where cloud based computing services have been employed, media sanitisation may be problematic and require the revocation and re-issue of new keys.

**17.6.7.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT allow versions of S/MIME earlier than 3.0 to be used.

# 17.7. OpenPGP Message Format

## Objective

17.7.1. OpenPGP Message Format is implemented correctly as an Approved Cryptographic Protocol.

## Context

### Scope

17.7.2. This section covers information on the conditions under which the OpenPGP Message Format can be used as an approved cryptographic protocol. It applies to the protocol as specified in IETF's RFC 2440 and RFC 4880, which supercedes RFC 2440.

17.7.3. When using a product that implements the OpenPGP Message Format, requirements for using approved cryptographic protocols will also need to be referenced from the Section 17.3 - Approved Cryptographic Protocols.

17.7.4. Information relating to the development of password selection policies and password requirements can be found in the Section 16.1 - Identification and Authentication.

## References

17.7.5. Further information on the OpenPGP Message Format can be found at:

| Title | Publisher | Source |
|---|---|---|
| **OpenPGP Message Format specification** | IETF | http://tools.ietf.org/html/rfc4880 |

## Rationale & Controls

### 17.7.6. Using OpenPGP Message Format

**17.7.6.R.01. Rationale**

If the private certificate and associated key used for encrypting messages is suspected of being compromised i.e. stolen, lost or transmitted over the Internet, then no assurance can be placed in the integrity of subsequent messages that are signed by that private key. Likewise no assurance can be placed in the confidentiality of a message encrypted using the public key as third parties could intercept the message and decrypt it using the private key.

**17.7.6.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST immediately revoke key pairs when a private certificate is suspected of being compromised or leaves the control of the agency.

# 17.8. Internet Protocol Security (IPSec)

## Objective

17.8.1. Internet Protocol Security (IPSec) is correctly implemented.

## Context

### Scope

17.8.2. This section covers information on the conditions under which IPSec can be used as an Approved Cryptographic Protocol.

17.8.3. When using a product that implements IPSec, requirements for using approved cryptographic protocols will also need to be referenced from Section 17.3 Approved Cryptographic Protocols.

### Modes of operation

17.8.4. IPSec can be operated in two modes: transport mode or tunnel mode.

### Cryptographic algorithms

17.8.5. Most IPSec implementations can accommodate a number of cryptographic algorithms for encrypting data when the Encapsulating Security Payload (ESP) protocol is used. These include 3DES and AES.

### Key exchange

17.8.6. Most IPSec implementations facilitate a number of methods for sharing keying material used in hashing and encryption processes. Two common methods are manual keying and IKE using the ISAKMP. Both methods are considered suitable for use.

### ISAKMP authentication

17.8.7. Most IPSec implementations can select from a number of methods for authentication as part of ISAKMP. These can include digital certificates, encrypted nonces or pre-shared keys. All these methods are considered suitable for use.

### ISAKMP modes

17.8.8. ISAKMP uses two modes to exchange information as part of IKE. These are main mode and aggressive mode.

## References

17.8.9. Further information on IPSec can be found at:

| Title | Publisher | Source |
|---|---|---|
| **Security Architecture for the IP overview** | IETF | http://tools.ietf.org/html/rfc2401 |

## Rationale & Controls

### 17.8.10. Mode of operation

**17.8.10.R.01. Rationale**

The tunnel mode of operation provides full encapsulation of IP packets whilst the transport mode of operation only encapsulates the payload of the IP packet.

**17.8.10.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use tunnel mode for IPSec connections.

**17.8.10.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies choosing to use transport mode SHOULD additionally use an IP tunnel for IPSec connections.

### 17.8.11. Protocol

**17.8.11.R.01. Rationale**

In order to provide a secure VPN style connection both authentication and encryption are needed. ESP is the only way of providing encryption yet Authentication Header (AH) and ESP can provide authentication for the entire IP packet and the payload respectively. ESP is generally preferred for authentication though as AH has inherent network address translation limitations.

**17.8.11.R.02. Rationale**

If however, maximum security is desired at the expense of network address translation functionality, then ESP can be wrapped inside of AH which will then authenticate the entire IP packet and not just the encrypted payload.

**17.8.11.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use the ESP protocol for IPSec connections.

### 17.8.12. ISAKMP modes

**17.8.12.R.01. Rationale**

Using main mode instead of aggressive mode provides greater security since all exchanges are protected.

**17.8.12.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies using ISAKMP SHOULD disable aggressive mode for IKE.

### 17.8.13. Security association lifetimes

**17.8.13.R.01. Rationale**

Using a secure association lifetime of four hours or 14400 seconds provides a balance between security and usability.

**17.8.13.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use a security association lifetime of four hours or 14400 seconds, or less.

### 17.8.14. HMAC algorithms

**17.8.14.R.01. Rationale**

MD5 and SHA-1 are no longer approved Cryptographic Protocols. The approved algorithms that can be used with HMAC are HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512.

**17.8.14.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use HMAC-SHA256, HMAC-SHA384 or HMAC-SHA512 as the HMAC algorithm.

### 17.8.15. DH groups

**17.8.15.R.01. Rationale**

Using a larger DH group provides more entropy for the key exchange.

**17.8.15.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use the largest modulus size available for the DH exchange.

### 17.8.16. Perfect Forward Secrecy

**17.8.16.R.01. Rationale**

Using Perfect Forward Secrecy reduces the impact of the compromise of a security association.

**17.8.16.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use Perfect Forward Secrecy for IPSec connections.

### 17.8.17. IKE Extended Authentication

**17.8.17.R.01. Rationale**

XAUTH using IKEv1 has documented vulnerabilities associated with its use.

**17.8.17.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD disable the use of XAUTH for IPSec connections using IKEv1.

## 17.9. Key Management

## Objective

17.9.1. Cryptographic keying material is protected by key management procedures.

## Context

### Scope

17.9.2. This section covers information relating to the general management of cryptographic system material. Because there is a wide variety of cryptographic systems and technologies available, and there are varied security risks for each, detailed key management guidance is not provided in this manual.

17.9.3. If HGCP or HGCE is being used, agencies are advised to consult the respective NZCSI national standards for the respective equipment.

17.9.4. In a cloud environment it is possible to outsource the control of cryptographic key to the cloud service provider, Hold Your Own Keys (HYOK) and Bring Your Own Keys (BYOK). It is important to note that there is little distinction between HYOK and BYOK.

17.9.5. Hold Your Own Keys (HYOK) generally refers to the management of keys by the agency or organisation where keys may be generated by the agency or by a third party such as a National Authority or a Certificate Authority. The agency retains full control of the management of the keys.

17.9.6. Bring Your Own Keys (BYOK) also refers to the management of keys by the agency or organisation. In this case keys are provided to cloud service (or other service) providers for use on outsourced services related to that agency. In such cases, the agency relinquishes some elements of control of the use, storage and protection of the keys.

### Applicability for cryptographic systems

17.9.7. In general, the requirements specified in this manual for systems apply equally to cryptographic systems. Where the requirements for cryptographic systems are different, the variations are contained in this section, and take precedence over requirements specified elsewhere in this manual.

**Background**

17.9.8. Encryption is an unparalleled technology for the protection of information but it relies on the strength of the algorithm, the strength of the key and, most importantly, strong key management.

17.9.9. All encryption has four important characteristics:

- The data to be protected;
- The algorithm used to encrypt the data;
- The protocol used to apply the algorithm; and
- The encryption key.

17.9.10. In almost all cases the algorithm is in the public domain and is not a secret. When an encryption algorithm is publically available, security rests entirely on the secrecy of the encryption key. It is also true that the effectiveness of most encryption systems depends on the secrecy of the encryption key. Approved Cryptographic Algorithms are described in Section 17.2. and Approved Cryptographic Protocols (applying the algorithms) are described in Section 17.3. These sections also specify key strengths to resist attempts to compromise the key through cryptanalysis.

17.9.11. While any algorithm can, theoretically, be broken through cryptanalysis, this may require the use of vast computing power and other resources, making this approach infeasible. If, however, the encryption key is compromised, there is no need to attack the algorithm itself. Attacks on encryption systems will always target the weakest point, the protection of the key. Attempts to compromise keys and key management are more likely and more efficient than attacks on the algorithm itself. This is why strong key management is vital in order to protect the encryption key and keep the key secure and secret. When key management fails, cryptographic security is compromised.

17.9.12. In today's Internet-connected world, almost all Internet security protocols use cryptography for authentication, integrity, confidentiality and non-repudiation. It is vital that good key management is implemented if these security protocols are to be protected, considered reliable and provide required levels of assurance to organisations and users.

17.9.13. In some cases, trusted third-party key management service providers furnish assistance to agencies in the generation, storage, operation, management and retirement (disposal) of keys associated with the agency.

**Key Management**

17.9.14. For encryption to be used effectively, the encryption keys must be managed with the same care and security as the data encrypted by those keys for the entire lifetime of those keys.

17.9.15. Key Management encompasses the operations and tasks necessary to create, protect and control the use of cryptographic keys. The process from creation to destruction of the encryption key is described as the key management life cycle.

**Key Management Life Cycle**

17.9.16. The key management lifecycle covers:

- Key generation;
- Key registration;
- Secure key storage;
- Key distribution and installation;
- Key use;
- Key rotation;
- Key backup (operational, backup and archive);
- Key replacement and reissue;
- Key recovery;
- Key revocation;
- Key suspension;
- Key retirement; and
- Key destruction.

**Open Networks**

17.9.17. Open networks, by definition, seek to establish arbitrary connections without there necessarily being a pre-existing relationship. Protocols have been developed to manage this requirement through key exchange protocols and through trusted agents., most often a National Authority or a Certificate Authority. Again it is important that approved protocols and algorithms, as specified in this document, are used. Refer to Sections 17,2 Approved Cryptographic Algorithms and 17.3 Approved Cryptographic Protocols.

**Public Key Infrastructure**

17.9.18. Public Key Infrastructure was first publically discussed in the early 1970's with some of the first PKI standards from the IETF published in the 1990's. PKI is the system to create, issue, manage and revoke digital certificates and their associated cryptographic keys. PKI has many different applications but typically used primarily for encrypting and digitally signing data in order to authenticate and protect data in transmission, supporting confidentiality and privacy. It is used extensively in ecommerce, internet banking and secure email as well as being a key element in protecting website traffic.

**Risks**

17.9.19. There are a number of specific risks related to the management of cryptographic keys. These include:

- Keys exposed to unauthorised persons or applications, potentially compromising the keys or data the encryption is protecting;
- Data breaches;
- Lost or unrecoverable cryptographic keys;
- Software based key management, which provides only limited protection;
- Fragmented key management as new systems are introduced; and
- Poorly documented and understood key management processes and activities increasing the possibility of compromise and potentially increasing compliance costs.

**Prioritisation**

17.9.20. Prioritisation helps identify and manage requirements for the use and management of cryptography and key management systems. This will determine the extent and complexity of the key management programme. Important aspects to consider are:

- Sensitivity and value of the data. This is summarised by the classification of the data but may not always reflect the values of aggregation, cost of compliance breaches or reputation damage from a breach.
- The volume of data and keys.
- The variety of key types, data formats, algorithms, protocols and sources.
- The speed and frequency of transactions, requirements for data access and availability.

## References

17.9.21. The NZCSI and NZCSS series of policy documents should be consulted for additional information on high grade cryptography.

17.9.22. Further information on key management practices can be found in the following references:

| Title | Publisher | Description & Source |
|---|---|---|
| **ISO 11568-1:2005 Banking -- Key management (retail) -- Part 1: Principles** | ISO / IEC | Specifies the principles for the management of keys used in cryptosystems implemented within the retail-banking environment. Focused mainly on card transactions and devices.<br>http://www.iso.org |
| **ISO 11568-2:2012 Financial services -- Key management (retail) -- Part 2: Symmetric ciphers, their key management and life cycle** | ISO / IEC | http://www.iso.org |
| **ISO 11568-4:2007 Banking -- Key management (retail) -- Part 4: Asymmetric cryptosystems -- Key management and life cycle** | ISO / IEC | http://www.iso.org |
| **ISO/IEC 11770-1:2010, Information Technology – Security Techniques – Key Management -- Part 1: Framework** | ISO / IEC | This standard describes the concepts of key management and some concept models for key distribution.<br>http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53456 |
| **ISO/IEC 11770-2:2008 Information technology -- Security techniques -- Key management -- Part 2:** | ISO / IEC | Mechanisms using symmetric techniques<br>http://www.iso.org |
| **ISO/IEC 11770-3:2015 Information technology -- Security techniques -- Key management -- Part 3:** | ISO / IEC | Mechanisms using asymmetric techniques<br>http://www.iso.org |
| **June 2005, RFC 4107, Guidelines for Cryptographic Key Management** | IETF | This document specifies an Internet Best Current Practices for the Internet Community https://tools.ietf.org/pdf/rfc4107.pdf |
| **Public Key Cryptography Standards** | IETF | Numbered #1 through #15 with some withdrawn (#4) or not completed (#13, #14). A series of Public Key Cryptography Standards.<br>https://tools.ietf.org |
| **August, 2013: NIST Special Publication (SP) 800-130, A Framework for Designing Cryptographic Key Management Systems.** | NIST | This publication contains a description of the topics to be considered and the documentation requirements to be addressed when designing a CKMS.<br>http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-130.pdf |
| **April 2013, Special Publication 800-53 R4, Security and Privacy** | NIST | Security and Privacy Controls for Federal Information Systems and Organizations updated 2015 |

| Title | Publisher | Description & Source |
|---|---|---|
| **Controls for Federal Information Systems** | | http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf |
| **December 2014 Special Publication 800-53A, R4 Assessing the Security Controls for Federal Information Systems** | NIST | http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf |
| **January, 2016: Revision 4 of Special Publication (SP) 800-57, Part 1, Recommendation for Key Management, Part 1: General.** | NIST | This publication contains basic key management guidance, including the security services that may be provided and the key types that may be employed in using cryptographic mechanisms, the functions involved in key management, and the protections and handling required for cryptographic keys. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf |
| **SP 800-57 Part 2, Recommendation for Key Management - Part 2: Best Practices for Key Management Organizations** | NIST | This recommendation provides guidance for system and application owners for use in identifying appropriate organisational key management infrastructures, establishing organizational key management policies, and specifying organisational key management practices. http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf |
| **January 2015: NIST Special Publication 800-57 Part 3 Revision 1, Recommendation for Key Management Part 1: General** | NIST | This document provides guidance on the use of application-specific key management. http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part3.pdf |
| **December 21, 2012: NIST Special Publication (SP) 800-133, Recommendation for Cryptographic Key Generation** | NIST | This Recommendation discusses the generation of the keys to be used with approved cryptographic algorithms. http://dx.doi.org/10.6028/NIST.SP.800-133 |
| **November, 2015: Special Publication (SP) 800-131A, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths.** | NIST | This Recommendation provides the approach for transitioning from the use of one algorithm or key length to another. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf |
| **Federal Information Processing Standards Publication FIPS Pub 140-2 Security Requirements For Cryptographic Modules** | NIST | This standard includes Annexes A-D and covers physical security as well as key management and design assurance. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf |
| **NISTIR 7609 January 2010 Cryptographic Key Management Workshop Summary** | NIST | Summary of workshop to develop and enhance key management standards. http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7609.pdf |
| **PCI Data Security Standards** | PCI | Requirements and Security Assessment Procedures Version 3.2 April 2016 https://www.pcisecuritystandards.org |

| Title | Publisher | Description & Source |
|---|---|---|
| **Enterprise Key Management Infrastructure (EKMI)** | OASIS | Guidance on standardising management of symmetric encryption cryptographic keys across the enterprise https://www.oasis-open.org |
| **Key Management Interoperability Protocol (KMIP)** | OASIS | Interoperability standard for enterprise encryption key management https://www.oasis-open.org |
| **Guidelines on Cryptographic Algorithms Usage and Key Management December 2016** | European Payments Council | http://www.europeanpaymentscouncil.eu/index.cfm/knowledge-bank/epc-documents/guidelines-on-cryptographic-algorithms-usage-and-key-management/ |

17.9.23. Further information on key establishment can be found in the following references:

| Key Establishment | | |
|---|---|---|
| **June 5, 2013: SP 800-56A Revision 2:**<br>**Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography** | NIST | The revisions are made on the March 2007 version of this Recommendation. The major revisions are summarized in Appendix D.<br>http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf |
| **August 27, 2009: SP 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography** | NIST | This Recommendation provides the specifications of key establishment schemes that are based on a standard developed by the Accredited Standards Committee (ASC) X9, Inc.: ANS X9.44, Key Establishment using Integer Factorization Cryptography. SP 800-56B provides asymmetric-based key agreement and key transport schemes that are based on the Rivest Shamir Adleman (RSA) algorithm.<br>http://csrc.nist.gov/publications/nistpubs/800-56B/sp800-56B.pdf |
| **December 11, 2011: NIST SP 800-56C,**<br>**Recommendation for Key Derivation through Extraction-then-Expansion** | NIST | This Recommendation specifies techniques for the derivation of keying material from a shared secret established during a key establishment scheme defined in NIST Special Publications 800-56A or 800-56B through an extraction-then-expansion procedure.<br>http://csrc.nist.gov/publications/nistpubs/800-56C/SP-800-56C.pdf |
| **December 2012: NIST has published an ITL Bulletin that summarizes NIST SP 800-133: Recommendation for Cryptographic Key Generation.** | NIST | http://csrc.nist.gov/publications/nistbul/itlbul2012_12.pdf<br>http://csrc.nist.gov/groups/ST/toolkit/key_management.html |
| **NIST Special Publication 800-38F, December 2012 - Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping** | NIST | http://dx.doi.org/10.6028/NIST.SP.800-38F |
| **Public Key Cryptography Standards** | IETF | Numbered #1 through #15 with some withdrawn (#4) or not completed (#13, #14). A series of Public Key Cryptography Standards.<br>https://tools.ietf.org |

## Rationale & Controls

### 17.9.24. Developing Key Management Plans (KMPs)

**17.9.24.R.01. Rationale**

Most modern cryptographic systems are designed to be highly resistant to cryptographic analysis but it MUST be assumed that a determined attacker could obtain details of the cryptographic logic either by stealing or copying relevant material directly or by suborning an New Zealand national or allied national. Cryptographic system material is safeguarded by implementing strong personnel, physical, documentation and procedural security measures.

**17.9.24.R.02. Rationale**

Cryptographic system material is safeguarded by implementing strong key management plan (KMP) encompassing personnel, physical, documentation and procedural security measures.

**17.9.24.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST develop a KMP when they have implemented a cryptographic system using HGCP.

**17.9.24.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

The level of detail included in a KMP MUST be consistent with the criticality and classification of the information to be protected.

**17.9.24.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD develop a KMP when they have implemented a cryptographic system using commercial grade cryptographic equipment.

### 17.9.25. Contents of KMPs

**17.9.25.R.01. Rationale**

When agencies implement the recommended contents for KMPs they will have a good starting point for the protection of cryptographic systems and their material within their agencies.

**17.9.25.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

The table below describes the minimum contents which SHOULD be documented in the KMP.

| Topic | Content |
|---|---|
| **Objectives** | • Objectives of the cryptographic system and KMP, including organisational aims.<br>• Refer to relevant NZCSIs. |
| **System description** | • The environment.<br>• Maximum classification of information protected.<br>• Topology Diagram(s) and description of the cryptographic system topology including data flows.<br>• The use of keys.<br>• Key algorithm.<br>• Key length.<br>• Key lifetime. |
| **Roles and administrative responsibilities.** | Documents roles and responsibilities, including the:<br>• COMSEC Custodian;<br>• Cryptographic systems administrator;<br>• Record keeper; and<br>• Auditor |
| **Accounting** | • How accounting will be undertaken for the cryptographic system. |
| | • What records will be maintained. |
| | • How records will be audited. |
| **Classification** | • Classification of the cryptographic system hardware. |
| | • Classification of cryptographic system software. |
| | • Classification of the cryptographic system documentation. |
| **Information security incidents** | • A description of the conditions under which compromise of key material should be declared. |
| | • References to procedures to be followed when reporting and dealing with information security incidents. |
| **Key management** | • Who generates keys. |
| | • How keys are delivered. |
| | • How keys are received |
| | • Key distribution, including local, remote and central. |
| | • How keys are installed. |
| | • How keys are transferred. |
| | • How keys are stored. |
| | • How keys are recovered. |
| | • How keys are revoked. |
| | • How keys are destroyed. |
| **Maintenance** | • Maintaining the cryptographic system software and hardware. |
| | • Destroying equipment and media. |
| **References** | • Vendor documentation |
| | • Related policies. |

### 17.9.26. Accounting

**17.9.26.R.01. Rationale**

As cryptographic equipment, and the keys they store, provide a significant security function for systems it is important that agencies are able to account for all cryptographic equipment.

**17.9.26.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST be able to readily account for all transactions relating to cryptographic system material including identifying hardware and all software versions issued with the equipment and materials, including date and place of issue.

**17.9.26.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD be able to readily account for all transactions relating to cryptographic system material including identifying hardware and all software versions issued with the equipment and materials, including date and place of issue.

### 17.9.27. Audits, compliance and inventory checks

**17.9.27.R.01. Rationale**

Cryptographic system audits are used as a process to account for cryptographic equipment.

**17.9.27.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST conduct audits using two personnel with cryptographic system administrator access.

**17.9.27.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD conduct audits of cryptographic system material:

- on handover/takeover of administrative responsibility for the cryptographic system;
- on change of personnel with access to the cryptographic system; and
- at least annually.

**17.9.27.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD perform audits to:

- account for all cryptographic system material; and
- confirm that agreed security measures documented in the KMP are being followed.

### 17.9.28. Access register

**17.9.28.R.01. Rationale**

Access registers can assist in documenting personnel that have privileged access to cryptographic systems along with previous accounting and audit activities for the system.

**17.9.28.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST hold and maintain an access register that records cryptographic system information such as:

- details of personnel with system administrator access;
- details of those whose system administrator access was withdrawn;
- details of system documents;
- accounting activities; and
- audit activities.

### 17.9.29. Cryptographic system administrator access

**17.9.29.R.01. Rationale**

The cryptographic system administrator is a highly privileged position which involves granting privileged access to a cryptographic system. Therefore extra precautions need to be put in place surrounding the security and vetting of the personnel as well as the access control procedures for individuals designated as cryptographic system administrators.

**17.9.29.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Before personnel are granted cryptographic system administrator access, agencies MUST ensure that they have:

- a demonstrated need for access;
- read and agreed to comply with the relevant Key Management Policy and Plan (KMP) for the cryptographic system they are using;
- a security clearance at least equal to the highest classification of information processed by the cryptographic system;
- agreed to protect the authentication information for the cryptographic system at the highest classification of information it secures;
- agreed not to share authentication information for the cryptographic system without approval;
- agreed to be responsible for all actions under their accounts;
- agreed to report all potentially security related problems to the GCSB; and
- ensure relevant staff have received appropriate training.

### 17.9.30. Area security and access control

**17.9.30.R.01. Rationale**

As cryptographic equipment contains particularly sensitive information additional physical security measures need to be applied to the equipment.

**17.9.30.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Cryptographic system equipment SHOULD be stored in a room that meets the requirements for a server room of an appropriate level based on the classification of information the cryptographic system processes.

**17.9.30.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Areas in which cryptographic system material is used SHOULD be separated from other areas and designated as a controlled cryptography area.

### 17.9.31. High grade cryptographic products

**17.9.31.R.01. Rationale**

The NZCSI series of documents provide product specific policy for HGCP.

**17.9.31.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST comply with NZCSI when using HGCP or HGCE.

### 17.9.32. Transporting commercial grade cryptographic equipment & products

**17.9.32.R.01. Rationale**

Transporting commercial grade cryptographic equipment in a keyed state exposes the equipment to the potential for interception and compromise of the key stored within the equipment. As such when commercial grade cryptographic equipment is transported in a keyed state it needs to be done so according to the requirements for the classification of the key stored in the equipment.

**17.9.32.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Unkeyed commercial grade cryptographic equipment MUST be distributed and managed by a means approved for the transportation and management of government property.

**17.9.32.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Keyed commercial grade cryptographic equipment MUST be distributed, managed and stored by a means approved for the transportation and management of government property based on the classification of the key within the equipment.

**17.9.32.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT transport commercial grade cryptographic equipment in a keyed state.

# 17.10. Hardware Security Modules

## Objective

17.10.1. Hardware Security Modules are used where additional security of cryptographic functions is desirable.

## Context

### Scope

17.10.2. This section covers information relating to Hardware Security Modules (HSMs). Detailed key management guidance is provided in Section 17.9 – Key Management.

### Hardware Security Module

17.10.3. Hardware Security Modules (HSMs) are defined as a hardware module or appliance which provides cryptographic functions. HSM's can be integrated into a design, installed in a host or be externally connected. HSM's can be packaged as discrete appliances, PCI cards, USB devices, smartcards or other form factors.

17.10.4. Functions include (but are not limited to) encryption, decryption, key generation, signing, hashing and cryptographic acceleration. The appliance usually also offers some level of physical tamper-resistance, has a user interface and a programmable interface for key management, configuration and firmware or software updates.

### Usage

17.10.5. HSMs are used in high assurance security solutions that satisfy widely established and emerging standards of due care for cryptographic systems and practices—while also maintaining high levels of operational efficiency. Traditional use of HSMs is within automatic teller machines, electronic fund transfer, and point-of-sale networks. HSMs are also used to secure CA keys in PKI deployments, SSL acceleration and DNSSEC (DNS Security Extensions) implementations.

### Physical Security

17.10.6. HSM's usually describe an encapsulated multi-chip module, device, card or appliance, rather than a single chip component or device. The nature of HSM's requires more robust physical security, including tamper resistance, tamper evidence, tamper detection, and tamper response.

### Tamper Resistance

17.10.7. Tamper Resistance is designed to limit the ability to physically tamper with, break into or extract useful information from an HSM. Often the boards and components are encased in an epoxy-like resin that will destroy any encapsulated components when drilled, scraped or otherwise physically tampered with.

### Tamper Evidence

17.10.8. The HSM is designed so that any attempts at tampering are evident. Many devices use seals and labels designed break or reveal a special message when physical tampering is attempted. Tamper evidence may require a regular inspection or audit mechanism.

17.10.9. HSMs can include features that detect and report tampering attempts. For example, embedding a conductive mesh within the epoxy-like package; internal circuitry monitored the electrical proper-ties of this mesh — properties which physical tamper would disrupt. Devices can also monitor for temperature extremes, radiation extremes, light, air and other unusual conditions.

### Tamper Response

17.10.10. HSMs can include defensive features that activate when tampering is detected. For example, cryptographic keys and sensitive data are deleted or zeroised. A trade-off exists between availability and security as an effective tamper response essentially renders the HSM unusable.

## References

17.10.11. Further references can be found at:

| Title | Publisher | Source |
|---|---|---|
| **Payment Card Industry (PCI) Hardware Security Module (HSM) - Security Requirements - Version 1.0, April 2009** | PCI | https://www.pcisecuritystandards.org/documents/PCI%20HSM%20Security%20Requirements%20v1.0%20final.pdf |
| **FIPS PUB 140-2 - Effective 15-Nov-2001 - Security Requirements for Cryptographic Modules** | NIST | http://csrc.nist.gov/groups/STM/cmvp/standards.html |

## Rationale & Controls

### 17.10.12. Hardware Security Modules

**17.10.12.R.01. Rationale**

Where high assurance or high security is required or high volumes of data are encrypted or decrypted, the use of an HSM should be considered when designing the network and security architectures.

**17.10.12.C.01. Control:** Systems Classification(s): C, S, TS; Compliance: MUST

Agencies MUST consider the use of HSMs when undertaking a security risk assessment or designing network and security architectures.

**17.10.12.C.02. Control:** Systems Classification(s): C, S, TS; Compliance: MUST

Agencies MUST follow the product selection guidance in this manual. See Chapter 12 – Product Security.

**17.10.12.C.03. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider the use of HSMs when undertaking a security risk assessment or designing network and security architectures.

**17.10.12.C.04. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD follow the product selection guidance in this manual. See Chapter 12 – Product Security.

# 18. Network security

## 18.1. Network Management

### Objective

18.1.1. Any change to the configuration of networks is authorised and controlled through appropriate change management processes to ensure security, functionality and capability is maintained.

### Context

#### Scope

18.1.2. This section covers information relating to the selection, management and documentation of network infrastructure.

#### Network diagrams

18.1.3. An agency's network diagrams should illustrate all network devices including firewalls, IDSs, IPSs, routers, switches, hubs, etc. It does not need to illustrate all IT equipment on the network, such as workstations or printers which can be collectively represented. The inclusion of significant devices such as MFD's and servers can aid interpretation.

#### Systems Documentation

18.1.4. Knowledge of systems design, equipment and implementation is a primary objective of those seeking to attack or compromise systems or to steal information. System documentation is a rich source allowing attackers to identify design weaknesses and vulnerabilities. The security of systems documentation is therefore important in preserving the security of systems.

18.1.5. Detailed network documentation and configuration details can contain information about IP addresses, port numbers, host names, services and protocols, software version numbers, patch status, security enforcing devices and information about information compartments and enclaves containing highly valuable information. This information can be used by a malicious actor to compromise an agency's network.

18.1.6. This information may be particularly exposed when sent to offshore vendors, consultants and other service providers. Encrypting this data will provide an important protective measure and assist in securing this data and information.

18.1.7. Reference should also be made to Section 12.7 – Supply Chain.

## PSR references

18.1.8. Relevant PSR requirements can be found at:

| Reference | Title | Source |
|---|---|---|
| **PSR Mandatory Requirements** | GOV5, GOV6, INFOSEC1, INFOSEC2, INFOSEC3 and INFOSEC4 | http://www.protectivesecurity.govt.nz |
| **PSR content protocols** | Management protocol for information security | http://www.protectivesecurity.govt.nz |
| **PSR requirements sections** | Handling requirements for protectively marked information and equipment<br>Supply chain security<br>Understand the information security lifecycle | http://www.protectivesecurity.govt.nz |
| **Managing specific scenarios** | Outsourced ICT facilities<br>Outsourcing, Offshoring and supply chains<br>Communication security<br>Mobile and remote working<br>Physical security for ICT systems<br>Working away from the office | http://www.protectivesecurity.govt.nz |

## Rationale & Controls

### 18.1.9. Classification of Network Documentation

**18.1.9.R.01. Rationale**

To provide an appropriate level of protection to systems and network documentation, a number of security aspects should be considered. These include:

- the existence of the system;
- the intended use;
- the classification of the data to be carried or processed by this system;
- the connectivity and agencies connected;
- protection enhancements and modifications; and
- the level of detail included in the documentation.

High level conceptual diagrams and accompanying documentation should also be subject to these considerations.

**18.1.9.C.01. Control:** Systems Classification(s): All Classifications; Compliance: MUST

Agencies MUST perform a security risk assessment before providing network documentation to a third party, such as a commercial provider or contractor.

**18.1.9.C.02. Control:** Systems Classification(s): C, S, TS; Compliance: MUST

Systems documentation and detailed network diagrams MUST be classified at least to the level of classification of the data to be carried on those systems.

**18.1.9.C.03. Control:** Systems Classification(s): All Classifications; Compliance: MUST

Network documentation provided to a third party, such as to a commercial provider or contractor, MUST contain only the information necessary for them to undertake their contractual services and functions, consistent with the need-to-know principle.

**18.1.9.C.04. Control:** Systems Classification(s): All Classifications; Compliance: MUST NOT

Detailed network configuration information MUST NOT be published in tender documentation.

**18.1.9.C.05. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD

Security aspects SHOULD be considered when determining the classification level of systems and network documentation.

### 18.1.10. Configuration management

**18.1.10.R.01. Rationale**

If the network is not centrally managed, there could be sections of the network that do not comply with the agency's security policies, and thus create a vulnerability.

**18.1.10.R.02. Rationale**

Changes should be authorised by a change management process, including representatives from all parties involved in the management of the network. This process ensures that changes are understood by all parties and reduces the likelihood of an unexpected impact on the network.

**18.1.10.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD keep the network configuration under the control of a network management authority.

**18.1.10.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

All changes to the configuration SHOULD be documented and approved through a formal change control process.

**18.1.10.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD regularly review their network configuration to ensure that it conforms to the documented network configuration.

**18.1.10.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD deploy an automated tool that compares the running configuration of network devices against the documented configuration.

### 18.1.11. Network diagrams

**18.1.11.R.01. Rationale**

As most decisions are made on the documentation that illustrates the network, it is important that:

- a network diagram exists;
- the security architecture is recorded;
- the network diagram is an accurate depiction of the network; and
- the network diagram indicates when it was last updated.

**18.1.11.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

For each network an agency manages they MUST have:

- a high-level diagram showing all connections and gateways into the network; and
- a network diagram showing all communications equipment.

### 18.1.12. Updating network diagrams

**18.1.12.R.01. Rationale**

Because of the importance of the network diagram and decisions made based upon its contents, it should be updated as changes are made. This will assist system administrators to completely understand and adequately protect the network.

**18.1.12.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

An agency's network diagrams MUST:

- be updated as network changes are made; and
- include a 'Current as at [date]' statement on each page.

**18.1.12.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

An agency's network diagrams SHOULD:

- be updated as network changes are made; and
- include a 'Current as at [date]' statement on each page.

### 18.1.13. Limiting network access

**18.1.13.R.01 Rationale**

If an attacker has limited opportunities to connect to a given network, they have limited opportunities to attack that network. Network access controls not only prevent against attackers traversing a network but also prevent system users carelessly connecting a network to another network of a different classification. It is also useful in segregating sensitive or compartmented information for specific system users with a need-to-know.

**18.1.13.R.02 Rationale**

Although circumventing some network access controls can be trivial, their use is primarily aimed at the protection they provide against accidental connection to another network.

**18.1.13.R.03 Rationale**

The design of a robust security architecture is fundamental to the security of a system. This may include concepts such as trust zones, application of the principles of separation and segregation through, for example, segmented networks and VPNs and other design techniques.

**18.1.13.C.01 Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST implement network access controls on all networks.

**18.1.13.C.02 Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD implement network access controls on all networks.

### 18.1.14. Management traffic

**18.1.14.R.01 Rationale**

Implementing protection measures specifically for management traffic provides another layer of defence on the network. This also makes it more difficult for an attacker to accurately define their target network.

**18.1.14.C.01 Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD implement protection measures to minimise the risk of unauthorised access to network management traffic on a network.

### 18.1.15. Simple Network Management IT Protocol (SNMP)

**18.1.15.R.01. Rationale**

The Simple Network Management Protocol (SNMP) can be used to monitor the status of network devices such as switches, routers and wireless access points. Early versions of SNMP were insecure. SNMPv3 uses stronger authentication methods but continues to establish default SNMP community strings and promiscuous access. Encryption may be used as an additional assurance measure but this may create additional workload in investigating faults. An assessment of risk, threats and the agency's requirements may be required to determine an appropriate configuration.

**18.1.15.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT use SNMP unless a specific requirement exists.

**18.1.15.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD implement SNMPv3 where a specific SNMP requirement exists.

**18.1.15.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD change all default community strings in SNMP implementations.

**18.1.15.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD

SNMP access SHOULD be configured as read-only.

# 18.2.Wireless Local Area Networks

## Objective

18.2.1. Wireless local area networks are deployed in a secure manner that does not compromise the security of information and systems.

## Context

### Scope

18.2.2. This section covers information on 802.11x WLANs. It does not cover other wireless communications. These communication methods are covered in Chapter 11 - Communications Systems and Devices. The description 802.11x refers to all versions and 802.11 standards.

| Title | Publisher | Source |
|---|---|---|
| **802.11 Wi-Fi** | IEEE | Wireless LAN Media Access Control and Physical Layer specification. 802.11a,b,g,etc. are amendments to the original 802.11 standard. Products that implement 802.11 standards must pass tests and are referred to as "Wi-Fi certified". |
| **802.15 Wireless Personal Area Networks** | IEEE | Communications specification that was approved in early 2002 by the IEEE for wireless personal area networks (WPANs and includes Bluetooth, Ultrs Wideband, Zigbee and Mesh Networks. |
| **802.16 Wireless Metropolitan Area Networks** | IEEE | This family of standards covers Fixed and Mobile Broadband Wireless Access methods used to create Wireless Metropolitan Area Networks (WMANs.) Connects Base Stations to the Internet using OFDM in unlicensed (900 MHz, 2.4, 5.8 GHz) or licensed (700 MHz, 2.5 – 3.6 GHz) frequency bands. Products that implement 802.16 standards can undergo WiMAX certification testing. |

18.2.3. Hardware Security Modules (HSMs) are defined as a hardware module or appliance that provides cryptographic functions. These functions include (but are not limited to) encryption, decryption, key generation, and hashing. The appliance usually also offers some level of physical tamper-resistance and has a user interface and a programmable interface. Refer also to Section 17.10 – Hardware Security Modules.

## References

18.2.4. Further information can be found at:

| Title | Publisher | Source |
|---|---|---|
| **Wi-Fi Alliance certification programs** | Wi-Fi Alliance | http://www.wi-fi.org/certification_programs.php |
| **802.11** | IEEE | http://standards.ieee.org/findstds/standard/802.11-2012.html |
| **EAP specification** | IETF | http://tools.ietf.org/html/rfc5247 |
| **EAP-TLS specification** | IETF | http://tools.ietf.org/html/rfc5216 |
| **EAP-TTLS specification** | IETF | http://tools.ietf.org/html/rfc5281 |
| **Payment Card Industry (PCI) Hardware Security Module (HSM) - Security Requirements - Version 1.0, April 2009** | PCI | https://www.pcisecuritystandards.org/documents/PCI%20HSM%20Security%20Requirements%20v1.0%20final.pdf |
| **FIPS PUB 140-2 - Effective 15-Nov-2001 - Security Requirements for Cryptographic Modules** | NIST | http://csrc.nist.gov/groups/STM/cmvp/standards.html |
| **Extensible Authentication Protocol** | Microsoft | https://technet.microsoft.com/en-us/network/bb643147.aspx |

## Rationale & Controls

### 18.2.5. Bridging networks

**18.2.5.R.01. Rationale**

When connecting devices via Ethernet to an agency's fixed network, agencies need to be aware of the risks posed by active wireless functionality. Devices may automatically connect to any open wireless networks they have previously connected to, which a malicious actor can use to masquerade and establish a connection to the device. This compromised device could then be used as a bridge to access the agency's fixed network. Disabling wireless functionality on devices, preferably by a hardware switch, whenever connected to a fixed network can prevent this from occurring. Additionally, devices do not have to be configured to remember and automatically connect to open wireless networks that they have previously connected to.

**18.2.5.C.01. Control:** Systems Classification(s): All Classifications; Compliance: MUST NOT

Devices MUST NOT be configured to remember and automatically connect to any wireless networks that they have previously connected to.

**18.2.5.C.02. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD

Wireless auto-connect functionality on devices SHOULD be disabled, preferably by a hardware switch, whenever connected to a fixed network.

### 18.2.6. Providing wireless communications for public access

**18.2.6.R.01. Rationale**

To ensure that a wireless network provided for public access cannot be used as a launching platform for attacks against an agency's system it MUST be segregated from all other systems. Security architectures incorporating segmented networks, DMZ's and other segregation mechanisms are useful in this regard.

**18.2.6.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies deploying a wireless network for public access MUST segregate it from any other agency network.

### 18.2.7. Using wireless communications

**18.2.7.R.01. Rationale**

As the Accreditation Authority for TOP SECRET systems, GCSB has mandated that all agencies considering deploying a wireless TOP SECRET deployment seek approval from GCSB prior to initiating any networking projects.

**18.2.7.C.01. Control:** System Classification(s): TS; Compliance: MUST NOT

Agencies MUST NOT use wireless networks unless the security of the agency's wireless deployment has been approved by GCSB.

### 18.2.8. Selecting wireless access point equipment

**18.2.8.R.01. Rationale**

Wireless access points that have been certified in a Wi-Fi Alliance certification program provide an agency with assurance that they conform to wireless standards. Deploying wireless access points that are guaranteed to be interoperable with other wireless access points on a wireless network will limit incompatibility of wireless equipment and incorrect implementation of wireless devices by vendors.

**18.2.8.C.01. Control:** Systems Classification(s): All Classifications; Compliance: MUST

All wireless access points used for government wireless networks MUST be Wi-Fi Alliance certified.

### 18.2.9. 802.1X Authentication

**18.2.9.R.01. Rationale**

A number of Extensible Authentication Protocol (EAP) methods, supported by the Wi-Fi Protected Access 2 (WPA2) protocol, are available.

**18.2.9.R.02. Rationale**

Agencies deploying a secure wireless network can choose WPA2-Enterprise with EAP-Transport Layer Security (EAP-TLS), WPA2-Enterprise with EAP-Tunnelled Transport Layer Security (EAP-TTLS) or WPA2-Enterprise with Protected EAP (PEAP) to perform mutual authentication.

**WPA2-Enterprise with EAP-TLS** is considered one of the most secure EAP methods. With its inclusion in the initial release of the WPA2 standard, it enjoys wide support in wireless access points and in numerous operating systems such as Microsoft Windows, Linux and Apple OS X. EAP-TLS uses a public key infrastructure (PKI) to secure communications between devices and a Remote Access Dial In User Service (RADIUS) server through the use of X.509 certificates. While EAP-TLS provides strong mutual authentication, it requires an agency to have established a PKI. This involves either deploying their own certificate authority and issuing certificates, or purchasing certificates from a commercial certificate authority, for every device that accesses the wireless network. This can introduce additional costs and management overheads but the risk and security management advantages are significant.

The **EAP-TTLS/MSCHAPv2, or simply EAP-TTLS**, method used with WPA2-Enterprise is generally supported through the use of third party software. It has support in multiple operating systems including Microsoft Windows 7, 8, 10 and Server 2012 but does **not** have native support in earlier versions of Microsoft Windows. EAP-TTLS is different to EAP-TLS in that devices do not authenticate to the server when the initial TLS tunnel is created. Only the server authenticates to devices. Once the TLS tunnel has been created, mutual authentication occurs through the use of another EAP method.

An advantage of EAP-TTLS over PEAP is that a username is never transmitted in the clear outside of the TLS tunnel. Another advantage of EAP-TTLS is that it provides support for many legacy EAP methods, while PEAP is generally limited to the use of EAP-MSCHAPv2.

**PEAPv0/EAP-MSCHAPv2, or simply PEAP**, is the second most widely supported EAP method after EAP-TLS. It enjoys wide support in wireless access points and in numerous operating systems such as Microsoft Windows, Linux and Apple OS X. PEAP operates in a very similar way to EAP-TTLS by creating a TLS tunnel which is used to protect another EAP method. PEAP differs from EAP-TTLS in that when the EAP-MSCHAPv2 method is used within the TLS tunnel, only the password portion is protected and not the username. This may allow an intruder to capture the username and replay it with a bogus password in order to lockout the user's account, causing a denial of service for that user. While EAP-MSCHAPv2 within PEAP is the most common implementation, Microsoft Windows supports the use of EAP-TLS within PEAP, known as PEAP-EAP-TLS. This approach is very similar in operation to traditional EAP-TLS yet provides increased protection, as parts of the certificate that are not encrypted with EAP-TLS are encrypted with PEAP-EAP-TLS. The downside to PEAP-EAP-TLS is its support is limited to Microsoft products.

#### 18.2.9.R.03. Rationale

Ultimately, an agency's choice in authentication method will often be based on the size of their wireless deployment, their security requirements and any existing authentication infrastructure. If an agency is primarily motivated by security they can implement either PEAP-EAP-TLS or EAP-TLS. If they are primarily motivated by flexibility and legacy support they can implement EAP-TTLS. If they are primarily motivated by simplicity they can implement PEAP with EAP-MSCHAPv2.

#### 18.2.9.C.01. Control: Systems Classification(s): All Classifications; Compliance: MUST

WPA2-Enterprise with EAP-TLS, WPA2-Enterprise with PEAP-EAP-TLS, WPA2-Enterprise with EAP-TTLS or WPA2-Enterprise with PEAP MUST be used on wireless networks to perform mutual authentication.

### 18.2.10. Evaluation of 802.1X authentication implementation

#### 18.2.10.R.01. Rationale

The security of 802.1X authentication is dependent on three main elements and their interaction. These three elements include supplicants (clients) that support the 802.1X authentication protocol, authenticators (wireless access points) that facilitate communication between supplicants and the authentication server, and the authentication server (RADIUS server) that is used for authentication, authorisation and accounting purposes. To provide assurance that these elements have been implemented appropriately, supplicants, authenticators and the authentication server used in wireless networks must have completed an appropriate product evaluation.

#### 18.2.10.C.01. Control: Systems Classification(s): C, S, TS; Compliance: MUST

Supplicants, authenticators and the authentication server used in wireless networks MUST have completed an appropriate product evaluation.

#### 18.2.10.C.02. Control: Systems Classification(s): All Classifications; Compliance: SHOULD

Supplicants, authenticators and the authentication server used in wireless networks SHOULD have completed an appropriate product evaluation.

### 18.2.11. Issuing certificates for authentication

**18.2.11.R.01. Rationale**

Certificates for authenticating to wireless networks can be issued to either or both devices and users. For assurance, certificates must be generated using a certificate authority product or hardware security module (HSM) that has completed an appropriate product evaluation.

**18.2.11.R.02. Rationale**

When issuing certificates to devices accessing wireless networks, agencies need to be aware of the risk that these certificates could be stolen by malicious software. Once compromised, the certificate could be used on another device to gain unauthorised access to the wireless network. Agencies also need to be aware that in only issuing a certificate to a device, any actions taken by a user will only be attributable to the device and not a specific user.

**18.2.11.R.03. Rationale**

When issuing certificates to users accessing wireless networks, they can either be in the form of a certificate that is stored on a device or a certificate that is stored within a smart card. Issuing certificates on smart cards provides increased security, but usually at a higher cost. Security is improved because a user is more likely to notice a missing smart card and alert their local security team, who is then able to revoke the credentials on the RADIUS server. This can minimise the time an intruder has access to a wireless network.

**18.2.11.R.04. Rationale**

In addition, to reduce the likelihood of a stolen smart card from being used to gain unauthorised access to a wireless network, two-factor authentication can be implemented through the use of Personal Identification Numbers (PINs) on smart cards. This is essential when a smart card grants a user any form of administrative access on a wireless network or attached network resource.

**18.2.11.R.05. Rationale**

For the highest level of security, unique certificates should be issued for both devices and users. In addition, the certificates for a device and user must not be stored on the same device. Finally, certificates for users accessing wireless networks should be issued on smart cards with access PINs and not stored with a device when not in use.

**18.2.11.C.01. Control:** Systems Classification(s): All Classifications; Compliance: MUST

Agencies MUST generate certificates using a certificate authority product or hardware security module that has completed an appropriate product evaluation.

**18.2.11.C.02. Control:** Systems Classification(s): All Classifications; Compliance: MUST NOT

The certificates for both a device and user accessing a wireless network MUST NOT be stored on the same device.

**18.2.11.C.03. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use unique certificates for both devices and users accessing a wireless network.

**18.2.11.C.04. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD

Certificates for users accessing wireless networks SHOULD be issued on smart cards with access PINs and not stored with a device when not in use.

**18.2.11.C.05. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD

Certificates stored on devices accessing wireless networks SHOULD be protected by implementing full disk encryption on the devices.

## 18.2.12. Using commercial certification authorities for certificate generation

**18.2.12.R.01. Rationale**

A security risk exists with EAP-TTLS and PEAP when a commercial certificate authority's certificates are automatically trusted by devices using vendor trusted certificate stores. This trust can be exploited by obtaining certificates from a commercial certificate authority under false pretences, as devices can be tricked into trusting their signed certificate. This will allow the capture of authentication credentials presented by devices, which in the case of EAP-MSCHAPv2 can be cracked using a brute force attack granting not only network access but most likely Active Directory credentials as well.

To reduce this risk, devices can be configured to:

- validate the server certificate;
- disable any trust for certificates generated by commercial certificate authorities that are not trusted;
- disable the ability to prompt users to authorise net servers or commercial certificate authorities; and
- set devices to enable identity privacy to prevent usernames being sent prior to being authenticated by the RADIUS server.

**18.2.12.C.01. Control:** Systems Classification(s): All Classifications; Compliance: MUST

Devices MUST be configured to validate the server certificate, disable any trust for certificates generated by commercial certificate authorities that are not trusted and disable the ability to prompt users to authorise new servers or commercial certification authorities.

**18.2.12.C.02. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD

Devices SHOULD be set to enable identity privacy.

### 18.2.13. Caching 802.1X authentication outcomes

**18.2.13.R.01. Rationale**

When 802.1X authentication is used, a shared secret key known as the Pairwise Master Key (PMK) is generated. Upon successful authentication of a device, the PMK can be cached to assist with fast roaming between wireless access points. When a device roams away from a wireless access point that it has authenticated to, it will not need to perform a full re-authentication should it roam back while the cached PMK remains valid. To further assist with roaming, wireless access points can be configured to pre-authenticate a device to other neighbouring wireless access points that the device might roam to. Although requiring full authentication for a device each time it roams between wireless access points is ideal, agencies can chose to use PMK caching and pre-authentication if they have a business requirement for fast roaming. If PMK caching is used, the PMK caching period should not be set to greater than 1440 minutes (24 hours).

**18.2.13.C.01. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD NOT

The PMK caching period SHOULD NOT be set to greater than 1440 minutes (24 hours).

### 18.2.14. Remote Authentication Dial-In User Service (RADIUS) authentication

**18.2.14.R.01. Rationale**

The RADIUS authentication process that occurs between wireless access points and the RADIUS server is distinct and a separate to the 802.1X authentication process. During the initial configuration of wireless networks using 802.1X authentication, a shared secret is entered into either the wireless access points or the RADIUS server. If configured on the wireless access points, the shared secret is sent to the RADIUS server via the RADIUS protocol, and vice versa if configured on the RADIUS server. This shared secret is used for both RADIUS authentication and confidentiality of RADIUS traffic.

**18.2.14.R.02. Rationale**

An intruder that is able to gain access to the RADIUS traffic sent between wireless access points and the RADIUS server may be able to perform a brute force or an off-line dictionary attack to recover the shared secret. This in turn allows the intruder to decrypt all communications between wireless access points and the RADIUS server. To mitigate this security risk, communications between wireless access points and a RADIUS server must be encapsulated with an additional layer of encryption using an appropriate encryption product (See Chapter 17 – Cryptography).

**18.2.14.C.01. Control:** Systems Classification(s): All Classifications; Compliance: MUST

Communications between wireless access points and a RADIUS server MUST be encapsulated with an additional layer of encryption using an approved encryption product (See Chapter 17 – Cryptography).

### 18.2.15. Encryption

#### 18.2.15.R.01. Rationale

As wireless transmissions are capable of radiating outside of secure areas into unsecure areas they need to be encrypted to the same level as classified information communicated over cabled infrastructure in unsecure areas.

#### 18.2.15.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies using wireless networks MUST ensure that classified information is protected by cryptography that meets the assurance level mandated for the communication of information over unclassified network infrastructure (See Section 17.2, Suite B).

### 18.2.16. Cipher Block Chaining Message Authentication Code Protocol (CCMP) Encryption

#### 18.2.16.R.01. Rationale

As wireless transmissions are capable of radiating outside of secure areas, agencies cannot rely on the traditional approach of physical security to protect against unauthorised access to sensitive or classified information on wireless networks. Using the AES based Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) helps protect the confidentiality and integrity of all wireless network traffic.

#### 18.2.16.C.01. Control: Systems Classification(s): All Classifications; Compliance: MUST

CCMP MUST be used to protect the confidentiality and integrity of all wireless network traffic.

### 18.2.17. Temporal Key Integrity Protocol (TKIP) and Wireless Encryption Protocol (WEP)

#### 18.2.17.R.01. Rationale

CCMP was introduced in WPA2 to address feasible attacks against the Temporal Integrity Key Protocol (TKIP) used by the Wi-Fi Protected Access (WPA) protocol as well as the original Wireless Encryption Protocol (WEP). A malicious actor seeking to exploit vulnerabilities in TKIP and WEP can attempt to connect to wireless access points using one of these protocols. By default, wireless access points will attempt to accommodate this request by falling back to a legacy protocol that the device supports. Disabling or removing TKIP and WEP support from wireless access points ensures that wireless access points do not fall back to an insecure encryption protocol.

#### 18.2.17.C.01. Control: Systems Classification(s): All Classifications; Compliance: MUST

TKIP and WEP support MUST be disabled or removed from wireless access points.

### 18.2.18. Wired Equivalent Privacy (WEP)

**18.2.18.R.01. Rationale**

WEP has serious flaws which allow it to be trivially compromised. A WEP network should be considered equivalent to an unprotected network.

**18.2.18.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT use WEP for wireless deployments.

### 18.2.19. Wi-Fi Protected Access (WPA)

**18.2.19.R.01. Rationale**

WPA has been superseded by WPA2. Agencies are strongly encouraged to deploy WPA2 wireless networks instead of unsecure, WEP or WPA based wireless networks.

**18.2.19.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT use Wi-Fi Protected Access (WPA) for wireless deployments.

### 18.2.20. Pre-shared keys

**18.2.20.R.01. Rationale**

The use of pre-shared keys is poor practice and not recommended for wireless authentication, in common with many authentication and encryption mechanisms, the greater the length of pre-shared keys the greater the security they provide.

**18.2.20.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST NOT

Agencies MUST NOT use pre-shared keys for wireless authentication.

**18.2.20.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

If pre-shared keys are used, agencies SHOULD use random keys of the maximum allowable length.

**18.2.20.C.03. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT use pre-shared keys for wireless authentication.

### 18.2.21. Administrative interfaces for wireless access points

**18.2.21.R.01. Rationale**

Administrative interfaces may allow users to modify the configuration and security settings of wireless access points. Often wireless access points by default allow users to access the administrative interface over methods such as fixed network connections, wireless network connections and serial connections directly on the device. Disabling the administrative interface on wireless access points will prevent unauthorised connections.

**18.2.21.C.01. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD disable the administrative interface on wireless access points for wireless connections.

### 18.2.22. Protecting management frames on wireless networks

**18.2.22.R.01. Rationale**

Effective DoS attacks can be performed on the 802.11 protocol by exploiting unprotected management frames using inexpensive commercial hardware. WPA2 provides no protection for management frames and therefore does not prevent spoofing or DoS attacks.

**18.2.22.R.02. Rationale**

The current release of the 802.11 standard provides no protection for management frames and therefore does not prevent spoofing or DoS attacks.

**18.2.22.R.03. Rationale**

However, 802.11w was ratified in 2009 and specifically addresses the protection of management frames on wireless networks. Wireless access points and devices should be upgraded to support the 802.11w amendment or any later amendment or version that includes a capability for the protection of management frames.

**18.2.22.C.01. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD

Wireless access points and devices SHOULD be upgraded to support a minimum of the 802.11w amendment.

### 18.2.23. Default service set identifiers (SSIDs)

**18.2.23.R.01. Rationale**

All wireless access points are configured with a default Service Set Identifier (SSID). The SSID is commonly used to identify the *name* of a wireless network to users. As the default SSIDs of wireless access points are well documented on online forums, along with default accounts and passwords, it is important to change the default SSID and default passwords of wireless access points.

**18.2.23.C.01. Control:** Systems Classification(s): All Classifications; Compliance: MUST

Agencies MUST change the default SSID of wireless access points.

**18.2.23.C.02. Control:** Systems Classification(s): All Classifications; Compliance: MUST

Agencies MUST rename or remove default accounts and passwords.

### 18.2.24. Changing the SSID

**18.2.24.R.01. Rationale**

When changing the default SSID, it is important that it lowers the profile of an agency's wireless network. In doing so, the SSID of a wireless network should not be readily associated with an agency, the location of or within their premises, or the functionality of the network.

**18.2.24.R.02. Rationale**

This procedure applies to wireless network assets owned/or managed by the agency, including any guest or other publically accessible networks.

**18.2.24.C.01. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD NOT

The SSID of a wireless network SHOULD NOT be readily associated with an agency, the premises, location or the functionality of the network.

### 18.2.25. SSID Broadcasting

**18.2.25.R.01. Rationale**

A common method to lower the profile of wireless networks is disabling SSID broadcasting. While this ensures that the existence of wireless networks are not broadcast overtly using beacon frames, the SSID is still broadcast in probe requests, probe responses, association requests and re-association requests for the network. Malicious actors can determine the SSID of wireless networks by capturing these requests and responses. By disabling SSID broadcasting agencies will make it more difficult for legitimate users to connect to wireless networks as legacy operating systems have only limited support for hidden SSIDs. Disabling SSID broadcasting infringes the design of the 802.11x standards.

**18.2.25.R.02. Rationale**

A further risk exists where an intruder can configure a wireless access point to broadcast the same SSID as the hidden SSID used by a legitimate wireless network. In this scenario devices will automatically connect to the wireless access point that is broadcasting the SSID they are configured to use *before* probing for a wireless access point that accepts the hidden SSID. Once the device is connected to the intruder's wireless access point the intruder can steal authentication credentials from the device to perform a man-in-the-middle attack to capture legitimate wireless network traffic or to later reuse to gain access to the legitimate wireless network.

**18.2.25.R.03. Rationale**

Disabling SSID broadcasting is not considered to be an effective control and may introduce additional risks.

**18.2.25.C.01. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT disable SSID broadcasting on wireless networks.

### 18.2.26. Static addressing

**18.2.26.R.01. Rationale**

Rogue devices or Access Points (APs) are unauthorised Wireless Access Points operating outside of the control of an agency. Assigning static IP addresses for devices accessing wireless networks can prevent a rogue device when connecting to a network from being assigned a routable IP address. However, some malicious actors will be able to determine IP addresses of legitimate users and use this information to guess or spoof valid IP address ranges for wireless networks. Configuring devices to use static IP addresses introduces a management overhead without any tangible security benefit.

**18.2.26.C.01. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use the Dynamic Host Configuration Protocol (DHCP) for assigning IP addresses on wireless networks.

### 18.2.27. Media Access Control address filtering

**18.2.27.R.01. Rationale**

Devices that connect to wireless networks have a unique Media Access Control (MAC) address. It is possible to use MAC address filtering on wireless access points to restrict which devices can connect to wireless networks. While this approach will introduce a management overhead of configuring whitelists of approved MAC addresses, it can prevent rogue devices from connecting to wireless networks. However, some malicious actors will be able to determine valid MAC addresses of legitimate users already on wireless networks and use this information to spoof valid MAC addresses and gain access to a network. MAC address filtering introduces a management overhead without any real tangible security benefit.

**18.2.27.C.01. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD NOT

MAC address filtering SHOULD NOT be used as a security mechanism to restrict which devices connect to a wireless network.

### 18.2.28. Documentation

**18.2.28.R.01. Rationale**

Wireless device driver and WAP vulnerabilities are very exposed to the threat environment and require specific attention as exploits can gain immediate unauthorised access to the network.

**18.2.28.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Key generation, distribution and rekeying procedures SHOULD be documented in the SecPlan for the wireless network.

**18.2.28.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Wireless device drivers and their versions SHOULD be documented in the SecPlan for the wireless network.

### 18.2.29. Non-agency devices connecting to agency controlled wireless networks

**18.2.29.R.01. Rationale**

As agencies have no control over the security of non-agency devices or knowledge of the security posture of such devices, allowing them to connect to agency controlled wireless networks poses a serious threat. Of particular concern is that non-agency devices may be infected with viruses, malware or other malicious code that could crossover onto the agency network. Furthermore, any non-agency devices connecting to agency controlled wireless networks will take on the classification of the network and will need to be appropriately sanitised and declassified before being released back to their owners.

**18.2.29.R.02. Rationale**

The practice of Bring Your Own Device (BYOD) is becoming more widespread but introduces a significant number of additional risks to agency systems. Refer to Section 21.4 for guidance on the use of BYOD.

**18.2.29.C.01. Control:** Systems Classification(s): All Classifications; Compliance: MUST

Where BYOD has been approved by an agency, any wireless network allowing BYOD connections MUST be segregated from all other agency networks, including any agency wireless networks.

**18.2.29.C.02. Control:** Systems Classification(s): All Classifications; Compliance: MUST

Any BYOD devices MUST comply with the policies and configuration described in Section 21.4– BYOD.

**18.2.29.C.03. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT allow non-agency devices to connect to agency controlled wireless networks not intended or configured for BYOD devices or for public access.

### 18.2.30. Agency devices connecting to non-agency controlled wireless networks

**18.2.30.R.01. Rationale**

When agency devices connect to non-agency controlled wireless networks, particularly public wireless networks, the devices may be exposed to viruses, malware or other malicious code.

**18.2.30.R.02. Rationale**

If any agency device becomes infected and is later connected to an agency controlled wireless network then a crossover of viruses, malware or malicious code could occur.

**18.2.30.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT allow agency devices to connect to non-agency controlled wireless networks.

### 18.2.31. Connecting wireless networks to fixed networks

**18.2.31.R.01. Rationale**

When an agency has a business requirement to connect a wireless network to a fixed network, it is important that they consider the security risks. While fixed networks can be designed with a certain degree of physical security, wireless networks are often easily accessible outside of the agency's controlled area. Treating connections between wireless networks and fixed networks in the same way agencies would treat connections between fixed networks and the Internet can help protect against an intrusion originating from a wireless network against a fixed network. For example, agencies can implement a gateway to inspect and control the flow of information between the two networks.

**18.2.31.C.01. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD

Connections between wireless networks and fixed networks SHOULD be treated in the same way as connections between fixed networks and the Internet.

### 18.2.32. Wireless network footprint and Radio Frequency (RF) Controls

**18.2.32.R.01. Rationale**

Minimising the output power of wireless access points will reduce the footprint of wireless networks. Instead of deploying a small number of wireless access points that broadcast on high power, more wireless access points that use minimal broadcast power should be deployed to achieve the desired wireless network footprint. This has the added benefit of providing redundancy for a wireless network should a wireless access point become unserviceable. In such a case, the output power of other wireless access points can be temporarily increased to cover the footprint gap until the unserviceable wireless access point can be replaced.

**18.2.32.C.01. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD

Instead of deploying a small number of wireless access points that broadcast on high power, more wireless access points that use minimal broadcast power SHOULD be deployed to achieve the desired wireless network footprint.

### 18.2.33. Radio Frequency (RF) Propagation & Controls

**18.2.33.R.01. Rationale**

An additional method to limit a wireless network's footprint is through the use of radio frequency (RF) shielding on an agency's premises. While expensive, this will limit the wireless communications to areas under the control of an agency. RF shielding on an agency's premises has the added benefit of preventing the jamming of wireless networks from outside of the premises in which wireless networks are operating.

**18.2.33.C.01. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD

The effective range of wireless communications outside an agency's area of control SHOULD be limited by:

- Minimising the output power level of wireless devices;
- Implementing RF shielding within buildings in which wireless networks are used.

### 18.2.34. Interference between wireless networks

**18.2.34.R.01. Rationale**

Where multiple wireless networks are deployed in close proximity, there is the potential for RF interference to adversely impact the availability of the network, especially when networks are operating on commonly used default channels of 1 and 11. This interference is also apparent where a large number of wireless networks are is use in close proximity to the agency's premises.

**18.2.34.R.02. Rationale**

Sufficiently separating wireless networks through the use of channel separation can help reduce this risk. This can be achieved by using wireless networks that are configured to operate with at least one channel separation. For example, channels 1, 3 and 5 could be used to separate three wireless networks.

**18.2.34.C.01. Control:** Systems Classification(s): All Classifications; Compliance: SHOULD

Wireless networks SHOULD be sufficiently segregated through the use of channel separation.

# 18.3.Video & Telephony Conferencing and Internet Protocol Telephony

## Objective

18.3.1. Video & Telephony Conferencing (VTC), Internet Protocol Telephony (IPT) and Voice over Internet Protocol (VoIP) systems are implemented in a secure manner that does not compromise security, information or systems and that they operate securely.

## Context

### Scope

18.3.2. This section covers information on VTC and IPT including Voice over Internet Protocol (VoIP). Although IPT refers generally to the transport of telephone calls over IP networks, the scope of this section includes connectivity to the PSTN as well as remote sites.

18.3.3. Additional information relating to topics covered in this section can be found in

- Chapter 12 – Product Security;
- Chapter 11 – Communications Systems and Devices;
- Chapter 19 – Gateways Security; and
- any section in this manual relating to the protection of data networks.

### Exception for VTC and IPT gateways

18.3.4. Where a gateway connects between an *analogue* telephone network such as the PSTN and a computer network, Chapter 19 – Gateway Security does not apply.

18.3.5. Where a gateway connects between a VTC or IPT network and any other VTC or IPT network, Chapter 19 – Gateway Security applies.

### Hardening VTC and IPT systems

18.3.6. Data in a VTC or IPT network consists of IP packets and should not be treated any differently to other data. In accordance with the principles of least-privilege and security-in-depth, hardening can be applied to all handsets, control units, software, servers and gateways. For example a Session Initiation Protocol (SIP) server could:

- have a fully patched software and operating system;
- only required services running;
- use encrypted non-replayable authentication; and
- apply network restrictions that only allow secure Session Initiation Protocol (SIP) and secure Real Time Transport (RTP) traffic from IP phones on a VLAN to reach the server.

## References

18.3.7. Further information can be found at:

| Reference | Title | Publisher | Source |
|---|---|---|---|
| **SP 800-58** | Security Considerations for Voice Over IP Systems | NIST | http://csrc.nist.gov/publications/nistpubs/ |
| | Security Issues and Countermeasure for VoIP | SANS | http://www.sans.org/reading-room/whitepapers/voip/security-issues-countermeasure-voip-1701 |
| **Report Number: I332-016R-2005** | Security Guidance for Deploying IP Telephony Systems Released: 14 February 2006 | Systems and Network Attack Center (SNAC) NSA | https://www.nsa.gov/ia/_files/voip/i332-016r-2005.pdf |
| **Report Number: I332-009R-2006** | Recommended IP Telephony Architecture, Updated: 1May2006 Version1.0 | Systems and Network Attack Center (SNAC) NSA | https://www.nsa.gov/ia/_files/voip/I332-009R-2006.pdf |
| | Mobility Capability Package March 26 2012 - Secure VoIP Version 1.2 | NSA | https://www.nsa.gov/ia/_files/Mobility_Capability_Pkg_Vers_1_2.pdf |
| | Protecting Telephone-based Payment Card Data PCI Data Security Standard (PCI DSS) Version: 2.0, March 2011 | The PCI Security Standards Council (PCI SSC) | https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf |
| | PCI Mobile Payment Acceptance Security Guidelines Version: 1.0 Date: September 2012 | PCI SSC | https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Developers_v1.pdf |
| | PCI Mobile Payment Acceptance Security Guidelines Version: 1.0 Date: February 2013 | PCI SSC | https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Merchants_v1.pdf |
| | Understanding Voice over Internet Protocol (VoIP): 2006 | US-CERT | https://www.us-cert.gov/sites/default/files/publications/understanding_voip.pdf |
| **CNSS Instruction No. 5000 April 2007** | Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony | Committee on National Security Systems | https://www.cnss.gov/CNSS/issuances/Instructions.cfm |
| | DHS 4300A Sensitive Systems Handbook Attachment Q5 To Handbook v. 11.0 Voice over Internet Protocol (VoIP) Version 11.0 December 22, 2014 | DHS | http://www.dhs.gov/sites/default/files/publications/4300A%20Handbook%20Attachment%20Q5%20-%20Voice%20over%20IP.pdf |

## Rationale & Controls

### 18.3.8. Video and voice-aware firewalls

**18.3.8.R.01. Rationale**

The use of video, unified communications and voice-aware firewalls ensures that only video or voice traffic (e.g. signalling and data) is allowed for a given call and that the session state is maintained throughout the transaction.

**18.3.8.R.02. Rationale**

The requirement to use a video, unified communication or voice-aware firewall does not necessarily require separate firewalls to be deployed for video conferencing, IP telephony and data traffic. If possible, agencies are encouraged to implement one firewall that is either video and data-aware; voice and data-aware; or video, voice and data-aware depending on their needs.

**18.3.8.R.03. Rationale**

Refer to Section 19.5 - Session Border Controllers.

**18.3.8.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use a video, unified communication or voice-aware firewall that meets the same minimum level of assurance as specified for normal firewalls.

### 18.3.9. Protecting IPT signalling and data

**18.3.9.R.01. Rationale**

IPT voice and signalling data is vulnerable to eavesdropping but can be protected with encryption. This control helps protect against DoS, man-in-the-middle and call spoofing attacks made possible by inherent weaknesses in the VTC and IPT protocols.

**18.3.9.R.02. Rationale**

When protecting IPT signalling and data, voice control signalling can be protected using TLS and the 'sips://' identifier to force the encryption of all legs of the connection. Similar protections are available for RTP and the Real-Time Control Protocol.

**18.3.9.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD protect VTC and IPT signalling and data by using encryption.

**18.3.9.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

An encrypted and non-replayable two-way authentication scheme SHOULD be used for call authentication and authorisation.

### 18.3.10. Establishment of secure signalling and data protocols

**18.3.10.R.01. Rationale**

Use of secure signalling and data protects against eavesdropping, some types of DoS, man-in-the-middle and call spoofing attacks.

**18.3.10.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that VTC and IPT functions are established using only the secure signalling and data protocols.

### 18.3.11. Local area network traffic separation

**18.3.11.R.01. Rationale**

Availability and quality of service are the main drivers for applying the principles of separation and segregation.

**18.3.11.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST either separate or segregate the VTC and IPT traffic from other data traffic.

**18.3.11.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD either separate or segregate the IPT traffic from other data traffic.

### 18.3.12. VTC and IPT Device setup

**18.3.12.R.01. Rationale**

VTC equipment and VoIP phones need to be hardened and separated or segregated from the data network to ensure they will not provide an easy entry point to the network for an attacker.

**18.3.12.R.02. Rationale**

USB ports on these devices can be used to circumvent USB workstation policy and upload malicious software for unauthorised call recording/spoofing and entry into the data network. Unauthorised or unauthenticated devices should be blocked by default to reduce the risk of a compromise or denial of service.

**18.3.12.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST:

- configure VTC and VoIP devices to authenticate themselves to the call controller upon registration;
- disable phone auto-registration and only allow a whitelist of authorised devices to access the network;
- block unauthorised devices by default;
- disable all unused and prohibited functionality; and
- use individual logins for IP phones.

**18.3.12.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD:

- configure VoIP phones to authenticate themselves to the call controller upon registration;
- disable phone auto-registration and only allow a whitelist of authorised devices to access the network;
- block unauthorised devices by default;
- disable all unused and prohibited functionality; and
- use individual logins for IP phones.

### 18.3.13. Call authentication and authorisation

**18.3.13.R.01. Rationale**

This control ensures server-client mutual authentication.

**18.3.13.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Authentication and authorisation SHOULD be used for all actions on the IPT network, including:

- call setup;
- changing settings; and
- checking voice mail.

**18.3.13.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

An encrypted and non-replayable two-way authentication scheme SHOULD be used for call authentication and authorisation.

**18.3.13.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Authentication SHOULD be enforced for:

- registering a new phone;
- changing phone users;
- changing settings; and
- accessing voice mail.

### 18.3.14. VTC and IPT device connection to workstations

**18.3.14.R.01. Rationale**

Availability and quality of service are the main drivers for applying the principles of separation and segregation.

**18.3.14.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST NOT

Agencies MUST NOT connect workstations to VTC or IPT devices unless the workstation or the device, as appropriate for the configuration, uses VLANs or similar mechanisms to maintain separation between VTC, IPT and other data traffic.

**18.3.14.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT connect workstations to VTC or IPT devices unless the workstation or the device, as appropriate for the configuration, uses VLANs or similar mechanisms to maintain separation between VTC, IPT and other data traffic.

### 18.3.15. Lobby and shared area IPT devices

**18.3.15.R.01. Rationale**

IPT devices in public areas may give an attacker opportunity to access the internal data network by replacing the phone with another device, or installing a device in-line. There is also a risk to the voice network of social engineering (since the call may appear to be internal) and data leakage from poorly protected voice mail-boxes.

**18.3.15.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Where an agency uses a VoIP phone in a lobby or shared area they SHOULD limit or disable the phone's:

- ability to access data networks;
- functionality for voice mail and directory services; and
- use a separate network segment.

**18.3.15.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD, where available, use traditional analogue phones in a lobby and shared areas.

### 18.3.16. Usage of Softphones, Webcams and similar sound and video devices

**18.3.16.R.01. Rationale**

Software and applications for softphones and webcams can introduce additional attack vectors into the network as they are exposed to threats from the data network via the workstation and can subsequently be used to gain access to the network.

**18.3.16.R.02. Rationale**

Softphones and webcams typically require workstation to workstation communication, normally using a number of randomly assigned ports to facilitate RTP data exchange. This presents a security risk as workstations generally should be separated using host-based firewalls that deny all connections between workstations to make malicious code propagation inside the network difficult.

**18.3.16.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies using softphones or webcams SHOULD have separate dedicated network interface cards on the host for VTC or IPT network access to facilitate VLAN separation.

**18.3.16.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies using softphones or webcams SHOULD install a host-based firewall on workstations utilising softphones or webcams that allows traffic only to and from a minimum number of ports.

**18.3.16.C.03. Control:** System Classification(s): C, S, TS; Compliance: SHOULD NOT

Agencies SHOULD NOT use softphones or webcams.

### 18.3.17. Workstations using USB softphones, webcams and similar sound and video devices

**18.3.17.R.01. Rationale**

Adding softphones and webcams to a whitelist of allowed USB devices on a workstation will assist with restricting access to only authorised devices, and allowing the SOE to maintain defences against removable media storage and other unauthorised USB devices.

**18.3.17.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use access control software to control USB ports on workstations using softphones and webcams by utilising the specific vendor and product identifier of the authorised device.

### 18.3.18. Developing a denial of service response plan

**18.3.18.R.01. Rationale**

Communications are considered critical for any business and are therefore especially vulnerable to Denial of Service (DoS). The guidance provided will assist in protecting against VTC or IPT DoS attacks, signalling floods, established call teardown and RTP data floods. These elements should be included in the agency's wider response plan (See Section 6.4 – Business Continuity and Disaster Recovery).

**18.3.18.R.02. Rationale**

Simple DoS attacks and incidents are often the result of bandwidth exhaustion. Agencies should also consider other forms of DoS including Distributed Denial of Service attacks (DdoS), DNS and latency incidents.

**18.3.18.R.03. Rationale**

System resilience can be improved by architecting a structured approach and providing layered defence such as network and application protection as separate layers.

**18.3.18.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD develop a Denial of Service response plan including:

- how to identify the precursors and other signs of DoS;
- how to diagnose the incident or attack type and attack method;
- how to diagnose the source of the DoS;
- what actions can be taken to clear the DoS;
- how communications can be maintained during a DoS; and
- report the incident.

### 18.3.19. Content of a Denial of Service (DoS) response plan

**18.3.19.R.01. Rationale**

An VTC or IPT DoS response plan will need to address the following:

- how to identify the source of the DoS, either internal or external (location and content of logs);
- how to diagnose the incident or attack type and attack method;
- how to minimise the effect on VTC or IPT, of a DoS of the data network (e.g. Internet or internal DoS), including separate links to other office locations for VTC and IPT and/or quality of service prioritisation;
- strategies that can mitigate the DOS (banning certain devices/Ips at the call controller and firewalls, implementing quality of service, changing VoIP authentication, changing dial-in authentication; and
- alternative communication options (such as designated devices or personal mobile phones) that have been identified for use in case of an emergency.

**18.3.19.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

A Denial of Service response plan SHOULD include monitoring and use of:

- router and switch logging and flow data;
- packet captures;
- proxy and call manager logs and access control lists;
- VTC and IPT aware firewalls and voice gateways;
- network redundancy;
- load balancing;
- PSTN failover; and
- alternative communication paths.

# 18.4. Intrusion Detection and Prevention

## Objective

18.4.1. An intrusion detection and prevention strategy is implemented for systems in order to respond promptly to incidents and preserve availability, confidentiality and integrity of systems.

## Context

### Scope

18.4.2. This section covers information relating to detection and prevention of malicious code propagating through networks as well as the detection and prevention of unusual or malicious activities.

### Methods of infections or delivery

18.4.3. Malicious code can spread through a system from a number of sources including:

- files containing macro viruses or worms;
- email attachments and Web downloads with malicious active content;
- executable code in the form of applications;
- security weaknesses in a system or network;
- security weaknesses in an application;
- contact with an infected system or media; or
- deliberate introduction of malicious code.

18.4.4. The speed at which malicious code can spread through a system presents significant challenges and an important part of any defensive strategy is to contain the attack and limit damage.

## References

18.4.5. Further references can be found at:

| Title | Publisher | Source |
|---|---|---|
| **ISO/IEC 27001:2006, A.15.3, Information Systems Audit Considerations** | ISO / IEC<br><br>Standards NZ | http://www.iso27001security.com/html/27001.html<br>http://www.standards.co.nz |
| **HB 171:2003 Guidelines for the Management of Information Technology Evidence** | Standards NZ | http://www.standards.co.nz |

## References – Endpoint Security

18.4.6. Further references can be found at:

| Title | Publisher | Source |
|---|---|---|
| **Transport Layer Protection Cheat Sheet** | OWASP | https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet |
| **RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2** | IETF | https://tools.ietf.org/html/rfc5246 |
| **RFC 7525 - Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)** | IETF | https://tools.ietf.org/html/rfc7525 |
| **RFC 6749 - The OAuth 2.0 Authorization Framework** | IETF | https://tools.ietf.org/pdf/rfc6749.pdf |
| **OpenID Connect** | OpenID Foundation | http://openid.net/connect/ |
| **New Zealand Security Assertion Messaging Standard Web Page** | NZ Government – Department of Internal Affairs | https://www.ict.govt.nz/guidance-and-resources/standards-compliance/authentication-standards/new-zealand-security-assertion-messaging-standard/ |
| **New Zealand Security Assertion Messaging Standard** | NZ Government – Department of Internal Affairs | https://www.ict.govt.nz/assets/Uploads/Documents/egif-authentication-NZSAMS-v1.0.pdf |

## Rationale & Controls

### 18.4.7. Intrusion Detection and Prevention strategy (IDS/IPS)

**18.4.7.R.01. Rationale**

An IDS/IPS when configured correctly, kept up to date and supported by appropriate processes, can be an effective way of identifying, responding to and containing known attack types, specific attack profiles or anomalous or suspicious network activities.

**18.4.7.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST develop, implement and maintain an intrusion detection strategy that includes:

- appropriate intrusion detection mechanisms, including network-based IDS/IPSs and host-based IDS/IPSs as necessary;
- the audit analysis of event logs, including IDS/IPS logs;
- a periodic audit of intrusion detection procedures;
- information security awareness and training programs;
- a documented Incident Response Plans (IRP); and
- provide the capability to detect information security incidents and attempted network intrusions on gateways and provide real-time alerts.

**18.4.7.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD develop, implement and maintain an intrusion detection strategy that includes:

- appropriate intrusion detection mechanisms, including network-based IDS/IPSs and host-based IDS/IPSs as necessary;
- the audit analysis of event logs, including IDS/IPS logs;
- a periodic audit of intrusion detection procedures;
- information security awareness and training programs; and
- a documented IRP.

**18.4.7.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure sufficient resources are provided for the maintenance and monitoring of IDS/IPS.

### 18.4.8. IDS/IPSs on gateways

**18.4.8.R.01. Rationale**

If the firewall is configured to block all traffic on a particular range of port numbers, then the IDS should inspect traffic for these port numbers and alert if they are detected.

**18.4.8.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD deploy IDS/IPSs in all gateways between the agency's networks and unsecure public networks or BYOD wireless networks.

**18.4.8.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD deploy IDS/IPSs at all gateways between the agency's networks and any network not managed by the agency.

**18.4.8.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD locate IDS/IPSs within the gateway environment, immediately inside the outermost firewall.

### 18.4.9. IDS/IPS Maintenance

**18.4.9.R.01. Rationale**

When signature-based intrusion detection is used, the effectiveness of the IDS/IPS will degrade over time as new intrusion methods are developed. It is for this reason that IDS/IPS systems and signatures need to be up to date to identify the latest intrusion detection methods.

**18.4.9.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST select IDS / IPS that monitor uncharacteristic and suspicious activities.

**18.4.9.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

When signature-based intrusion detection is used, agencies MUST keep the signatures and system patching up to date.

### 18.4.10. Malicious code counter-measures

**18.4.10.R.01. Rationale**

Implementing policies and procedures for preventing and dealing with malicious code outbreaks that enables agencies to provide consistent incident response, as well as giving clear directions to system users on how to respond to an information security incident.

**18.4.10.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST:

- develop and maintain a set of policies and procedures covering how to:
  - minimise the likelihood of malicious code being introduced into a system;
  - prevent all unauthorised code from executing on an agency network;
  - detect any malicious code installed on a system;
- make their system users aware of the agency's policies and procedures; and
- ensure that all instances of detected malicious code outbreaks are handled according to established procedures.

### 18.4.11. Configuring the IDS/IPS

**18.4.11.R.01. Rationale**

Generating alerts for any information flows that contravene any rule within the firewall rule set will assist security personnel in identifying and reporting to any possible breaches of agency systems.

**18.4.11.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

In addition to agency defined configuration requirements, agencies SHOULD ensure that IDS/IPSs located inside a firewall are configured to generate a log entry, and an alert, for any information flows that contravene any rule within the firewall rule set.

**18.4.11.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD test IDS/IPSs rule sets prior to implementation to ensure that they perform as expected.

**18.4.11.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

If a firewall is configured to block all traffic on a particular range of port numbers, the IDP/IPSs SHOULD inspect traffic for these port numbers and generate an alert if they are detected.

### 18.4.12. Event management and correlation

**18.4.12.R.01. Rationale**

Deploying tools to manage correlation of suspicious events or events of interest across all agency networks will assist in identifying suspicious patterns in information flows throughout the agency.

**18.4.12.R.02. Rationale**

The history of events is important in this analysis and should be accommodated in any archiving decisions.

**18.4.12.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD deploy tools for:

- the management and archive of security event information; and
- the correlation of suspicious events or events of interest across all agency networks.

### 18.4.13. Host-based IDS/IPSs

**18.4.13.R.01. Rationale**

Host-based IDS/IPS use behaviour-based detection schemes and can therefore assist in the detection of previously unidentified anomalous and suspicious activities such as:

- process injection;
- keystroke logging;
- driver loading;
- library additions or supercessions;
- call hooking.

They may also identify new malicious code. It should be noted that some anti-virus and similar security products are evolving into converged endpoint security products that incorporate HIDS/HIPS.

**18.4.13.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD install host-based IDS/IPSs on authentication, DNS, email, Web and other high value servers.

### 18.4.14. Active content blocking

**18.4.14.R.01. Rationale**

Filtering unnecessary content and disabling unwanted functionality reduces the number of possible entry points that an attacker can exploit.

**18.4.14.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use:

- filters to block unwanted content and exploits against applications that cannot be patched;
- settings within the applications to disable unwanted functionality; and
- digital signatures to restrict active content to trusted sources only.

# 18.5.Internet Protocol Version 6

## Objective

18.5.1. IPv6 is disabled until it is ready to be deployed.

## Context

### Scope

18.5.2. This section covers information on IPv6 and its deployment within networks. Where this manual specifies requirements for network devices, the requirements apply equally whether deploying IPv6 or IPv4.

18.5.3. IPv6 was officially launched by the Internet Society in June 2012. With the change from IPv4 to IPv6, there is the potential to introduce vulnerabilities to agency networks through incorrect or mis-configuration, poor design and poor device compatibility. Attackers will also be actively seeking to exploit vulnerabilities that will inevitably be exposed.

18.5.4. Agencies unable to meet the compliance requirements as specified for a control when deploying IPv6 network infrastructure will need to follow the procedures as specified in this manual for varying from a control and the associated compliance requirements.

### DNS Security Extensions (DNSSEC)

18.5.5. DNSSEC has been developed to enhance Internet security and can digitally 'sign' data to assure validity. It is essential that DNSSEC is deployed at each step in the lookup from root zone to final domain name (e.g., www.icann.org). Signing the root (deploying DNSSEC on the root zone) is a necessary step in this overall process. Importantly it does not encrypt *data*. It just attests to the validity of the address of the site you visit. DNSSEC and IPv6 have been engineered to integrate and thus enhance Internet security.

## References

18.5.6. Further references can be found at:

| Title | Publisher | Source |
|---|---|---|
| **A strategy for the transition to IPv6 for Australian Government agencies. (archived document)** | Australian Government Information Management Office | https://www.finance.gov.au/files/2011/10/Australian-Government-Transition-to-IPv6-2011.doc |
| **Manageable Network Plan** | NSA | www.nsa.gov/ia/_files/vtechrep/ManageableNetworkPlan.pdf |
| **Router Security Configuration Guide Supplement – Security for IPv6 Routers, 23 May 2006 Version: 1.0** | NSA | http://www.nsa.gov/ia/_files/routers/I33-002R-06.pdf |
| **Firewall Design Considerations for IPv6, 10/3/2007** | NSA | http://www.hpc.mil/images/hpcdocs/ipv6/nsa-firewall-design-ipv6-i733-041r-2007.pdf |
| **Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41, Revision 1, September 2009** | NIST | http://csrc.nist.gov/publications/PubsSPs.html |
| **Guidelines for secure deployment of IPv6, Special Publication 800-119, December 2010** | NIST | http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf |
| **A Complete Guide on IPv6 Attack and Defense** | SANS Institute | http://www.sans.org/reading-room/whitepapers/detection/complete-guide-ipv6-attack-defense-33904?show=complete-guide-ipv6-attack-defense-33904&cat=detection |
| **Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, December 1998** | IETF | http://www.ietf.org/rfc/rfc2460.txt |
| **IP Version 6 Addressing Architecture, RFC 4291, February 2006** | IETF | http://tools.ietf.org/html/rfc4291 |
| **A Recommendation for IPv6 Address Text Representation, ISSN: 2070-1721, RFC 5952, August 2010** | IETF | http://tools.ietf.org/html/rfc5952 |
| **Ipv6 Addressing of IPv4/IPv6 Translators, ISSN: 2070-1721, RFC 6052, October 2010** | IETF | http://tools.ietf.org/html/rfc6052 |
| **Significance of IPv6 Interface Identifiers, RFC 7136, ISSN: 2070-1721, February 2014** | IETF | http://tools.ietf.org/html/rfc7136 |
| **DNSSEC Operational Practices, Version 2** | IETF | http://tools.ietf.org/search/rfc6781 |
| **Clarifications and Implementation Notes for DNS Security (DNSSEC)** | IETF | http://tools.ietf.org/search/rfc6840 |
| **A Framework for DNSSEC Policies** | IETF | http://tools.ietf.org/html/rfc6841 |

| Title | Publisher | Source |
|---|---|---|
| **and DNSSEC Practice Statements** | | |
| **IETF RFC 7123 Security Implications of IPv6 on IPv4 Networks** | IETF | http://tools.ietf.org/html/rfc7123 |
| **IETF RFC 4861 Neighbor Discovery for IP version 6 (IPv6)** | IETF | http://tools.ietf.org/html/rfc4861 |
| **IETF RFC 5942 IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes** | IETF | http://tools.ietf.org/html/rfc5942 |
| **IETF RFC 3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)** | IETF | http://www.ietf.org/rfc/rfc3315.txt |
| **IETF RFC 6104 Rogue IPv6 Router Advertisement Problem Statement** | IETF | http://tools.ietf.org/html/rfc6104 |
| **IPv6 First-Hop Security Concerns** | Cisco | http://www.cisco.com/web/about/security/intelligence/ipv6_first_hop.html |
| **DNSSEC – What Is It and Why Is It Important?** | Internet Corporation for Assigned Names and Numbers (ICAAN) | http://www.icann.org/en/about/learning/factsheets/dnssec-qaa-09oct08-en.htm |

## Rationale & Controls

### 18.5.7. Use of dual-stack equipment

**18.5.7.R.01. Rationale**

In order to reduce the attack surface area of agency systems, it is good practice that agencies disable unused services and functions within network devices and operating systems. If agencies are deploying dual-stack equipment but not using the IPv6 functionality, then that functionality should be disabled. It can be re-enabled when required. This will reduce the opportunity to exploit IPv6 functionality before appropriate security measures have been implemented.

**18.5.7.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies not using IPv6, but which have deployed dual-stack network devices and ICT equipment that supports IPv6, MUST disable the IPv6 functionality, unless that functionality is required.

**18.5.7.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Network security devices on IPv6 or dual-stack networks MUST be IPv6 capable.

### 18.5.8. Using IPv6

**18.5.8.R.01. Rationale**

The information security implications around the use of IPv6 are still largely unknown and un-tested. As many of the deployed network protection technologies, such as firewalls and IDSs, do not consistently support IPv6, agencies choosing to implement IPv6 face an increased risk of systems compromise.

**18.5.8.R.02. Rationale**

A number of tunnelling protocols have been developed to facilitate interoperability between IPv4 and IPv6. Disabling IPv6 tunnelling protocols when this functionality is not explicitly required will reduce the risk of bypassing network defences by means of encapsulating IPv6 data inside IPv4 packets.

**18.5.8.R.03. Rationale**

Stateless Address Autoconfiguration (SLAAC) is a method of stateless IP address configuration in IPv6. SLAAC reduces the ability to maintain complete logs of IP address assignment on the network. To avoid this constraint, stateless IP addressing SHOULD NOT be used.

**18.5.8.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies using IPv6 MUST conduct a security risk assessment on risks that could be introduced as a result of running a dual stack environment or transitioning completely to IPv6.

**18.5.8.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies implementing a dual stack or wholly IPv6 network or environment MUST re-accredit their networks.

**18.5.8.C.03. Control:** System Classification(s): All Classifications; Compliance: MUST

IPv6 tunnelling MUST be disabled on all network devices, unless explicitly required.

**18.5.8.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Dynamically assigned IPv6 addresses SHOULD be configured with DHCPv6 in a stateful manner and with lease information logged and logs stored in a centralised logging facility.

### 18.5.9. New systems and networks

**18.5.9.R.01. Rationale**

Planning and accommodating changes in technology are an essential part of securing architectures and systems development.

**18.5.9.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Any network defence elements and devices MUST be IPv6 aware.

**18.5.9.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

New network devices, including firewalls, IDS and IPS, MUST be IPv6 capable.

**18.5.9.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider the use of DNSSEC.

### 18.5.10. Introducing IPv6 capable equipment to gateways

**18.5.10.R.01. Rationale**

Introducing IPv6 capable network devices into agency gateways can introduce a significant number of new security risks. Undergoing reaccreditation when new IPv6 equipment is introduced will ensure that any IPv6 functionality that is not intended to be used cannot be exploited by an attacker before appropriate information security mechanisms have been put in place.

**18.5.10.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

IPv6 tunnelling MUST be blocked by network security devices at externally connected network boundaries.

**18.5.10.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies deploying IPv6 equipment in their gateway but not enabling the functionality SHOULD undergo reaccreditation.

### 18.5.11. Enabling IPv6 in gateways

#### 18.5.11.R.01. Rationale

Once agencies have completed the transition to a dual-stack environment or completely to an IPv6 environment, reaccreditation will assist in ensuring that the associated information security mechanisms for IPv6 are working effectively.

#### 18.5.11.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies enabling a dual-stack environment or a wholly IPv6 environment in their gateways MUST reaccredit their gateway systems.

# 18.6.Peripheral (KVM) Switches

## Objective

18.6.1. An evaluated peripheral switch is used when sharing keyboards, monitors and mice or other user interface devices, between different systems.

## Context

### Scope

18.6.2. This section covers information relating specifically to the use of keyboard/video/mouse (KVM) switches.

18.6.3. It is important to recognise that any cross-connection of system must be carefully controlled in order not to compromise trust zones. The principles of separation and segregation must be applied. These principles are discussed in section 22.1 – Cloud Computing and section 22.2 – Virtualisation.

18.6.4. Cross-connection of system may also functionally create a gateway, whether or not it meets the technical definition of gateways. It is important to refer to section 19.1 – Gateways and section 19.2 – Cross Domain Solutions.

### Peripheral switches with more than two connections

18.6.5. If the peripheral switch has more than two systems connected then the level of assurance needed is determined by the highest and lowest of the classifications involved.

### Electrical Safety

18.6.6. Electrical safety is paramount. Cross-connecting systems may create ground loops if different power sources are used for different elements of the computer system. This may result in catastrophic failure if power supplies connected to different phases are cross-connected.

### Product Assurance

18.6.7. Product assurance is discussed in Chapter 12- Product Security It is important to note the role of the Common Criteria, the related CCRA and the use of assurance levels in determining product assurance. Chapter 12 also provides essential reference to assurance levels, evaluation levels and defines high assurance as shown in the table at 18.6.8 Assurance Requirements.

## Rationale & Controls

### 18.6.8. Assurance requirements

**18.6.8.R.01. Rationale**

When accessing multiple systems through a peripheral switch it is important that sufficient assurance is available in the operation of the switch to ensure that information does not accidently pass between the connected systems.

**18.6.8.R.02. Rationale**

It is important to maintain the integrity of Trust Zones and adhere to the principles of separation and segregation in order to avoid inadvertently compromising Trust Zones – even if they are at the same level of classification.

**18.6.8.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies accessing a classified system and a less classified system via a peripheral switch MUST use an evaluated product with a level of assurance as indicated in the table below.

| High system | Low system/ Alternate Trust Domain | Required level of assurance |
|---|---|---|
| **RESTRICTED & all lower classifications** | UNCLASSIFIED | EAL2 or PP |
| **CONFIDENTIAL** | UNCLASSIFIED | high assurance |
| | RESTRICTED | high assurance |
| | CONFIDENTIAL | high assurance |
| **SECRET** | UNCLASSIFIED | high assurance |
| | RESTRICTED | high assurance |
| | CONFIDENTIAL | high assurance |
| | SECRET | high assurance |
| **TOP SECRET** | UNCLASSIFIED | high assurance |
| | RESTRICTED | high assurance |
| | CONFIDENTIAL | high assurance |
| | SECRET | high assurance |
| | TOP SECRET | high assurance |

### 18.6.9. Assurance requirements for NZEO systems

**18.6.9.R.01. Rationale**

NZEO systems are particularly sensitive. Additional security measures need to be put in place when connecting them to other systems.

**18.6.9.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies accessing a system containing NZEO information and a system of the same classification that is not accredited to process NZEO information, MUST use an evaluated product with an EAL2 (or higher) or a PP level of assurance.

### 18.6.10. Cross-Connecting Systems with a device other than a KVM

**18.6.10.R.01. Rationale**

Cross-connecting systems with any device other than a KVM approved gateway or an approved cross-domain solution may be high risk, may compromise the integrity of Trust Zones, and may create an electrical hazard.

**18.6.10.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Cross-connection of security domains and Trust Zones MUST be enabled through an approved KVM, Gateway or Cross-Domain solution only.

# 19. Gateway security

## 19.1. Gateways

### Objective

19.1.1. To ensure that gateways are properly configured to protect agency systems and information transferred between systems from different security domains.

### Context

#### Scope

19.1.2. Gateways can be considered to be information flow control mechanisms operating at the Network layer and may also control information flow at the Transport, Session, Presentation and Application layers of the Open Systems Interconnection model (OSI). Specific controls for different technologies can be found in Section 19.3 –Firewalls, Section 19.4 – Diodes, Section 18.6 – Peripheral (KVM) switches and Section 19.5 – Session Border Controllers.

19.1.3. Additional information relating to topics covered in this section can be found in the following sections of this manual:

- Section 4.4 – Accreditation Framework;
- Section 8.2 – Servers and Network Devices;
- Section 8.3 – Network Infrastructure;
- Section 8.4 – IT Equipment;
- Chapter 12 – Product Security;
- Section 16.1 – Identification and Authentication;
- Section 16.5 – Event Logging and Auditing;
- Section 19.3 – Firewalls;
- Section 19.4 – Diodes;
- Section 19.5 – Session Border Controllers;
- Section 20.1 – Data Transfers;
- Section 20.2 – Data Import and Export; and
- Section 20.3 – Content Filtering.

### Deploying gateways

19.1.4. This section provides a baseline for agencies deploying gateways. Agencies will need to consult additional sections of this manual depending on the specific type of gateways deployed.

19.1.5. For network devices used to control data flow in bi-directional gateways, Section 19.3 – Firewalls will need to be consulted. Section 19.4 – Diodes will also need to be consulted for one-way gateways. Additionally, for both types of gateways, Section 20.1 - Data Transfers and Section 19.2 - Cross-Domain Solutions, will need to be consulted for requirements on appropriately controlling data flows.

19.1.6. The requirements in this manual for content filtering, data import and data export apply to all types of gateways.

### Gateway classification

19.1.7. For the purposes of this chapter, the gateway assumes the highest classification of the connected domains.

## References

19.1.8. Further references can be found at:

| Title | Publisher | Source |
|---|---|---|
| **ISO/IEC 27033-4:2014**<br>**Information technology -- Security techniques -- Network security -- Part 4: Securing communications between networks using security gateways** | ISO | Revising ISO/IEC 18028-3:2005<br>http://www.iso.org |
| **Gateway / Cross Domain Solution Audit Guide, Australian Government** | ASD | http://www.asd.gov.au/publications/Gateway_CDS_Audit_Guide.docx |
| **Guidelines on Firewalls and Firewall Policy, NIST SP800-41,** | NIST | http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf |
| **Good Practices for deploying DNSSEC, ENISA** | ENISA | http://www.enisa.europa.eu/activities/Resilience-and-CIIP/networks-and-services-resilience/dnssec/gpgdnssec |
| **The OSI model**<br>**ISO/IEC 7498-1:1994**<br>**Information Technology – Open Systems Interconnection: The Basic Model** | ISO / IEC | http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html |

## PSR references

19.1.9. Relevant PSR requirements can be found at:

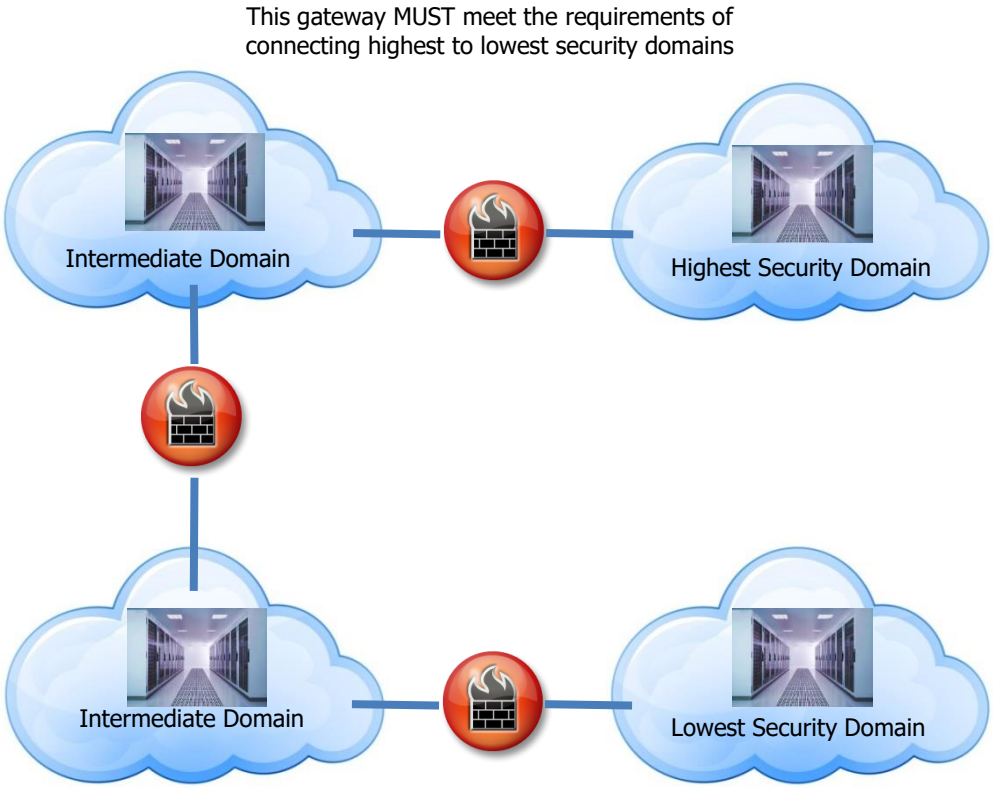
| Reference | Title | Source |
|---|---|---|
| **PSR Mandatory Requirements** | GOV5, GOV6, INFOSEC1, INFOSEC2, INFOSEC3 and INFOSEC4 | http://www.protectivesecurity.govt.nz |
| **PSR content protocols** | Management protocol for information security | http://www.protectivesecurity.govt.nz |
| **PSR requirements sections** | Handling requirements for protectively marked information and equipment<br>Supply chain security<br>Understand your information security measures | http://www.protectivesecurity.govt.nz |
| **Managing specific scenarios** | Outsourced ICT facilities<br>Outsourcing, Offshoring and supply chains<br>Physical security for ICT systems<br>Communication security<br>Transacting online with the public | http://www.protectivesecurity.govt.nz |

## Rationale & Controls

### 19.1.10. Gateways involving cascaded connections

#### 19.1.10.R.01. Rationale

Protecting a cascaded connection path with the minimum assurance requirement of a direct connection between the highest and lowest networks ensures appropriate reduction in security risks of the extended connection. An illustration of a cascaded connection can be seen below.




#### 19.1.10.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

When agencies have cascaded connections between networks involving multiple gateways they MUST ensure that the assurance levels specified for network devices between the overall lowest and highest networks are met by the gateway between the highest network and the next highest network within the cascaded connection.

### 19.1.11. Using gateways

**19.1.11.R.01. Rationale**

Physically locating all gateway components inside a secure server room will reduce the risk of unauthorised access to the device(s).

**19.1.11.R.02. Rationale**

The system owner of the higher security domain of connected security domains would be most familiar with the controls required to protect the more sensitive information and as such is best placed to manage any shared components of gateways. In some cases where multiple security domains from different agencies are connected to a gateway, it may be more appropriate to have a qualified third party manage the gateway on behalf of all connected agencies.

Gateway components may also reside in a virtual environment – refer to Section 22.2 – Virtualisation and Section 22.3 – Virtual Local Area Networks.

**19.1.11.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that:

- all agency networks are protected from networks in other security domains by one or more gateways;
- all gateways contain mechanisms to filter or limit data flow at the network and content level to only the information necessary for business purposes; and
- all gateway components, discrete and virtual, are physically located within an appropriately secured server room.

**19.1.11.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

For gateways between networks in different security domains, any shared components MUST be managed by the system owners of the highest security domain or by a mutually agreed party.

### 19.1.12. Configuration of gateways

**19.1.12.R.01. Rationale**

Gateways are essential in controlling the flow of information between security domains. Any failure, particularly at the higher classifications, may have serious consequences. Hence mechanisms for alerting personnel to situations that may give rise to information security incidents are especially important for gateways.

**19.1.12.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that gateways:

- are the only communications paths into and out of internal networks;
- by default, deny all connections into and out of the network;
- allow only explicitly authorised connections;
- are managed via a secure path isolated from all connected networks (i.e. physically at the gateway or on a dedicated administration network);
- provide sufficient logging and audit capabilities to detect information security incidents, attempted intrusions or anomalous usage patterns; and
- provide real-time alerts.

### 19.1.13. Operation of gateways

**19.1.13.R.01. Rationale**

Providing an appropriate logging and audit capability will help to detect information security incidents and attempted network intrusions, allowing the agency to respond and to take measures to reduce the risk of future attempts.

**19.1.13.R.02. Rationale**

Storing event logs on a separate, secure log server will assist in preventing attackers from deleting logs in an attempt to destroy evidence of any intrusion.

**19.1.13.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that all gateways connecting networks in different security domains:

- include a firewall of an appropriate assurance level on all gateways to filter and log network traffic attempting to enter the gateway;
- are configured to save event logs to a separate, secure log server;
- are protected by authentication, logging and audit of all physical access to gateway components; and
- have all controls tested to verify their effectiveness after any changes to their configuration.

### 19.1.14. Demilitarised zones

**19.1.14.R.01. Rationale**

Demilitarised zones are used to prevent direct access to information and systems on internal agency networks. Agencies that require certain information and systems to be accessed *from* the Internet or some other form of remote access, should place them in the less trusted demilitarised zone instead of on internal agency networks.

**19.1.14.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST use demilitarised zones to house systems and information directly accessed externally.

**19.1.14.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use demilitarised zones to house systems and information directly accessed externally.

### 19.1.15. Risk assessment

**19.1.15.R.01. Rationale**

Performing a risk assessment on the gateway and its configuration prior to its implementation will assist in the early identification and mitigation of security risks.

**19.1.15.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST perform a risk assessment on gateways and their configuration *prior* to their implementation.

### 19.1.16. Risk transfer

**19.1.16.R.01. Rationale**

Gateways could connect networks with different domain owners, including across agency boundaries. As a result, all domain and system owners MUST understand and accept the risks from all other networks before gateways are implemented.

**19.1.16.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

All domain and system owners connected through a gateway MUST understand and accept the residual security risk of the gateway and from any connected domains including those via a cascaded connection.

**19.1.16.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD annually review the security architecture of the gateway and risks of all connected domains including those via a cascaded connection.

### 19.1.17. Information stakeholders and Shared Ownership

**19.1.17.R.01. Rationale**

Changes to a domain connected to a gateway can affect the security posture of other connected domains. All domains owners should be considered stakeholders in all connected domains.

**19.1.17.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Once connectivity is established, domain owners MUST be considered information stakeholders for all connected domains.

**19.1.17.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Once connectivity is established, domain owners SHOULD be considered information stakeholders for all connected domains.

### 19.1.18. System user training

**19.1.18.R.01. Rationale**

It is important that system users are competent to use gateways in a secure manner. This can be achieved through appropriate training before being granted access.

**19.1.18.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

All system users MUST be trained on the secure use and security risks of the gateways before being granted access.

**19.1.18.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

All system users SHOULD be trained in the secure use and security risks of the gateways before being granted access.

### 19.1.19. Administration of gateways

**19.1.19.R.01. Rationale**

Application of role separation and segregation of duties in administration activities will protect against security risks posed by a malicious system user with extensive access to gateways.

**19.1.19.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST limit access to gateway administration functions.

**19.1.19.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that system administrators are formally trained to manage gateways by qualified trainers.

**19.1.19.C.03. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that all system administrators of gateways that process NZEO information meet the nationality requirements for these endorsements.

**19.1.19.C.04. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST separate roles for the administration of gateways (e.g. separate network and security policy configuration roles).

**19.1.19.C.05. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD separate roles for the administration of gateways (e.g. separate network and security policy configuration roles).

### 19.1.20. System user authentication

**19.1.20.R.01. Rationale**

Authentication to networks as well as gateways can reduce the risk of unauthorised access and provide an audit capability to support the investigation of information security incidents.

**19.1.20.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST authenticate system users to all classified networks accessed through gateways.

**19.1.20.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that only authenticated and authorised system users can use the gateway.

**19.1.20.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use multi-factor authentication for access to networks and gateways.

### 19.1.21. IT equipment authentication

**19.1.21.R.01. Rationale**

Authenticating IT equipment to networks accessed through gateways will assist in preventing unauthorised IT equipment connecting to a network.

**19.1.21.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD authenticate any IT equipment that connects to networks accessed through gateways.

### 19.1.22. Configuration control

**19.1.22.R.01. Rationale**

To avoid changes that may introduce vulnerabilities into a gateway, agencies should fully consider any changes and associated risks. Changes may also necessitate re-certification and accreditation of the system, see Chapter 4 – System Certification and Accreditation.

**19.1.22.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST undertake a risk assessment and update the SRMP before changes are implemented.

**19.1.22.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST document any changes to gateways in accordance with the agency's Change Management Policy.

**19.1.22.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD undertake a risk assessment and update the SRMP before changes are implemented.

### 19.1.23. Testing of gateways

**19.1.23.R.01. Rationale**

The testing of security measures on gateways will assist in ensuring that the integrity of the gateway is being maintained. An attacker who is aware of the regular testing schedule may cease malicious activities during such periods to avoid detection. Any test should, therefore, be unannounced and conducted at irregular intervals.

**19.1.23.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that testing of security measures is performed at random intervals no more than six months apart.

# 19.2. Cross Domain Solutions (CDS)

## Objective

19.2.1. Cross-Domain Solutions secure transfers between systems of differing classifications or trust levels with high assurance over the security of systems and information.

## Context

### Scope

19.2.2. This section describes the use and implementation of Cross Domain Solutions (CDS).

19.2.3. CDS provide information flow control mechanisms at each layer of the OSI model with a higher level of assurance than typical gateways. This section extends the preceding Gateways section. CDS systems must apply controls from each section.

19.2.4. Additional information relating to topics covered in this section can be found in the following chapters and sections:

- Section 4.4 – Accreditation Framework;
- Section 8.2 – Servers and Network Devices;
- Section 8.3 – Network Infrastructure;
- Section 8.4 – IT Equipment;
- Chapter 12 – Product Security;
- Section 16.1 – Identification and Authentication;
- Section 16.5 – Event Logging and Auditing;
- Section 19.1 – Gateways;
- Section 19.3 – Firewalls;
- Section 19.4 – Diodes;
- Section 19.5 – Session Border Controllers;
- Section 20.1 – Data Transfers;
- Section 20.2 – Data Import and Export; and
- Section 20.3 – Content Filtering.

### Deploying Cross Domain Solutions

19.2.5. Consult the section on Firewalls in this chapter for devices used to control data flow in bi-directional gateways.

19.2.6. Consult the section on Diodes in this chapter for devices used to control data flow in uni-directional gateways.

19.2.7. Consult the Data Transfers and Content Filtering sections for requirements on appropriately controlling data flows in both bi-directional and uni-directional gateways

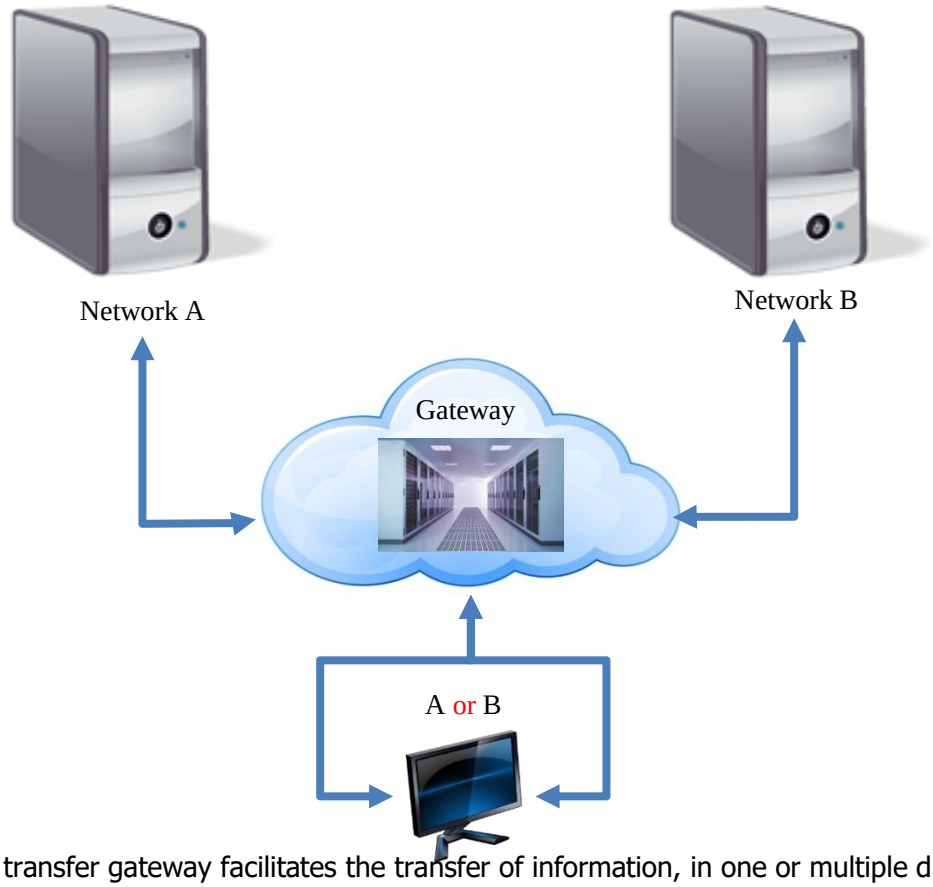
### Types of gateways

19.2.8. This manual defines three types of gateways:

- access gateways;
- multilevel gateways; and
- transfer gateways.

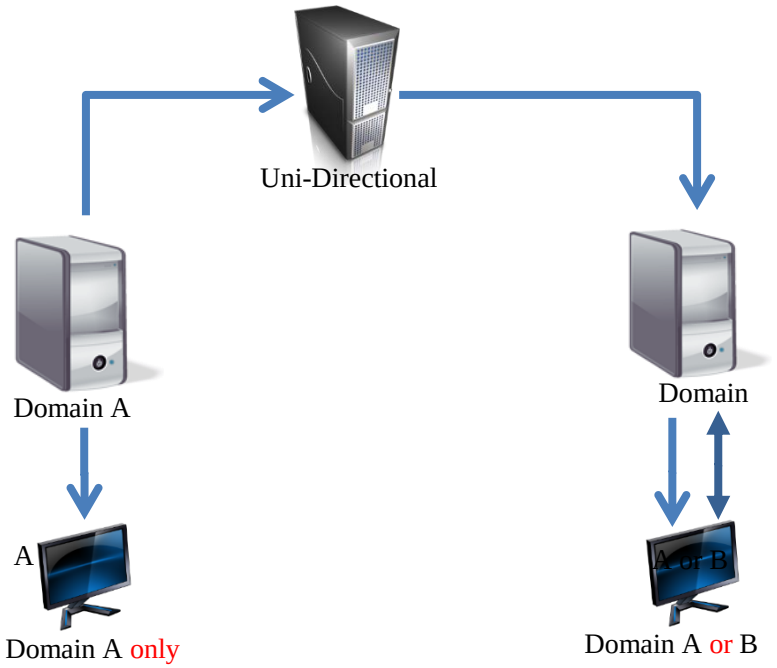
### Access Gateway

19.2.9. An access gateway provides the system user with access to multiple security domains from a single device.

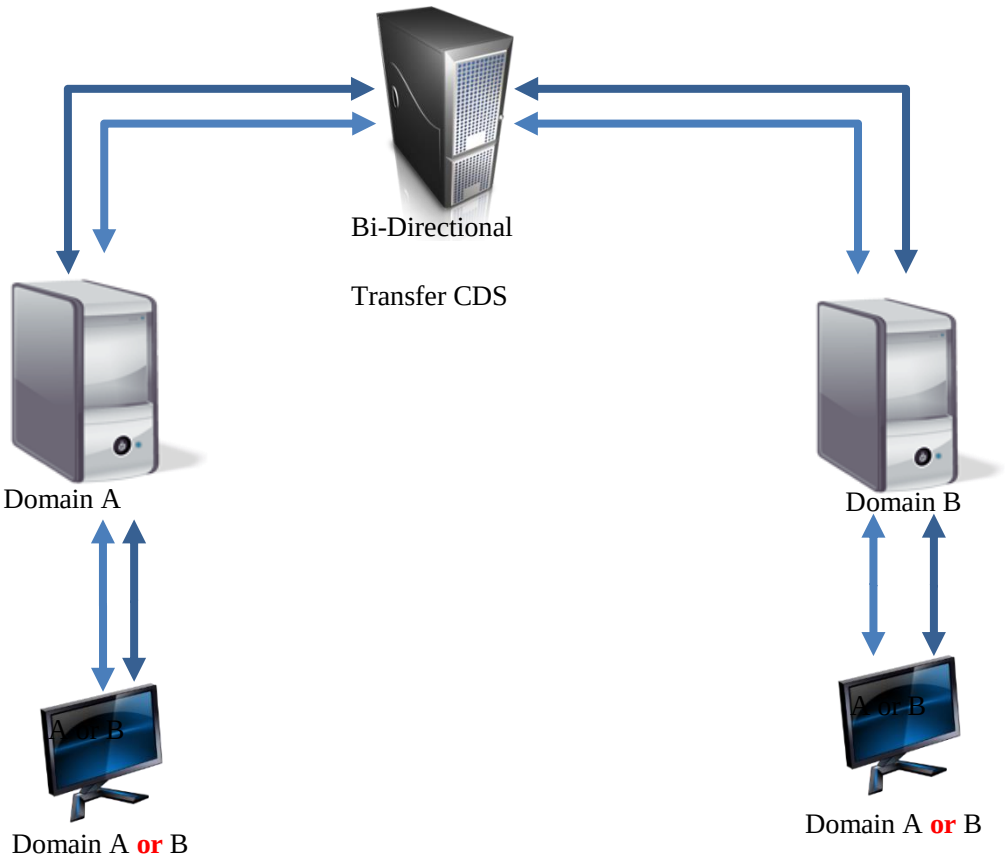



19.2.10. A transfer gateway facilitates the transfer of information, in one or multiple directions (low to high or high to low) between different security domains. A traditional gateway to the Internet is considered a form of transfer gateway.

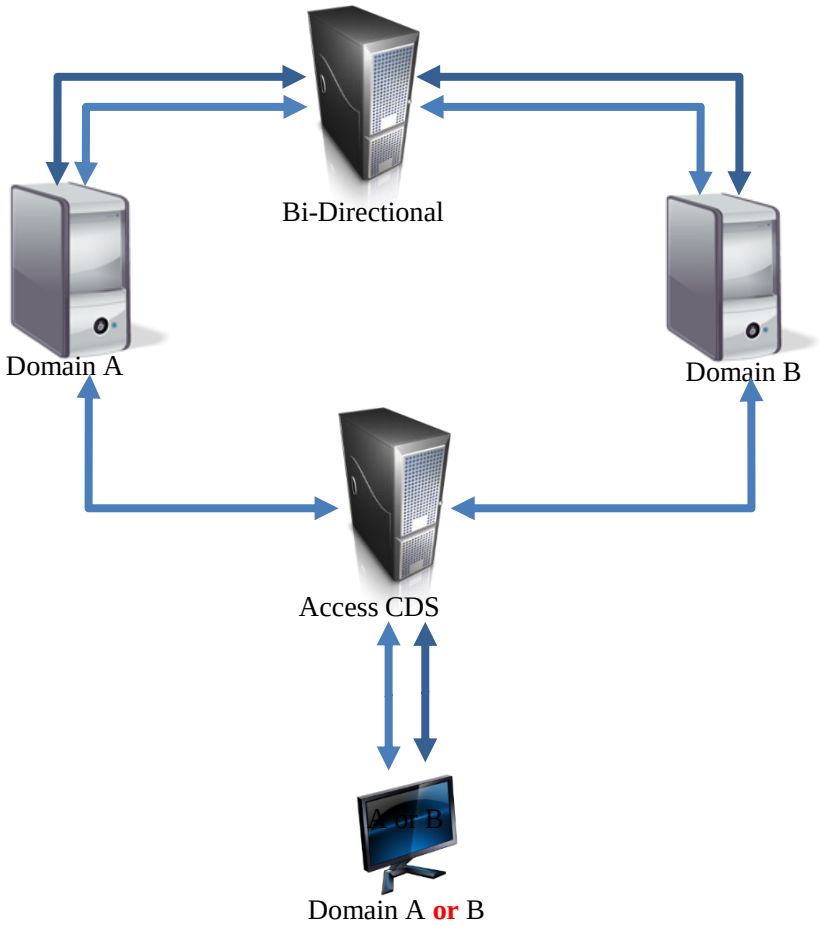
19.2.11. The following illustrates a Uni-Directional Transfer Cross Domain Solution.




19.2.12. A Bi-Directional Cross Domain Solution enables access, based on authorisations, to data at multiple classifications and releasability levels.



19.2.13. A Multi-Level Transfer Cross Domain Solution enables access, based on authorisations, to data at multiple classifications and releasability levels.



## References

19.2.14. Additional guidance can be found at:

| Title | Publisher | Source |
|---|---|---|
| **Information Assurance Guidance For Systems Based On A Security Real-Time Operating System Systems Security Engineering, Sse-100-1, 14 December 2005** | NSA | http://www.nsa.gov/ia/_files/SSE-100-1.pdf |
| **Solving the Cross-Domain Conundrum,** **Colonel Bernard F. Koelsch United States Army, 2013** | US Army War College | http://handle.dtic.mil/100.2/ADA589325 |
| **Client Side Cross-Domain Security,** **Microsoft Corporation June 2008** | Microsoft | https://msdn.microsoft.com/en-us/library/cc709423(v=vs.85).aspx |
| **Secure Cross Domain Solution** | Detica, BAE Systems | https://www.apm.org.uk/sites/default/files/protected/Secure%20Cross%20Domain%20Solutions%20v0.10c.pdf |
| **Cross Domain Security Primer** | CSE Canada | https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsb120-eng.pdf |
| **Shedding Light on Cross Domain Solutions** | SANS | https://www.sans.org/reading-room/whitepapers/dlp/shedding-light-cross-domain-solutions-36492 |

## Rationale & Controls

### 19.2.15. Gateway classification

**19.2.15.R.01. Rationale**

The trust level or classification of systems directs users and systems administrators to the appropriate handling instructions and level of protection required for those systems. This aids in the selection of systems controls.

**19.2.15.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

For the purposes of this Manual, the CDS MUST be classified at the highest classification of connected domains.

### 19.2.16. Allowable gateways

**19.2.16.R.01. Rationale**

Connecting systems to the Internet attracts significant risk and so highly classified systems are prohibited from being *directly* connected to each other or to the Internet. If an agency wishes to connect a highly classified system to the Internet the connection will need to be cascaded through a system of a lesser classification that is approved to connect directly to the Internet.

**19.2.16.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies connecting a TOP SECRET, SECRET OR CONFIDENTIAL network to any other network MUST implement a CDS.

**19.2.16.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST NOT

Agencies MUST NOT implement a gateway permitting data to flow *directly* from:

- a TOP SECRET network to any network below SECRET;
- a SECRET network to an UNCLASSIFIED network; or
- a CONFIDENTIAL network to an UNCLASSIFIED network.

### 19.2.17. Implementing Cross Domain Solutions

**19.2.17.R.01. Rationale**

Connecting multiple sets of gateways and Cross Domain Solutions (CDS) increases the threat surface and, consequently, the likelihood and impact of a network compromise. When a gateway and a CDS share a common network, the higher security domain (such as a classified agency network) can be exposed to malicious activity, exploitation or denial of service from the lower security domain (such as the Internet).

#### 19.2.17.R.02. Rationale

To manage this risk, CDS should implement products that have completed a high assurance evaluation, see Chapter 12 – Product Security. The AISEP Evaluated Product List (EPL) includes products that have been evaluated in the high assurance scheme but is not an exhaustive list.

Where CDS are not listed on the AISEP EPL, the GCSB can provide guidance on product selection and implementation on request.

#### 19.2.17.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

When designing and deploying a CDS, agencies MUST consult with the GCSB and comply with all directions provided.

#### 19.2.17.C.02. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies connecting a typical gateway and a CDS to a common network MUST consult the GCSB on the impact to the security of the CDS and comply with all directions provided.

### 19.2.18. Separation of data flows

#### 19.2.18.R.01. Rationale

Gateways connecting highly classified systems to lower classified, or Internet connected systems need to incorporate physically separate paths to provide stronger control of information flows. Typically this is achieved through separate pathing and the use of diodes. Such gateways are generally restricted to process and communicate only highly-structured formal messaging traffic.

#### 19.2.18.C.01. Control: System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST ensure that all bi-directional gateways between TOP SECRET and SECRET networks, SECRET and less classified networks, and CONFIDENTIAL and less classified networks, have separate upward and downward paths which use a diode and physically separate infrastructure for each path.

### 19.2.19. Trusted sources

**19.2.19.R.01. Rationale**

Trusted sources are designated personnel who have the delegated authority to assess and approve the transfer or release of data or documents. Trusted sources may include security personnel within the agency such the CISO and the ITSM.

**19.2.19.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Trusted sources MUST be:

- a strictly limited list derived from business requirements and the result of a security risk assessment;
- where necessary an appropriate security clearance is held; and
- approved by the Accreditation Authority.

**19.2.19.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST

Trusted sources MUST authorise all data to be exported from a security domain.

### 19.2.20. Operation of the Cross Domain Solution

**19.2.20.R.01. Rationale**

The highly sensitive nature of the data within cross domain solutions requires additional audit and logging for control, management, record and forensic purposes. This is in addition to the audit and logging requirements in Section 16.5 – Event Logging and Auditing.

**19.2.20.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

All data exported from a security domain MUST be logged.

# 19.3. Firewalls

## Objective

19.3.1. Agencies operating bi-directional gateways implement firewalls and traffic flow filters to provide a protective layer to their networks in both discrete and virtual environments.

## Context

### Scope

19.3.2. This section covers information relating to filtering requirements for bi-direction gateways between networks of different security domains.

19.3.3. When a control specifies a requirement for a diode or filter the appropriate information can be found within Section 19.4 –Diodes and Section 20.3 – Content Filtering.

19.3.4. Additional information that also applies to topics covered in the section can be found in:

- Chapter 12 – Product Security which provides advice on the selection of evaluated products;
- Section 20.1 – Data Transfers;
- Section 20.2 – Data Import and Export; and
- Section 22.2 – Virtualisation.

### Inter-connecting networks within an agency

19.3.5. When connecting networks accredited to the same classification and set of endorsements within an agency the requirements of this section may not apply. When connecting networks accredited with different classifications or endorsements within an agency the information in this section applies.

### Connecting agency networks to the Internet

19.3.6. When connecting an agency network to the Internet, the Internet is considered an UNCLASSIFIED and insecure network.

## References

19.3.7. Further information on the Network Device Protection Profile (NDPP) and firewalls can be found at:

| Title | Publisher | Source |
|---|---|---|
| **Network Device Protection Profile (NDPP)** | (US) National Information Assurance Partnership | http://www.niap-ccevs.org/pp/pp_nd_v1.0/ |

## Rationale & Controls

### 19.3.8. Firewall assurance levels

**19.3.8.R.01. Rationale**

The higher the required assurance level for a firewall, the greater the assurance that it provides an appropriate level of protection against an attacker. For example, an EAL2 firewall is certified to provide protection against a basic threat potential, whilst an EAL4 firewall is certified to provide protection against a moderate threat potential. A Protection Profile (PP) is considered to be equivalent to EAL2 under its Common Criteria Recognition Arrangement.

**19.3.8.R.02. Rationale**

If a uni-directional connection between two networks is being implemented only one gateway is necessary with requirements being determined based on the source and destination networks. However, if a bi-directional connection between two networks is being implemented both gateways will be configured and implemented with requirements being determined based on the source and destination networks.

**19.3.8.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

All gateways MUST contain a firewall in both physical and virtual environments.

**19.3.8.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST check the evaluation has examined the security enforcing functions by reviewing the target of evaluation/security target and other testing documentation.

**19.3.8.C.03. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST use devices as shown in the following table for their gateway when connecting two networks of different classifications or two networks of the same classification but of different security domains.

| Your network | Their network | You require | They require |
|---|---|---|---|
| RESTRICTED and below | UNCLASSIFIED | EAL4 firewall | N/A |
| | RESTRICTED | EAL2 or PP firewall | EAL2 or PP firewall |
| | CONFIDENTIAL | EAL2 or PP firewall | EAL4 firewall |
| | SECRET | EAL2 or PP firewall | EAL4 firewall |
| | TOP SECRET | EAL2 or PP firewall | Consultation with GCSB |
| CONFIDENTIAL | UNCLASSIFIED | Consultation with GCSB | N/A |
| | RESTRICTED | EAL4 firewall | EAL2 or PP firewall |
| | CONFIDENTIAL | EAL2 or PP firewall | EAL2 or PP firewall |
| | SECRET | EAL2 or PP firewall | EAL4 firewall |
| | TOP SECRET | EAL2 or PP firewall | Consultation with GCSB |
| SECRET | UNCLASSIFIED | Consultation with GCSB | N/A |
| | RESTRICTED | EAL4 firewall | EAL2 or PP firewall |
| | CONFIDENTIAL | EAL4 firewall | EAL2 or PP firewall |
| | SECRET | EAL2 or PP firewall | EAL2 or PP firewall |
| | TOP SECRET | EAL2 or PP firewall | EAL4 firewall |
| TOP SECRET | UNCLASSIFIED | Consultation with GCSB | N/A |
| | RESTRICTED | Consultation with GCSB | EAL2 or PP firewall |
| | CONFIDENTIAL | Consultation with GCSB | EAL2 or PP firewall |
| | SECRET | EAL4 firewall | EAL2 or PP firewall |
| | TOP SECRET | EAL4 firewall | EAL4 firewall |

**19.3.8.C.04. Control:** System Classification(s): All Classifications; Compliance: MUST

The requirement to implement a firewall as part of gateway architecture MUST be met separately and independently by both parties (gateways) in both physical and virtual environments.

Shared equipment DOES NOT satisfy the requirements of this control.

### 19.3.9. Firewall assurance levels for NZEO networks

**19.3.9.R.01. Rationale**

As NZEO networks are particularly sensitive, additional security measures need to be put in place when connecting them to other networks.

**19.3.9.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST use a firewall of at least an EAL4 assurance level between an NZEO network and a foreign network in addition to the minimum assurance levels for firewalls between networks of different classifications or security domains.

**19.3.9.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

In all other circumstances the table at 19.3.8.C.03 MUST apply.

**19.3.9.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use a firewall of at least an EAL2 assurance level or a Protection Profile between an NZEO network and another New Zealand controlled network within a single security domain.

# 19.4. Diodes

## Objective

19.4.1. Networks connected to one-way (uni-directional) gateways implement diodes in order to protect the higher classified system.

## Context

### Scope

19.4.2. This section covers information relating to filtering requirements for one-way gateways used to facilitate data transfers. Additional information that also applies to topics covered in the section can be found in:

- Chapter 12 – Product Security which provides advice on selecting evaluated products.
- Section 20.1 – Data Transfers; and
- Section 20.2 – Data Import and Export;

## References

19.4.3. Further information on the Evaluated Products List can be found at:

| Title | Publisher | Source |
|---|---|---|
| **Evaluated Products List (EPL)** | AISEP | http://www.asd.gov.au/infosec/epl/index.php |

## Rationale & Controls

### 19.4.4. Diode assurance levels

**19.4.4.R.01. Rationale**

A diode enforces one-way flow of network traffic thus requiring separate paths for incoming and outgoing data. As such, it is much more difficult for an attacker to use the same path to both launch an attack and release the information. Using diodes of higher assurance levels for higher classified networks provides an appropriate level of assurance to agencies that the specified security functionality of the product will operate as claimed.

**19.4.4.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST use devices as shown in the following table for controlling the data flow of one-way gateways between networks of different classifications.

| High network | Low network | You require |
|---|---|---|
| **RESTRICTED** | **UNCLASSIFIED** | **EAL2 or PP diode** |
| | **RESTRICTED** | **EAL2 or PP diode** |
| **CONFIDENTIAL** | **UNCLASSIFIED** | **high assurance diode** |
| | **RESTRICTED** | **high assurance diode** |
| | **CONFIDENTIAL** | **High assurance diode** |
| **SECRET** | **UNCLASSIFIED** | **high assurance diode** |
| | **RESTRICTED** | **high assurance diode** |
| | **CONFIDENTIAL** | **high assurance diode** |
| | **SECRET** | **high assurance diode** |
| **TOP SECRET** | **UNCLASSIFIED** | **high assurance diode** |
| | **RESTRICTED** | **high assurance diode** |
| | **CONFIDENTIAL** | **high assurance diode** |
| | **SECRET** | **high assurance diode** |
| | **TOP SECRET** | **high assurance diode** |

### 19.4.5. Diode assurance levels for NZEO networks

**19.4.5.R.01. Rationale**

As NZEO networks are particularly sensitive additional security measures are necessary when connecting them to other networks.

**19.4.5.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST use a diode of at least an EAL4 assurance level between an NZEO network and a foreign network in addition to the minimum assurance levels for diodes between networks of different classifications.

**19.4.5.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

In all other circumstances the table at 19.4.4.C.01 MUST apply.

**19.4.5.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use a diode of at least an EAL2 assurance level or a Protection Profile between an NZEO network and another New Zealand controlled network within a single security domain.

### 19.4.6. Volume Checking

**19.4.6.R.01. Rationale**

Monitoring the volume of data being transferred across a diode will ensure that it conforms to expectations. It can also alert the agency to potential malicious activity if the volume of data suddenly changes from the norm.

**19.4.6.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies deploying a diode to control data flow within one-way gateways SHOULD monitor the volume of the data being transferred.

# 19.5.Session Border Controllers

## Objective

19.5.1. To ensure the use of Session Border Controllers (SBCs) is integrated with the agency's security architecture and that use is consistent with other requirements for gateway security in this chapter.

## Context

### Scope

19.5.2. This section encompasses the use of SBCs in Voice over Internet Protocol (VoIP) and Unified Communication (UC) networks within an agency. It describes key risks and threats and provides guidance on the conceptual design of security for such systems.

19.5.3. It is important to note that Service Providers generally have operational objectives different to those of the agency and typically they will:

- Design a highly operationally optimised network requiring minimal maintenance;
- Provide resources, including SBCs, softswitches and media gateways that are shared between a number of customers (such as multi-tenanted data centres);
- The standard model may not accommodate all unique agency or NZ Government requirements which will then require special consideration.

19.5.4. Reference should also be made to the following sections:

- Chapter 6 – Information Security Monitoring;
- Chapter 7 – Information Security Incidents;
- Chapter 9 – Personnel Security;
- Chapter 11 – Communications Systems and Devices;
- Section 13.1.12 – Archiving;
- Chapter 16 – Access Control;
- Section 18.3 - Video & Telephony Conferencing and Internet Protocol Telephony.

**Definitions**

19.5.5. A **Session Border Controller** (**SBC**) is a device (physical or virtual) used in IP networks to control and manage the signalling and media streams of real-time UC and VoIP connections. See also Section 18.3 – Video & Telephony Conferencing and Internet Protocol Telephony. It includes establishing, controlling, and terminating calls, interactive media communications or other VoIP connections. SBCs enable VoIP traffic to navigate gateways and firewalls and ensure interoperability between different SIP implementations. Careful selection of SBCs will provide such functionality as prevention of toll fraud, resistance to denial of service attacks and resistance to eavesdropping.

19.5.6. **Unified Communications (UC)** is a term describing the integration of real-time and near real time communication and interaction services in an organisation or agency. UC may integrate several communication systems including unified messaging, collaboration, and interaction systems; real-time and near real-time communications; and transactional applications.

19.5.7. UC may, for example, include services such as instant messaging (chat), presence information, voice, mobility, audio, web & video conferencing, data sharing (such as interactive whiteboards), voicemail, e-mail, SMS and fax. UC is not necessarily a single product, but more usually a set of products designed to provide a unified user-interface and user-experience across multiple devices and media-types.

## Purpose

19.5.8. Traditional demarcation points, such as media gateways, are no longer natural boundaries. Older firewall technology impacts the performance of communications systems, including VoIP and UC. SBCs were introduced to improve performance and provide interoperability with real-time and near real-time communications. They provide a new natural demarcation point.

19.5.9. SBCs can provide a demarcation or normalisation point within the agency's network, allow enforcement of agency specific security policies and provide a greater degree of accountability than the usual contract with service providers.

## Risks and Threats

19.5.10. Risks and threats associated with the use of VoIP and UC include:

- Confidentiality (eavesdropping);
- Integrity (enabling fraud and theft as well as compromising privacy); and
- Availability (including Denial of Service [DoS or DDoS]).

### Confidentiality

19.5.11. There is a high likelihood of eavesdropping in VoIP systems**.** Traditional telephone systems require physical access to tap a line or compromise a PABX or switch. In VoIP networks, virtual LAN environments can be exploited remotely to identify weaknesses within and between virtual LANs and gain access to valuable information. Sniffing is another form of eavesdropping that involves capturing unencrypted voice traffic with malware or a specific VoIP sniffer tool. In common with other Internet connected systems, man-in-the-middle exploits are also used to eavesdrop on both data and VoIP networks.

### Integrity

19.5.12. Exploits such as caller ID spoofing are relatively easy to execute and can be extremely costly to businesses. Information from a stolen credit card or acquisition of other sensitive data, can compromise an employee's caller ID, and have funds transferred while posing as the employee. Cyber criminals can also change an employee's registration information in order to eavesdrop on or intercept all incoming calls for that individual.

19.5.13. Integrity compromise may include modification or insertion into UC. As many UC elements, such as voicemail or email, may encompass electronic records as defined in legislation it is vital that these elements are preserved unaltered.

### Availability

19.5.14. Because VoIP and UC places high levels of demand on any network, managing Quality of Service (QoS), latency, jitter, packet loss and other service impediments are important aspects of availability. In the event of major faults or outages, diversity and fault tolerance is vital for all key sites. To enable failover, for example, where calls leave the customer network, call diversity and call failover are essential configuration elements.

### Denial of Service

19.5.15. Denial of Service (DoS) attacks abuse signalling protocols to deny availability of VoIP data and degrade performance. If the telecommunications network is compromised, it is possible to also traverse systems to attack or infect the agency's data networks and other systems.

## Common VoIP and UC Security Risks and Threats

19.5.16. Common VoIP and UC security risks and threats.

| Risk | Typical Symptoms | Threat | Countermeasures |
|---|---|---|---|
| **Reconnaissance scan** | Address or port scan is used to footprint network topology | Targeted denial of service, fraud, theft | • Intrusion detection<br>• Protection against registration floods |
| **Man in the middle** | Attacker intercepts session to impersonate(spoof) caller | Targeted denial of service, breach of privacy, fraud, theft | • TLS encryption for SIP with separate TLS certificates for SIP Service Providers |
| **Eavesdropping** | Attacker "sniffs" session for the purpose of social engineering | Breach of privacy, fraud, theft | • Intrusion detection<br>• Encryption |
| **Session hijacking** | Attacker compromises valuable information by rerouting call | Breach of privacy, fraud, theft | • Intrusion detection |
| **Session overload** | Excessive signalling or media traffic(malicious, non-malicious) is experienced | Denial of service | • Protection against registration floods |
| **Protocol fuzzing** | Malformed packets, semantically or syntactically incorrect flows are encountered | Denial of service | • Malformed packet protection<br>• Protocol anomaly protection<br>• TCP reassembly for fragmented packet protection<br>• Strict TCP validation to ensure TCP session state enforcement, validation of sequence and acknowledgement numbers, rejection of bad TCP flag combinations |
| **Media injection** | Attacker inserts unwanted or corrupted content into messages compromising packet/data stream integrity | Denial of service, fraud | • Application aware firewalls<br>• Intrusion prevention /detection<br>• Encryption |
| **Toll Fraud** | Unexplained/unusual calling activity, increased costs/carrier | Fraud, financial loss, breach of privacy, information loss | • Application aware firewalls<br>• Intrusion prevention |

| Risk | Typical Symptoms | Threat | Countermeasures |
|---|---|---|---|
| | notification/alert | | /detection<br>• Encryption |

19.5.17. Encryption is discussed in Chapter 17.

## Product Selection

### Protection Profiles

19.5.18. One Protection Profile for SBCs has been published by NIAP (dated July 24, 2015 - see reference table). Several other Protection profiles (PPs) specifically for SBCs are in development but not yet published (as at September 2015). Gateway and other border control device PPs are used as surrogates in the interim. Refer to Chapter 12 – Product Security.

### Desirable SBC Functionality

19.5.19. To manage risks and threats and to safeguard performance there are a number of desirable features in an SBC. These include:

- Security – SBC DoS protection, access control, topology hiding, VPN separation, service infrastructure DoS prevention;
- Encryption – Support for Suite B encryption;
- Service Reach – surrogate registration IP PBX endpoints, SIP IMS-H.323 PBX IWF; VPN bridging;
- SLA assurance – admission control; bandwidth per VPN & site, session agent constraints, policy server; intra-VPN media release; QoS marking/mapping; QoS reporting;
- Fraud and Revenue protection – bandwidth policing, QoS theft protection, accounting, session timers;
- Regulatory compliance – provision of emergency service calls (111) & lawful intercept.

## Security Architecture

19.5.20. Typical use of session border controller in an agency gateway is illustrated in Figure 1 below:

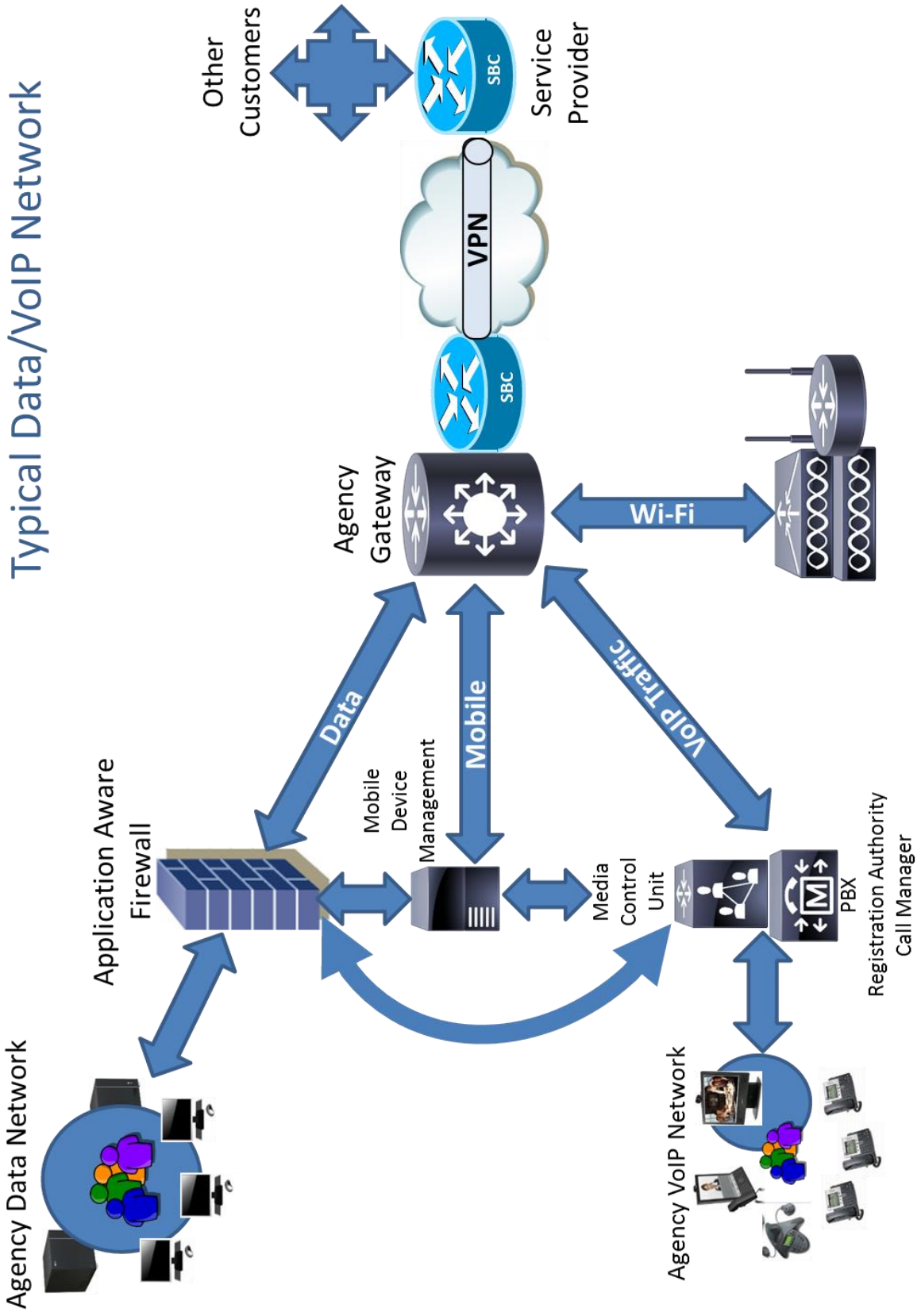



Figure: 1

## General References

19.5.21. Additional information on Session Border Controllers can be found in the following references:

| Reference | Title | Publisher | Source |
|---|---|---|---|
| **NIST SP 800-58** | Security Considerations for Voice Over IP Systems | NIST | http://csrc.nist.gov/publications/nistpubs/ |
| | Security Issues and Countermeasure for VoIP | SANS | http://www.sans.org/reading-room/whitepapers/voip/security-issues-countermeasure-voip-1701 |
| **Report Number: I332-016R-2005** | Security Guidance for Deploying IP Telephony Systems Released: 14 February 2006 | Systems and Network Attack Center (SNAC) NSA | https://www.nsa.gov/ia/_files/voip/i332-016r-2005.pdf |
| **Report Number: I332-009R-2006** | Recommended IP Telephony Architecture, Updated: 1May2006 Version1.0 | Systems and Network Attack Center (SNAC) NSA | https://www.nsa.gov/ia/_files/voip/I332-009R-2006.pdf |
| | Mobility Capability Package March 26 2012 - Secure VoIP Version 1.2 | NSA | https://www.nsa.gov/ia/_files/Mobility_Capability_Pkg_Vers_1_2.pdf |
| | Protecting Telephone-based Payment Card Data PCI Data Security Standard (PCI DSS) Version: 2.0, March 2011 | The PCI Security Standards Council (PCI SSC) | https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf |
| | Understanding Voice over Internet Protocol (VoIP): 2006 | US-CERT | https://www.us-cert.gov/sites/default/files/publications/understanding_voip.pdf |
| **CNSS Instruction No. 5000 April 2007** | Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony | Committee on National Security Systems | https://www.cnss.gov/CNSS/issuances/Instructions.cfm |
| | Infrastructure qualified for Microsoft Lync | Microsoft TechNet | https://technet.microsoft.com/en-us/office/dn788945.aspx |
| | A Guide to the Public Records Act | Archives New Zealand | http://records.archives.govt.nz/home/public-records-act-2005/ |
| **Public Act 2002 No.35** | Electronic Transactions Act 2002 | | http://www.legislation.govt.nz/act/public/2002/0035/latest/DLM154185.html |
| | Network Device Collaborative Protection Profile (NDcPP) Extended Package Session Border Controller, July 2015 | NIAP | https://www.niap-ccevs.org/pp/cpp_nd_sbc_ep_v1.0.pdf |
| | Protection Profile for Voice Over IP (VoIP) Applications, 3 November 2014, Version 1.3 | | https://www.niap-ccevs.org/pp/cpp_nd_sbc_ep_v1.0.pdf |
| | DHS 4300A Sensitive Systems Handbook Attachment Q5 To Handbook v. 11.0 Voice over Internet Protocol (VoIP) Version 11.0 December 22, 2014 | DHS | http://www.dhs.gov/sites/default/files/publications/4300A%20Handbook%20Attachment%20Q5%20-%20Voice%20over%20IP.pdf |
| | 2015 Global Fraud Loss Survey | CFCA | http://www.cfca.org/fraudlosssurvey |

## Media Technical References

19.5.22. Media technical references are listed below:

| Reference | Title | Publisher | Source |
|---|---|---|---|
| **RFC 2833** | RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals | IETF | www.ietf.org/ |
| **RFC 3313** | Private Session Initiation Protocol (SIP) Extensions for Media Authorization | IETF | www.ietf.org/ |
| **RFC 3550** | RTP: A Transport Protocol for Real-Time Applications | IETF | www.ietf.org/ |
| **RFC 3685** | Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP) | IETF | www.ietf.org/ |
| **RFC 3362** | Real-time Facsimile (T.38) - image/t38 MIME Sub-type Registration | IETF | www.ietf.org/ |
| **T.38 (09/2010)** | Procedures for real-time Group 3 facsimile communication over IP networks | International Telecommunication Union | http://www.itu.int/rec/T-REC-T.38/e |
| **V.150.1 (01/2003)** | Modem-over-IP networks: Procedures for the end-to-end connection of V-series DCEs | International Telecommunication Union | https://www.itu.int/rec/T-REC-V.150.1-200301-I/en |
| **G.711** | Pulse code modulation (PCM) of voice frequencies | International Telecommunication Union | http://www.itu.int/rec/T-REC-G.711/ |
| **G.726** | 40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM) | International Telecommunication Union | http://www.itu.int/rec/T-REC-G.726/e |
| **G. 729 (06/2012)** | Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction (CS-ACELP) | International Telecommunication Union | http://www.itu.int/rec/T-REC-G.729/e |

## Signalling Technical References

19.5.23. Signalling technical references are listed below:

| Reference | Title | Publisher | Source |
|---|---|---|---|
| **RFC 2705** | Media Gateway Control Protocol (MGCP) Version 1.0 | IETF | www.ietf.org/ |
| **RFC 3525** | Gateway Control Protocol Version 1.0 | IETF | www.ietf.org/ |
| **RFC 3261** | SIP: Session Initiation Protocol | IETF | www.ietf.org/ |
| **RFC 3263** | Locating SIP Servers | IETF | www.ietf.org/ |
| **draft-ietf-sip-session-timer** | SIP Session Timer | IETF | www.ietf.org/ |
| **RFC 3966** | The tel URI for Telephone Numbers | IETF | www.ietf.org/ |
| **RFC 3924** | Cisco Architecture for Lawful Intercept in IP Networks | IETF | www.ietf.org/ |
| **RFC 2327** | Session Description Protocol | IETF | www.ietf.org/ |
| **RFC 3025** | Gateway Control Protocol Version 1, June 2003 | IETF | www.ietf.org/ |
| **H.248 (03/2013)** | Media Gateway Control (Megaco): Version 3 | International Telecommunication Union | http://www.itu.int/rec/T-REC-H.248.1/en |
| **H.323 (12/2009)** | Packet-based multimedia communications systems | International Telecommunication Union | http://www.itu.int/rec/T-REC-H.323/en/ |
| **H.450** | Supplementary Services for H.323 | International Telecommunication Union | http://www.itu.int/ |
| **MSF Technical Report MSF-TR-QoS-001-FINAL** | Quality of Service for next generation VoIP networks framework | Multiservice Switching Forum | http://www.recursosvoip.com/docs/english/MSF-TR-QoS-001-FINAL.pdf |
| **ETSI TS 129 305 V8.0.0 (2009-01)** | Universal Mobile Telecommunications System (UMTS); LTE; InterWorking Function (IWF) between MAP based and Diameter based interfaces. | European Telecommunications Standards Institute | http://www.etsi.org/deliver/etsi_ts/129300_129399/129305/08.00.00_60/ts_129305v080000p.pdf |

## Rationale & Controls

### 19.5.24. Risk Assessment

**19.5.24.R.01. Rationale**

The adoption of Voice over Internet Protocol (VoIP) and Unified Communication (UC) networks will introduce a range of technology risks *in addition* to the technology and systems risks that already exist for agency systems. It is vital that these risks are identified and assessed in order to design a robust security architecture and to select appropriate controls and countermeasures.

**19.5.24.R.02. Rationale**

The availability of agency systems, business functionality and any customer or client online services, is subject to further risks in an outsourced environment. A risk assessment will include consideration of business requirements on availability in a VoIP and UC environment.

**19.5.24.R.03. Rationale**

Risks to business functionality may include service outages, such as communications, data centre power, backup and other failures or interruptions. Entity failures such as the merger, acquisition or liquidation of the service provider may also present a significant business risk to availability.

**19.5.24.R.04. Rationale**

Testing is a valuable tool when assessing risk. A UC environment with complex communications streams can provide opportunities for exploitation, especially where the configuration is weak or has itself been compromised. One of the fundamental tools is penetration testing.

**19.5.24.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies intending to adopt VoIP or UC technologies or services MUST conduct a comprehensive risk assessment *before* implementation or adoption.

**19.5.24.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies intending to adopt VoIP or UC technologies or services MUST consider the risks to the availability of systems and information in their design of VoIP and UC systems architecture, fault tolerance, fail over and supporting controls and governance processes.

**19.5.24.C.03. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure risks for any VoIP or UC service adopted are understood and formally accepted by the agency's Accreditation Authority as part of the Certification and Accreditation process (See Chapter 4).

**19.5.24.C.04. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies intending to adopt VoIP or UC technologies or services MUST determine where the responsibility (agency or VoIP and UC service provider) for implementing, managing and maintaining controls lies in accordance with agreed trust boundaries.

**19.5.24.C.05. Control:** System Classification(s): All Classifications; Compliance: MUST

Any contracts for the provision of VoIP or UC services MUST include service level, availability, recoverability and restoration provisions as formally determined by business requirements.

**19.5.24.C.06. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure contracts with VoIP or UC service providers include provisions to manage risks associated with the merger, acquisition, liquidation or bankruptcy of the service provider and any subsequent termination of VoIP or UC services.

**19.5.24.C.07. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies procuring or using VoIP or UC services to be used by multiple agencies MUST ensure all interested parties formally agree to the risks, controls and any residual risks of such VoIP and UC services. The lead agency normally has this responsibility (see Chapter 2 and Chapter 4).

**19.5.24.C.08. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider the use of assessment tools, such as penetration testing, when undertaking the risk assessment.

### 19.5.25. Non-Agency Networks

**19.5.25.R.01. Rationale**

Networks furnished by a service provider are invariably shared networks. Much of the security configuration is designed to maximise operational efficiency of the Service Providers network. Any agency specific security requirements may attract additional cost.

**19.5.25.R.02. Rationale**

It is preferable to maintain an agency designed and controlled gateway to ensure security requirements are properly accommodated. The use of SBCs should be carefully considered in order to maximise efficiency consistent with security requirements.

**19.5.25.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST follow the gateway requirements described in Chapter 19.

### 19.5.26. Security Architecture and Configuration

**19.5.26.R.01. Rationale**

Trust boundaries must be defined to assist in determining effective controls and where these controls can best be applied. Trust zones and trust boundaries are discussed in 22.1.3. The use of SBCs will assist with the definition of trust boundaries and allow the segregation of UC and normal data.

**19.5.26.R.02. Rationale**

The threat model for IP is well understood. Data packets can be intercepted or eavesdropped anywhere along the transmission path including the corporate network, by the internet service provider and along the backbone. The prevalence and ease of packet sniffing and other techniques for capturing packets on an IP based network increases this threat level. VoIP Encryption is an effective means of mitigating this threat.

**19.5.26.R.03. Rationale**

The nature of traffic through an SBC is an important factor in determining the type and configuration of the SBC. This also plays an important role in determining the resilience of the system. Systems may require high availability (HA), depending on business requirements for availability and continuity of service. The use of split trunks for HA normal traffic may provide resilience at reduced costs.

**19.5.26.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies intending to adopt VoIP or UC technologies or services MUST determine trust boundaries *before* implementation.

**19.5.26.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Updates to the SBC and related devices MUST be verified by the administrator to ensure they are obtained from a trusted source and are unaltered.

**19.5.26.C.03. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST include defence mechanisms for the Common VoIP and UC Security Risks and Threats described in 19.5.10 above.

**19.5.26.C.04. Control:** System Classification(s): All Classifications; Compliance: MUST

Agency networks MUST ensure the SBC includes a topology hiding capability.

**19.5.26.C.05. Control:** System Classification(s): All Classifications; Compliance: MUST

Agency networks MUST consider the use of call diversity and call failover configurations.

**19.5.26.C.06. Control:** System Classification(s): All Classifications; Compliance: MUST

In a virtualised environment, agencies MUST ensure any data contained in a protected resource is deleted or not available when the virtual resource is reallocated.

**19.5.26.C.07. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD conduct a traffic analysis to ensure the agency's network and architecture is capable of supporting all VoIP, media and UC traffic. The traffic analysis SHOULD also determine any high availability requirements.

**19.5.26.C.08. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD design a security and gateway architecture that segregates UC and normal data traffic. Firewall requirements (Section 19.3) continue to apply to data traffic.

**19.5.26.C.09. Control:** System Classification(s): All Classifications; Compliance: SHOULD

In a virtualised environment, agencies SHOULD create separate virtual LANs for data traffic and UC traffic.

**19.5.26.C.010. Control:** System Classification(s): All Classifications; Compliance: SHOULD

In a non-virtualised environment, agencies SHOULD create separate LANs for data traffic and UC traffic.

**19.5.26.C.011. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agency networks SHOULD use encryption internally on VoIP and unified communications traffic.

**19.5.26.C.012. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agency networks SHOULD ensure intrusion prevention systems and firewalls are VoIP-aware.

### 19.5.27. Access Control

**19.5.27.R.01. Rationale**

Network access control and password requirements are described in Chapter 16, in particular 16.5 – Event Logging and Auditing. Event logging helps improve the security posture of a system by increasing the accountability of all user actions, thereby improving the chances that malicious behaviour will be detected and assist in the investigation of incidents. A fundamental of access control is to manage access rights including physical access, file system and data access permissions and programme execution permissions. In addition, access control provides a record of usage in the event of an incident. Retention of records and archiving is discussed in Section 13.1.12.

**19.5.27.R.02. Rationale**

Similar requirements apply to VoIP and UC networks as these are also IP based. This will include any service enabled as part of the UC environment, such as Chat, IM, video and teleconferencing.

**19.5.27.R.03. Rationale**

There may be special cases, such as a 24x7 operations centre, where VoIP phones are shared by several duty officers on a shift basis. Workloads may require a number of duty personnel at any one time. In such cases it may be impractical to allocate individual VoIP or UC UserID and passwords. The risks in such cases must be clearly identified and compensating controls applied to ensure traceability in the event of fault finding or an incident. Examples of compensating controls include physical access control, CCTV, and duty registers. Identification of shared facilities is important and may comprise a UserID such as "Duty Officer", SOC, or agency name in a multi-agency facility.

**19.5.27.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Any shared facilities MUST be clearly identifiable both physically and logically.

**19.5.27.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST provide a protected communication channel for administrators, and authorised systems personnel. Such communication MUST be logged.

**19.5.27.C.03. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure administrative access to the SBC is available only through a trusted LAN and secure communication path.

**19.5.27.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Access control and password requirements SHOULD apply to VoIP and UC networks in all cases where individual access is granted.

**19.5.27.C.05. Control:** System Classification(s): All Classifications; Compliance: SHOULD

In special cases where individual UserIDs and Passwords are impractical, a risk assessment SHOULD be completed and compensating controls applied.

**19.5.27.C.06. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Event logs covering all VoIP and UC services SHOULD be maintained in accordance with the requirements of the NZISM. See section 16.5 Event Logging and Auditing and 13.1.12 Archiving.

### 19.5.28. Incident Handling and Management

**19.5.28.R.01. Rationale**

Service providers may not provide the same level of incident identification and management as provided by agencies. In some cases, these services will attract additional costs. Careful management of contracts is required to ensure agency requirements for incident detection and management are fully met when adopting VoIP and UC services.

**19.5.28.R.02. Rationale**

Blacklisting allows blocking of calls to specific numbers, range of numbers or countries. Whitelisting specifically allows calls to numbers, range of numbers or countries. A combination of black and white listing enables a flexible method of preventing call fraud (hijacking and "call pumping") where forbidden destinations are blacklisted and exceptions are whitelisted. This, for example, allows calls to a specific number within a forbidden country.

**19.5.28.R.03. Rationale**

Call Rate Limiting allows the restriction of outbound call volumes to specific numbers, range of numbers or countries. This is a useful mitigation for "traffic pumping" call fraud schemes. Call rate limiting also allows temporary limits to be placed on call from or to particular destinations while a security incident is investigated.

**19.5.28.R.04. Rationale**

Call Redirection enables the transfer of blocked calls to another destination including via monitoring and recording systems. Blocked calls may be dropped or a message played indicating, for example, that calls cannot be connected.

**19.5.28.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST include incident handling and management services in contracts with service providers.

**19.5.28.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop and implement incident identification and management processes in accordance with this manual (See Chapter 6 – Information Security Monitoring, Chapter 7 – Information Security Incidents, Chapter 9 – Personnel Security and Chapter 16 – Access Control).

**19.5.28.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD implement fraud detection monitoring to identify suspicious activity and provide alerting so that remedial action can be taken.

**19.5.28.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD regularly review call detail records for patterns of service theft.

**19.5.28.C.05. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider the use of blacklisting and whitelisting to manage fraudulent calls to known fraudulent call destinations.

**19.5.28.C.06. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider the use of call rate limiting as a fraud mitigation measure.

**19.5.28.C.07. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider the use of call redirection to manage blocked calls.

### 19.5.29. User Awareness and Training

**19.5.29.R.01. Rationale**

The introduction of VoIP and UC services will introduce change to the appearance and functionality of systems, how users access agency systems and types of user support. It is essential that users are aware of information security and privacy concepts and risks associated with the services they use.

Support provided by the VoIP and UC service provider may attract additional charges.

**19.5.29.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop and implement user awareness and training programmes to support and enable safe use of VoIP and UC services (See Section 9.1 – Information Security Awareness and Training).

# 20. Data management

## 20.1. Data Transfers

### Objective

20.1.1. Data transfers between systems are controlled and accountable.

### Context

**Scope**

20.1.2. This section covers the fundamental requirements of data transfers between systems and applies equally to data transfers using removal media and to data transfers via gateways.

20.1.3. Additional requirements for data transfers using removal media can be found in the Section 13.3 – Media Usage and additional requirements for data transfers via gateways can be found in the Section 20.2 – Data Import and Export.

20.1.4. Transfers from a classified system where strong information security controls exist to a system of lower classification where controls may not be as robust, can lead to data spills, information loss and privacy breaches. It is important that appropriate levels of oversight and accountability are in place to minimise or prevent the undesirable loss or leakage of information.

### PSR references

20.1.5. Relevant PSR requirements can be found at:

| Reference | Title | Source |
|---|---|---|
| **PSR Mandatory Requirements** | GOV2, GOV6, INFOSEC1, INFOSEC2, INFOSEC3 and INFOSEC4, PERSEC1, PERSEC2, PERSEC3 and PERSEC4 | http://www.protectivesecurity.govt.nz |
| **PSR content protocols** | Management protocol for information security<br>Management protocol for personnel security | http://www.protectivesecurity.govt.nz |
| **PSR requirements sections** | Classify and assign protective markings<br>Understand the information security lifecycle | http://www.protectivesecurity.govt.nz |
| **Managing specific scenarios** | Transacting online with the public | http://www.protectivesecurity.govt.nz |

## Rationale & Controls

### 20.1.6. User responsibilities

**20.1.6.R.01. Rationale**

When users transfer data to and from systems they need to be aware of the potential consequences of their actions. This could include data spills of classified information onto systems not accredited to handle the classification of the data or the unintended introduction of malicious code. Accordingly agencies will need to hold personnel accountable for all data transfers that they make.

**20.1.6.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST establish a policy and train staff in the processes for data transfers between systems and the authorisations required before transfers can take place.

**20.1.6.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that system users transferring data to and from a system are held accountable for the data they transfer.

### 20.1.7. Data transfer processes and procedures

**20.1.7.R.01. Rationale**

Personnel can assist in preventing information security incidents by checking protective markings (classifications, endorsements and releasability) checks to ensure that the destination system is appropriate for the protection of the data being transferred, performing antivirus checks on data to be transferred to and from a system, and following all processes and procedures for the transfer of data.

**20.1.7.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST ensure that data transfers are performed in accordance with processes and procedures approved by the Accreditation Authority.

**20.1.7.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that data transfers are performed in accordance with processes and procedures approved by the Accreditation Authority.

### 20.1.8. Data transfer authorisation

**20.1.8.R.01. Rationale**

Using a trusted source to approve transfers from a classified system to another system of a lesser classification or where a releasability endorsement is applied to the data to be transferred, ensures appropriate oversight and reporting of the activity.

**20.1.8.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST ensure that all data transferred to a system of a lesser classification or a less secure system, is approved by a trusted source.

### 20.1.9. Trusted sources

**20.1.9.R.01. Rationale**

Trusted sources are designated personnel who have the delegated authority to assess and approve the transfer or release of data or documents. Trusted sources may include security personnel within the agency such as the CISO and the ITSM.

**20.1.9.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Trusted sources MUST be:

- a strictly limited list derived from business requirements and the result of a security risk assessment;
- where necessary an appropriate security clearance is held; and
- approved by the Accreditation Authority.

### 20.1.10. Import of data

**20.1.10.R.01. Rationale**

Scanning imported data for active or malicious content reduces the security risk of a system or network being infected, thus allowing the continued confidentiality, integrity and availability of the system or network.

**20.1.10.R.02. Rationale**

Format checks provide a method to prevent known malicious formats from entering the system or network. Keeping and regularly auditing these logs allow for the system or network to be checked for any unusual activity or usage.

**20.1.10.R.03. Rationale**

Personnel reporting unexpected events through the agency's incident management process provide an early opportunity to contain malware, limit damage and correct errors.

**20.1.10.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies importing data to a system MUST ensure that the data is scanned for malicious and active content.

**20.1.10.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies importing data to a system MUST implement the following controls:

- scanning for malicious and active content;
- data format checks;
- identify unexpected attachments or embedded objects;
- log each event; and
- monitoring to detect overuse/unusual usage patterns.

### 20.1.11. Export of highly formatted textual data

**20.1.11.R.01. Rationale**

When highly formatted textual data with no free text fields is to be transferred between systems, the checking requirements are lessened because the format of the information is strongly defined.

**20.1.11.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

When agencies export formatted textual data with no free text fields and all fields have a predefined set of permitted formats and data values, agencies MUST implement the following controls:

- protective marking checks;
- data validation and format checks;
- size limits;
- keyword checks;
- identify unexpected attachments or embedded objects;
- log each event; and
- monitoring to detect overuse/unusual usage patterns.

### 20.1.12. Export of other data

**20.1.12.R.01. Rationale**

Textual data that it is not highly formatted can be difficult to check in an automated manner. Agencies will need to implement measures to ensure that classified information is not accidentally being transferred to another system not accredited for that classification or transferred into the public domain.

**20.1.11.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST

When agencies export data, other than highly formatted textual data, agencies MUST implement the following controls:

- protective marking checks;
- data validation and format checks;
- limitations on data types;
- size limits;
- keyword checks;
- identify unexpected attachments or embedded objects;
- log each event; and
- monitoring to detect overuse/unusual usage patterns.

### 20.1.13. Preventing export of NZEO data to foreign systems

**20.1.13.R.01. Rationale**

In order to reduce the security risk of spilling data with an endorsement onto foreign systems, it is important that procedures are developed to detect NZEO marked data and to prevent it from crossing into foreign systems or being exposed to foreign nationals.

**20.1.13.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST:

- ensure that keyword searches are performed on all textual data;
- ensure that any identified data is quarantined until reviewed and approved for release by a trusted source other than the originator; and
- develop procedures to prevent NZEO information in both textual and non-textual formats from being exported.

# 20.2. Data Import and Export

## Objective

20.2.1. Data is transferred through gateways in a controlled and accountable manner.

## Context

### Scope

20.2.2. This section covers the specific requirements relating to the movement of data between systems via gateways. Fundamental requirements of data transfers between systems can be found in Section 20.1 – Data Transfers. These fundamental requirements apply to gateways.

## Rationale & Controls

### 20.2.3. User responsibilities

**20.2.3.R.01. Rationale**

When users transfer data to or from a system they need to be aware of the potential consequences of their actions. This could include data spills of sensitive or classified data onto systems not accredited to handle the data, or the unintended introduction of malicious code to a system. Accordingly, users need to be held accountable for all data transfers they make.

**20.2.3.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Users transferring data to and from a system MUST be held accountable for the data they transfer.

### 20.2.4. Data Transfer authorisation

**20.2.4.R.01. Rationale**

Users can help prevent information security incidents by:

- checking protective markings to ensure that the destination system is appropriate for the data being transferred;
- performing antivirus checks on data to be transferred to and from a system;
- following the processes and procedures for the transfer of data.

**20.2.4.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

All data transferred to a system of a lesser sensitivity or classification MUST be approved by a trusted source.

### 20.2.5. Trusted sources

**20.2.5.R.01. Rationale**

Trusted sources are designated personnel who have the delegated authority to assess and approve the transfer or release of data or documents. Trusted sources may include security personnel within the agency such as the CISO and the ITSM.

**20.2.5.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Trusted sources MUST be:

- a strictly limited list derived from business requirements and the result of a security risk assessment;
- where necessary an appropriate security clearance is held; and
- approved by the Accreditation Authority.

### 20.2.6. Import of data through gateways

**20.2.6.R.01. Rationale**

In order to ensure the continued functioning of systems it is important to constantly analyse data being imported. Converting data from one format into another can effectively destroy most malicious active content.

**20.2.6.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

When agencies import data to a system through gateways, the data MUST be filtered by a product specifically designed for that purpose, including filtering malicious and active content.

**20.2.6.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST

When agencies import data to a system through gateways, full or partial audits of the event logs MUST be performed at least monthly.

**20.2.6.C.03. Control:** System Classification(s): C, S, TS; Compliance: SHOULD

Agencies SHOULD convert data being imported at gateways into an alternative format before entering the network.

### 20.2.7. Export of data through gateways

**20.2.7.R.01. Rationale**

In order to ensure the continued integrity and confidentiality of data on an agency network, data MUST pass through a series of checks before it is exported onto systems of a lesser classification.

**20.2.7.R.02. Rationale**

Filtering content based on protective markings is an adequate method to protect the confidentiality of lesser classified material.

**20.2.7.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD restrict the export of data to a system of a lesser classification by filtering data using at least protective marking checks.

### 20.2.8. Export of highly formatted textual data through gateways

**20.2.8.R.01. Rationale**

The security risks of releasing higher classified data are partially reduced when the data is restricted to highly formatted textual data. In such cases the data is less likely to contain hidden data and have classified content. Such data can be automatically scanned through a series of checks to detect classified content. Risk is further reduced when there is a gateway filter that blocks (rejects) the export of data classified above the classification of the network outside of the gateway, and logs are regularly reviewed to detect if there has been unusual usage or overuse.

**20.2.8.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

When the export of highly formatted textual data occurs through gateways agencies MUST implement:

- checks for protective markings;
- data filtering performed by a product specifically designed for that purpose;
- data range and data type checks; and
- full or partial audits of the event logs performed at least monthly.

### 20.2.9. Export of other data through gateways

**20.2.9.R.01. Rationale**

Textual data which is not highly formatted can contain hidden data as well as having a higher classification due to the aggregated content. Risk is somewhat reduced by running additional automated checks on non-formatted data being exported, in addition to those checks for highly formatted textual data. Where a classification cannot be automatically determined, a human trusted source should make that determination.

**20.2.9.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

When agencies export data, other than highly formatted textual data, through gateways, agencies MUST implement data filtering performed by a product specifically designed for that purpose.

**20.2.9.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST

When agencies do not perform audits of the complete data transfer logs at least monthly they MUST perform randomly timed audits of random subsets of the data transfer logs on a weekly basis.

**20.2.9.C.03. Control:** System Classification(s): C, S, TS; Compliance: SHOULD

Where the classification cannot be determined automatically, a human trusted source SHOULD assess the classification of the data.

**20.2.9.C.04. Control:** System Classification(s): C, S, TS; Compliance: SHOULD

When the export of other data occurs through gateways agencies SHOULD perform audits of the complete data transfer logs at least monthly.

### 20.2.10. Preventing export of NZEO data to foreign systems

**20.2.10.R.01. Rationale**

NZEO networks are particularly sensitive and further security measures need to be put in place when connecting them to other networks.

**20.2.10.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

To prevent the export of NZEO data to foreign systems, agencies MUST implement NZEO data filtering performed by a product specifically designed or configured for that purpose.

**20.2.10.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST undertake checks of protective markings and keywords before permitting data export.

### 20.2.11. Requirement to sign exported data

**20.2.11.R.01. Rationale**

Digitally signing data being exported, demonstrates authenticity and improves assurance that the data has not been altered in transit.

**20.2.11.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

A trusted source MUST sign the data to be exported if the data is to be communicated over a network to which untrusted personnel or systems have access.

**20.2.11.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST ensure that the gateway verifies authority to release prior to the release of the data to be exported.

**20.2.11.C.03. Control:** System Classification(s): C, S, TS; Compliance: SHOULD

Agencies SHOULD use a product evaluated to at least an EAL4 assurance level for the purpose of data signing and signature confirmation.

# 20.3. Content Filtering

## Objective

20.3.1. The flow of data within gateways is examined and controls applied in accordance with the agency's security policy. To prevent unauthorised or malicious content crossing security domain boundaries.

## Context

### Scope

20.3.2. This section covers information relating to the use of content filters within bi-directional or one-way gateways in order to protect security domains.

20.3.3. Content filters reduce the risk of unauthorised or malicious content crossing a security domain boundary.

## Rationale & Controls

### 20.3.4. Limiting transfers by file type

**20.3.4.R.01. Rationale**

The level of security risk will be affected by the degree of assurance agencies can place in the ability of their data transfer filters to:

- confirm the file type by examination of the contents of the file;
- confirm the absence of malicious content;
- confirm the absence of inappropriate content;
- confirm the classification of the content; and
- handle compressed files appropriately.

Reducing the number of allowed file types reduces the number of potential vulnerabilities available for an attacker to exploit.

**20.3.4.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST strictly define and limit the types of files that can be transferred based on business requirements and the results of a security risk assessment.

**20.3.4.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD strictly define and limit the types of files that can be transferred based on business requirements and the results of a security risk assessment.

### 20.3.5. Blocking active content

**20.3.5.R.01. Rationale**

Many files are executable and are potentially harmful if activated by a system user. Many static file type specifications allow active content to be embedded within the file, which increases the attack surface.

**20.3.5.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST block all executables and active content from entering a security domain.

**20.3.5.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD block all executables and active content from being communicated though gateways.

### 20.3.6. Blocking suspicious data

#### 20.3.6.R.01. Rationale

The definition of suspicious content will depend on the system's risk profile and what is considered normal traffic. The table below identifies some filtering techniques that can be used to identify suspicious data.

| Technique | Purpose |
|---|---|
| **Antivirus scan** | Scans the data for viruses and other malicious code. |
| **Data format check** | Inspects data to ensure that it conforms to expected/permitted format(s). |
| **Data range check** | Checks the data within each field to ensure that it falls within the expected/permitted range. |
| **Data type check** | Inspects each file header to determine the file type. |
| **File extension check** | Checks file extensions to ensure that they are permitted. |
| **Keyword search** | Searches data for keywords or 'dirty words' that could indicate the presence of classified or inappropriate material. |
| **Metadata check** | Inspects files for metadata that should be removed prior to release. |
| **Protective marking check** | Validates the protective marking of the data to ensure that it complies with the permitted classifications and endorsements. |
| **Manual inspection** | The manual inspection of data for suspicious content that an automated system could miss, which is particularly important for the transfer of image files, multi-media or content-rich files. |

#### 20.3.6.C.01. Control: System Classification(s): All Classifications; Compliance: MUST

Agencies MUST block, quarantine or drop any data identified by a data filter as suspicious until reviewed and approved for transfer by a trusted source other than the originator.

### 20.3.7. Content validation

#### 20.3.7.R.01. Rationale

Content validation aims to ensure that the content received conforms to a defined, approved standard. Content validation can be an effective means of identifying malformed content, allowing agencies to block potentially malicious content. Content validation operates on a whitelisting principle, blocking all content except for that which is explicitly permitted. Examples of content validation include:

- ensuring numeric fields only contain numeric numbers;
- other fields operate with defined character sets;
- ensuring content falls within acceptable length boundaries;
- ensuring XML documents are compared to a strictly defined XML schema.

**20.3.7.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST perform validation on all data passing through a content filter, blocking content which fails the validation.

**20.3.7.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD perform validation on all data passing through a content filter, blocking content which fails the validation.

### 20.3.8. Content conversion and transformation

**20.3.8.R.01. Rationale**

Content conversion, file conversion or file transformation can be an effective method to render potentially malicious content harmless by separating the presentation format from the data. By converting a file to another format, the exploit, active content and/or payload can often be removed or disrupted enough to be ineffective.

Examples of file conversion and content transformation to mitigate the threat of content exploitation include:

- converting a Microsoft Word document to a PDF file;
- converting a Microsoft PowerPoint presentation to a series of JPEG images;
- converting a Microsoft Excel spreadsheet to a Comma Separated Values (CSV) file; or
- converting a PDF document to a plain text file.

Some file types, such as XML, will not benefit from conversion. The conversion process should also be applied to any attachments or files contained within other files, for example, archive files or encoded files embedded in XML.

**20.3.8.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD perform content conversion, file conversion, or both for all data transiting a security domain boundary (both ingress and egress).

### 20.3.9. Content sanitisation

**20.3.9.R.01. Rationale**

Sanitisation is the process of attempting to make potentially malicious content safe to use by removing or altering active content while leaving the original content as intact as possible. Sanitisation is not as secure a method of content filtering as conversion, though many techniques may be combined. Extraneous application and protocol data, including metadata, should also be inspected and filtered where possible. Examples of sanitisation to mitigate the threat of content exploitation include:

- removal of document properties information in Microsoft Office documents;
- removal or renaming of Javascript sections from PDF files;
- removal of metadata such as EXIF information from within JPEG files.

**20.3.9.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD perform content and file sanitisation on suitable file types if content or file conversion is not appropriate for data transiting a security domain boundary.

### 20.3.10. Antivirus scans

**20.3.10.R.01. Rationale**

Antivirus scanning is used to prevent, detect and remove malicious software that includes computer viruses, worms, Trojans, spyware and adware.

**20.3.10.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD perform antivirus scans on all content using up-to-date engines and signatures, using multiple different scanning engines.

### 20.3.11. Archive and container files

**20.3.11.R.01. Rationale**

Archive and container files can be used to bypass content filtering processes if the content filter does not handle the file type and embedded content correctly. The content filtering process should recognise archived and container files, ensuring the embedded files they contain are subject to the same content filtering measures as un-archived files.

**20.3.11.R.02. Rationale**

Archive files can be constructed in a manner which can pose a denial-of-service risk due to processor, memory or disk space exhaustion. To limit the risk of such an attack, content filters can specify resource constraints/quotas while extracting these files. If these constraints are exceeded the inspection is terminated, the content blocked and a security administrator alerted.

**20.3.11.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD extract the contents from archive and container files and subject the extracted files to content filter tests.

**20.3.11.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD perform controlled inspection of archive and container files to ensure that content filter performance and availability is not adversely affected.

**20.3.11.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD block files that cannot be inspected and generate an alert or notification.

### 20.3.12. Whitelisting permitted content

**20.3.12.R.01. Rationale**

Creating and enforcing a whitelist of allowed content/files is a strong content filtering method. Allowing content that satisfies a business requirement only can reduce the attack surface of the system. As a simple example, an email content filter might allow only Microsoft Office documents and PDF files.

**20.3.12.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST create and enforce a whitelist of permitted content types based on business requirements and the results of a security risk assessment.

**20.3.12.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD create and enforce a whitelist of permitted content types based on business requirements and the results of a security risk assessment.

### 20.3.13. Data integrity

**20.3.13.R.01. Rationale**

Ensuring the authenticity and integrity of content reaching a security domain is a key component in ensuring its trustworthiness. It is also essential that content that has been authorised for release from a security domain is not modified or contains other data not authorised for release, for example by the addition or substitution of sensitive information.

**20.3.13.R.02. Rationale**

If content passing through a filter contains a form of integrity protection, such as a digital signature, the content filter should verify the content's integrity before allowing it through. If the content fails these integrity checks it may have been spoofed or tampered with and should be dropped or quarantined for further inspection.

Examples of data integrity checks include:

- an email server or content filter verifying an email protected by DKIM;
- a web service verifying the XML digital signature contained within a SOAP request;
- validating a file against a separately supplied hash;
- checking that data to be exported from the security domain has been digitally signed by the release authority.

**20.3.13.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

If data is signed, agencies MUST ensure that the signature is validated before the data is exported.

**20.3.13.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD verify the integrity of content where applicable, and block the content if verification fails.

### 20.3.14. Encrypted data

**20.3.14.R.01. Rationale**

Encryption can be used to bypass content filtering if encrypted content cannot be subject to the same checks performed on unencrypted content. Agencies will need to consider the need to decrypt content, depending on:

- the security domain they are communicating with;
- whether the need-to-know principle is to be enforced;
- end-to-end encryption requirements; or
- any privacy and policy requirements.

**20.3.14.R.02. Rationale**

Choosing not to decrypt content poses a risk of encrypted malicious software communications and data moving between security domains. Additionally, encryption could mask the movement of information at a higher classification being allowed to pass to a security domain of lower classification, which could result in a data spill.

**20.3.14.R.03. Rationale**

Some systems allow encrypted content through external/boundary/perimeter controls to be decrypted at a later stage, in which case the content should be subject to all applicable content filtering controls after it has been decrypted.

**20.3.14.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD decrypt and inspect all encrypted content, traffic and data to allow content filtering.

### 20.3.15. Monitoring data import and export

**20.3.15.R.01. Rationale**

To ensure the continued confidentiality and integrity of systems and data, import and export processes should be monitored and audited.

**20.3.15.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST use protective marking checks to restrict the export of data from each security domain, including through a gateway.

**20.3.15.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST

When importing data to each security domain, including through a gateway, agencies MUST audit the complete data transfer logs at least monthly.

### 20.3.16. Exception Handling

**20.3.16.R.01. Rationale**

Legitimate reasons may exist for the transfer of data that may be identified as suspicious according to the criteria established for content filtering. It is important to have an accountable and auditable mechanism in place to deal with such exceptions.

**20.3.16.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD create an exception handling process to deal with blocked or quarantined file types that may have a valid requirement to be transferred.

## 20.4. Databases

### Objective

20.4.1. Database content is protected from personnel without a need-to-know.

### Context

#### Scope

20.4.2. This section covers information relating to databases and interfaces to databases such as search engines.

## Rationale & Controls

### 20.4.3. Data labelling

**20.4.3.R.01. Rationale**

Protective markings can be applied to records, tables or to the database as a whole, depending on structure and use. Query results will often need a protective marking to reflect the aggregate of the information retrieved.

**20.4.3.C.01. Control:** System Classification(s): TS; Compliance: MUST

Agencies MUST ensure that all classified information stored within a database is associated with an appropriate protective marking if the information:

- could be exported to a different system; or
- contains differing classifications or different handling requirements.

**20.4.3.C.02. Control:** System Classification(s): TS; Compliance: MUST

Agencies MUST ensure that protective markings are applied with a level of granularity sufficient to clearly define the handling requirements for any classified information retrieved or exported from a database.

**20.4.3.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that all classified information stored within a database is associated with an appropriate protective marking if the information:

- could be exported to a different system; or
- contains differing classifications or different handling requirements.

**20.4.3.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that protective markings are applied with a level of granularity sufficient to clearly define the handling requirements for any classified information retrieved or exported from a database.

### 20.4.4. Database files

**20.4.4.R.01. Rationale**

Even though a database may provide access controls to stored data, the database files themselves MUST also be protected.

**20.4.4.C.01. Control:** System Classification(s): TS; Compliance: MUST

Agencies MUST protect database files from access that bypasses the database's normal access controls.

**20.4.4.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD protect database files from access that bypass normal access controls.

### 20.4.5. Accountability

**20.4.5.R.01. Rationale**

If system users' interactions with databases are not logged and audited, agencies will not be able to appropriately investigate any misuse or compromise of database content.

**20.4.5.C.01. Control:** System Classification(s): TS; Compliance: MUST

Agencies MUST enable logging and auditing of system users' actions.

**20.4.5.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that databases provide functionality to allow for auditing of system users' actions.

### 20.4.6. Search engines

**20.4.6.R.01. Rationale**

Even if a search engine restricts viewing of classified information that a system user does not have sufficient security clearances to access, the associated metadata can contain information above the security clearances of the system user. In such cases, restricting access to, or sanitising, this metadata effectively controls the possible release of information the system user is not cleared to view.

**20.4.6.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

If results from database queries cannot be appropriately filtered, agencies MUST ensure that all query results are appropriately sanitised to meet the minimum security clearances of system users.

**20.4.6.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that system users who do not have sufficient security clearances to view database contents cannot see or interrogate associated metadata in a list of results from a search engine query.

# 21. Working Off-Site

## 21.1. Agency-owned Mobile Devices

### Objective

21.1.1. Information on agency-owned mobile devices is protected from unauthorised disclosure.

### Context

#### Scope

21.1.2. This section covers information relating to the use of agency-owned mobile devices including, but not restricted to, mobile phones, smartphones, portable electronic devices, personal digital assistants, laptops, netbooks, tablet computers, and other portable Internet connected devices.

21.1.3. It is important to note that product security, selection, maintenance, sanitisation and disposal requirements in Chapter 12 – Product Security also apply to agency-owned mobile devices.

#### Trusted Operating Environments

21.1.4. A Trusted Operating Environment (TOE) provides assurance that every reasonable effort has been made to secure the operating system of a mobile device such that it presents a managed risk to an agency's information and systems. Any residual risks are explicitly accepted by the agency.

21.1.5. Special care is necessary when dealing with All-of-Government systems or systems that affect several agencies. Security measures that can be implemented to assist in the development of a TOE include:

- strong usage policies are in place;
- unnecessary hardware, software and operating system components are removed;
- unused or undesired functionality in software and operating systems is removed or disabled;
- anti-malware and other security software is installed and regularly updated;
- downloads of software, data or documents are limited or not permitted;
- installation of unapproved applications is not permitted;
- software-based firewalls limiting inbound and outbound network connections are installed;
- patching of installed the operating system and other software is current;
- each connection is authenticated (multi-factor) before permitting access to an agency network;
- both the user and mobile device are authenticated during the authentication process;
- mobile device configurations may be validated before a connection is permitted;
- privileged access from the mobile device to the agency network is not allowed;
- access to some data may not be permitted; and
- agency control of the mobile device may supersede any convenience aspects.

### Treating workstations as mobile devices

21.1.6. When an agency issues a workstation for home-based work instead of a mobile device the requirements in this section apply equally to the issued workstation.

### Devices with multiple operating states

21.1.7. Some mobile devices may have functionality to allow them to operate in either an unclassified state or a classified state. In such cases the mobile devices will need to be handled according to the state that it is being operated in at the time. For example, some devices can start-up in an unclassified mode or start-up in a cryptographically protected mode.

### Bluetooth and Infra-Red Devices

21.1.8. Bluetooth and Infra-Red devices, such as keyboards, headsets and mice are subject to an additional set of risks. Refer to Chapter 11 – Communication Systems and Devices.

## PSR references

21.1.9. Relevant PSR requirements can be found at:

| Reference | Title | Source |
|---|---|---|
| **PSR Mandatory Requirements** | GOV2, GOV4. GOV6, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2 | http://www.protectivesecurity.govt.nz |
| **PSR content protocols** | Management protocol for information security<br>Management protocol for physical security | http://www.protectivesecurity.govt.nz |
| **PSR requirements sections** | Build security awareness<br>Working away from the office | http://www.protectivesecurity.govt.nz |
| **Managing specific scenarios** | Mobile and remote working<br>Communications security | http://www.protectivesecurity.govt.nz |

## Rationale & Controls

### 21.1.10. Mobile devices usage policy

**21.1.10.R.01. Rationale**

As mobile devices routinely leave the office environment and the physical protection it affords it is important that policies are developed to ensure that they are protected in an appropriate manner when used outside of controlled agency facilities.

**21.1.10.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop a policy governing the use of mobile devices.

**21.1.10.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST NOT

Agencies MUST NOT allow mobile devices to process or store TOP SECRET information unless explicitly approved by GCSB to do so.

**21.1.10.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD implement a Mobile Device Management (MDM) solution.

### 21.1.11. Personnel awareness

**21.1.11.R.01. Rationale**

Mobile devices can have both a data and voice component capable of processing or communicating classified information. In such cases, personnel will need to be aware of the approved classification level for each function.

This includes Paging Services, Multi-Media Message Service (MMS) and Short Message Service (SMS) which are NOT appropriate for sensitive or classified information. Paging and message services do not appropriately encrypt information and cannot be relied upon for the communication of classified information.

**21.1.11.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST advise personnel of the maximum permitted classifications for data and voice communications when using mobile devices.

**21.1.11.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT use Paging Services, SMS or MMS for sensitive or classified communications.

### 21.1.12. Non-agency owned and controlled mobile devices

**21.1.12.R.01. Rationale**

Agencies need to retain control of any non-agency device that contains agency or government information. Non-agency devices are discussed in Section 21.4 – BYOD.

**21.1.12.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST apply the full set of BYOD controls for devices NOT directly owned and controlled by the agency. These controls are detailed in Section 21.4 – BYOD.

### 21.1.13. Agency owned mobile device storage encryption

**21.1.13.R.01. Rationale**

Encrypting the internal storage and removable media of agency owned mobile devices will reduce the risk of data loss associated with a lost or stolen device. While the use of encryption may not be suitable to treat the device as an unclassified asset it will still present a significant challenge to a malicious actor looking to gain easy access to information stored on the device. To ensure that the benefits of encryption on mobile devices are maintained, users must not store passphrases, passwords, PINS or other access codes for the encryption software on, or with, the device.

**21.1.13.R.02. Rationale**

Information on the use of encryption to reduce storage and physical transfer requirements is detailed in Section 17.1 – Cryptographic Fundamentals and 17.2 – Approved Cryptographic Algorithms.

**21.1.13.R.03. Rationale**

Encrypting Information on handling instructions are detailed in the PSR, refer to Protecting Mobile Devices; Mobile and Remote Working; and Assessing the risks of Mobile working.

**21.1.13.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies unable to lower the storage and physical transfer requirements of a mobile device to an unclassified level through the use of encryption MUST physically store or transfer the device as a classified asset in accordance with the relevant handling instructions.

**21.1.13.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

Users MUST NOT store passwords, passphrases, PINs or other access codes for encryption on or with the mobile device on which data will be encrypted when the device is issued for normal operations.

**21.1.13.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies unable to lower the storage and physical transfer requirements of a mobile device to an unclassified level through the use of encryption SHOULD physically store or transfer the device as a classified asset in accordance with the relevant handling instructions.

**21.1.13.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD encrypt classified information on all mobile devices using an Approved Cryptographic Algorithm.

**21.1.13.C.05. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Pool or shared devices SHOULD be reissued with unique passwords, passphrases, PINs or other access codes for each separate issue or deployment.

### 21.1.14. Mobile device communications encryption

**21.1.14.R.01. Rationale**

The above approach cannot be used for communicating classified information over public infrastructure, the internet or non-agency controlled networks. If appropriate encryption is not available the mobile device will not be approved for communicating classified information.

**21.1.14.R.02. Rationale**

Note: This applies to information and systems classified as RESTRICTED/SENSITIVE and any higher classification.

**21.1.14.R.03. Rationale**

Encryption does not change the classification level of the information or system itself but allows reduced handling requirements to be applied.

**21.1.14.C.01. Control:** System Classification(s): RESTRICTED/SENSITIVE, C, S, TS; Compliance: MUST

Agencies MUST use encryption on mobile devices communicating over public infrastructure, the Internet or non-agency controlled networks.

**21.1.14.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use encryption for Official Information or any classified information on mobile devices communicating over public infrastructure, the Internet or non-agency controlled networks.

### 21.1.15. Mobile device privacy filters

**21.1.15.R.01. Rationale**

Privacy filters can be applied to the screens of mobile devices to prevent onlookers from reading the contents off the screen of the device. This assists in mitigating a shoulder surfing or other oversight attack or compromise.

**21.1.15.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD apply privacy filters to the screens of mobile devices.

### 21.1.16. Disabling Bluetooth functionality

**21.1.16.R.01. Rationale**

As Bluetooth provides little security for the information that is passed between devices and a number of exploits have been publicised, it SHOULD NOT be used on mobile devices. Refer to Chapter 11 – Communications Systems and Devices.

**21.1.16.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST NOT

Agencies MUST NOT enable Bluetooth functionality on mobile devices.

**21.1.16.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT enable Bluetooth functionality on mobile devices.

### 21.1.17. Configuration control

**21.1.17.R.01. Rationale**

Poorly controlled devices are more vulnerable to compromise and provide an attacker with a potential access point into agency systems. Although agencies may initially provide a secure device, the state of security may degrade over time. The agency will need to revaluate the security of devices regularly to ensure their integrity.

**21.1.17.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

Agency personnel MUST NOT disable security functions or security configurations on a mobile device once provisioned.

**21.1.17.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD control the configuration of mobile devices in the same manner as devices in the agency's office environment.

**21.1.17.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD prevent personnel from installing unauthorised applications on a mobile device once provisioned.

### 21.1.18. Maintaining mobile device security

**21.1.18.R.01. Rationale**

As mobile devices are not continually connected to ICT systems within an agency it is important that they are routinely returned to the agency so that patches can be applied and they can be tested to ensure that they are still secure.

Alternatively a mobile device management solution may implement policy checks and updates on connection to agency systems.

**21.1.18.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that mobile devices have security updates applied on a regular basis and are tested to ensure that the mobile devices are still secure.

**21.1.18.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD conduct policy checks as mobile devices connect to agency systems.

### 21.1.19. Connecting mobile devices to the Internet

**21.1.19.R.01. Rationale**

During the period that a device is connected to the Internet, without a VPN connection, it is exposed to attacks. This period needs to be minimised to reduce the security risks. Minimising this period includes ensuring that system users do not connect directly to the Internet to access the Web between VPN sessions.

**21.1.19.R.02. Rationale**

A split tunnel VPN can allow access to an agency's systems from another network, including unsecure networks such as the Internet. If split tunnelling is enabled there is an increased security risk that the VPN connection is susceptible to attack from such networks.

**21.1.19.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST disable split tunnelling when using a VPN connection from a mobile device to connect to an agency network.

**21.1.19.C.02. Control:** System Classification(s): C, S, TS; Compliance: SHOULD NOT

Agencies SHOULD NOT allow mobile devices to connect to the Internet except when temporarily connecting to facilitate the establishment of a VPN connection to an agency network.

### 21.1.20. Emergency destruction

**21.1.20.R.01. Rationale**

Where a mobile device carries classified information, or there is an increased risk of loss or compromise of the device, agencies will need to develop emergency destruction procedures. Such procedures should focus on the destruction of information on the mobile device and not necessarily the device itself. Many mobile devices used for classified information achieve this through the use of a cryptographic key zeroise or sanitisation function.

**21.1.20.R.02. Rationale**

Staff will need to understand the rationale and be familiar with emergency destruction procedures, especially where there is a higher probability of loss, theft or compromise.

**21.1.20.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop an emergency destruction plan for mobile devices.

**21.1.20.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

If a cryptographic zeroise or sanitise function is provided for cryptographic keys on a mobile device it MUST be used as part of the emergency destruction procedures.

**21.1.20.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure personnel are trained in emergency destruction procedures and are familiar with the emergency destruction plan.

### 21.1.21. Labelling

**21.1.21.R.01. Rationale**

Agencies may wish to affix an additional label to mobile devices asking finders of lost devices to hand it in to any New Zealand police station, or if overseas, a New Zealand embassy, consulate or high commission.

**21.1.21.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD use soft labelling for mobile devices when appropriate to reduce their attractiveness value.

### 21.1.22. Unauthorised use of mobile devices

**21.1.22.R.01. Rationale**

Where mobile devices are issued to personnel for business purposes their use for private purposes should be governed by agency policy and agreed by the employee or contractor to whom the device is issued.

**21.1.22.R.02. Rationale**

Agencies must recognise the risks and costs associated with personal use of an agency device.

**21.1.22.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD develop a policy to manage the non-business or personal use of an agency owned device.

**21.1.22.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Mobile devices SHOULD NOT be used other than by personnel specifically authorised by the agency.

# 21.2. Working Outside the Office

## Objective

21.2.1. Information on mobile devices is not accessed from public or insecure locations.

## Context

### Scope

21.2.2. This section covers information on accessing information using agency-owned mobile devices from unsecured locations outside the office and home environments. This section does not apply to working from home; requirements relating to home-based work are outlined in Section 21.3 – Working From Home. Further information on the use of mobile devices can be found in Section 21.1 – Agency Owned Mobile Devices.

21.2.3. Also refer to Chapter 12 – Product Security for requirements on product security, selection, maintenance, sanitisation and disposal.

## Rationale & Controls

### 21.2.4. Working outside the office

**21.2.4.R.01. Rationale**

As the security risk relating to specific targeting of mobile devices capable of processing highly classified information is high, these mobile devices cannot be used outside of facilities certified to an appropriate level to allow for their use. In addition, as agencies have no control over public locations including, but not limited to, such locations as public transport, transit lounges, hotel lobbies, and coffee shops, mobile devices are not approved to process classified information as the security risk of classified information being overheard or observed is considered to be too high in such locations.

**21.2.4.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT allow personnel to access or communicate classified information on mobile devices outside of secure areas unless there is a reduced chance of being overheard and having the screen of the device observed.

**21.2.4.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies allowing personnel to access or communicate classified information outside of the office SHOULD NOT allow personnel to do so in public locations (e.g. public transport, transit lounges, hotel lobbies and coffee shops).

### 21.2.5. Carrying mobile devices

**21.2.5.R.01. Rationale**

Mobile devices used outside the office are frequently transferred through areas not certified to process the classified information on the device. Mechanisms need to be put in place to protect the information stored on those devices.

**21.2.5.R.02. Rationale**

When agencies apply encryption to mobile devices to reduce their physical transfer requirements it is only effective when the encryption function of the device is not authenticated. In most cases this will mean the mobile device will be in an unpowered state (i.e. not turned on), however, some devices are capable of deauthenticating the cryptography when it enters a locked state after a predefined timeout period. Such mobile devices can be carried in a locked state in accordance with reduced physical transfer requirements based on the assurance given in the cryptographic functions.

**21.2.5.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure mobile devices are carried in a secured state when not being actively used, by:

- power off; or
- power on but pass code enabled.

### 21.2.6. Using mobile devices

**21.2.6.R.01. Rationale**

Mobile devices are portable in nature and can be easily stolen or misplaced. It is strongly advised that personnel do not leave mobile devices unattended at any time.

**21.2.6.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

When in use mobile devices MUST be kept under continual direct supervision.

### 21.2.7. Travelling with mobile devices

**21.2.7.R.01. Rationale**

If personnel place mobile devices or media in checked-in luggage when travelling they lose control over the devices. Such situations provide an opportunity for mobile devices to be stolen or tampered with by an attacker.

**21.2.7.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

When travelling with mobile devices and media, personnel MUST retain control over them at all times including by not placing them in checked-in luggage or leaving them unattended.

**21.2.7.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Travelling personnel requested to decrypt mobile devices for inspection or from whom mobile devices are taken out of sight by border control MUST report the potential compromise of classified information or the device to an ITSM as soon as possible.

# 21.3. Working From Home

## Objective

21.3.1. Personnel working from home protect classified information in the same manner as in the office environment.

## Context

### Scope

21.3.2. This section covers accessing official information and agency information using mobile devices from a home environment in order to conduct home-based work. Further information on the use of mobile devices can be found in Section 21.1 – Agency Owned Mobile Devices.

### The use of workstations instead of mobile devices

21.3.3. Where an agency chooses to issue a workstation for home-based work instead of a mobile device, the requirements for mobile devices within Section 21.1 – Agency Owned Mobile Devices, equally apply to the workstation that is used.

21.3.4. Also refer to Chapter 12 – Product Security for requirements on product security, selection, maintenance, sanitisation and disposal.

21.3.5. It is important to note that product security, selection, maintenance, sanitisation and disposal requirements in Chapter 12 – Product Security apply to all agency-owned devices.

## Rationale & Controls

### 21.3.6. Storage requirements

**21.3.6.R.01. Rationale**

All mobile devices have the potential to store classified information and therefore need protection against loss and compromise.

**21.3.6.R.02. Rationale**

Information on physical security requirements are detailed in the PSR, refer to Protecting Mobile Devices; Mobile and Remote Working; and Assessing the risks of Mobile working.

**21.3.6.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that when mobile devices are not being actively used they are secured in accordance with the minimum physical security requirements as stated in the PSR.

### 21.3.7. Processing requirements

**21.3.7.R.01. Rationale**

When agencies consider allowing personnel to work from a home environment they need to be aware that implementing physical security measures may require modifications to the person's home, or the provision of approved containers or secure storage units at the expense of the agency.

**21.3.7.R.02. Rationale**

Information on physical security requirements are detailed in the PSR, refer to Protecting Mobile Devices; Mobile and Remote Working; and Assessing the risks of Mobile working.

**21.3.7.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure that the area within which mobile devices are used meets the minimum physical security requirements as stated in the PSR.

# 21.4. Non-Agency Owned Devices and Bring Your Own Device (BYOD)

## Objective

21.4.1. Where an Agency permits personnel to supply their own mobile devices (such as smartphones, tablets and laptops), Official Information and agency information systems are protected to a level equivalent to an agency provided and managed office environment.

## Context

### Scope

21.4.2. This section provides information on the use and security of **non-agency owned or provided** mobile devices when used for official business. This is commonly known as Bring Your Own Device (BYOD). The use of agency owned devices is described earlier in Section 21.1 – Agency Owned Mobile Devices.

21.4.3. In the context of this section, a BYOD Network is any agency owned or provided network dedicated to BYOD. A BYOD Network is usually within an agency's premises but does NOT include networks and related services provided by commercial telecommunication or other technology providers.

21.4.4. BYOD will introduce a wide range of risks, including information and privacy risks, to an organisation, in addition to the existing ICT risks and threats. Agencies will need to carefully examine and consider the security, privacy, governance, assurance and compliance risks and implications of BYOD.

21.4.5. Mobile devices are a "soft" target for malware and cybercrime providing a further attack channel or vector for organisational ICT infrastructures and networks. Risks fall principally into the following categories:

- Data exfiltration and theft;
- Data tampering;
- Data loss;
- Malware;
- System outages and Denial of Service; and
- Increased incident management and recovery costs.

## References

21.4.6. Further references can be found at:

| Title | Publisher | Source |
|---|---|---|
| **Risk Management of Enterprise Mobility including Bring Your Own Device** | ASD | http://www.asd.gov.au/publications/csocprotect/Enterprise_Mobility_BYOD.pdf |
| **End User Devices Security and Configuration Guidance** | NCSC, UK | https://www.ncsc.gov.uk/eud-guidance |
| **NIST 800-121 Guide to Bluetooth Security** | NIST | http://www.csrc.nist.gov/publications/nistpubs/800-121-rev1/sp800-121_rev1.pdf |
| **NIST Special Publication 800-46 Revision 2 - Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security** | NIST | http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf |
| **NIST Special Publication 800-114 Revision 1**<br>**User's Guide to Telework and Bring Your Own Device (BYOD) Security** | NIST | http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf |
| **BYOD Guidance: Device Security Considerations** | GOV.UK | https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360960/BYOD_Guidance_-_Device_Security_Considerations.pdf |

## Rationale & Controls

### 21.4.7. Risk Assessment

**21.4.7.R.01. Rationale**

Commonly termed "Bring Your Own Device" (BYOD), personal use of mobile computing in an organisational environment is widespread and personnel have become accustomed to the use of a variety of personal mobile devices. BYOD can have many advantages for an agency and for personnel. At the same time, BYOD will introduce a range of new information security risks and threats and may exacerbate existing risks.

**21.4.7.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST undertake a risk assessment and implement appropriate controls BEFORE implementing a BYOD Policy and permitting the use of BYOD.

**21.4.7.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST take an integrated approach to BYOD security, covering policy, training, support, systems architecture, security, systems management, change management, incident detection & management and business continuity.

### 21.4.8. Applicability and Usage

**21.4.8.R.01. Rationale**

BYOD introduces number of additional risks and attack vectors to agency systems. Not all BYOD risks can be fully mitigated with technologies available today. It is therefore important that, where feasible, all the controls specified in this section are implemented.

**21.4.8.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

BYOD MUST **only** be permitted for agency information systems up to and including RESTRICTED.

**21.4.8.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST NOT

BYOD MUST NOT be used for CONFIDENTIAL, SECRET or TOP SECRET systems.

### 21.4.9. Technical Controls

**21.4.9.R.01. Rationale**

"Jail-Breaking" and "rooting" are terms applied to devices where operating systems controls have been by-passed to allow installation of alternate operating systems or software applications that are not otherwise permitted. This is a risky practice and can create opportunities for device compromise. Users may wish to alter settings to allow the download of personal apps. This can result in security setting violations.

**21.4.9.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

Devices that have been "jail-broken", "rooted" or have settings violations MUST NOT be used for any agency business or be allowed to connect to any agency systems UNLESS this been specifically authorised.

### 21.4.10. BYOD Policy

**21.4.10.R.01. Rationale**

Technical controls fall into two categories: organisational systems and device controls. Protection for organisational systems will start with a risk assessment which guides the development of a secure architecture to support BYOD operations. Additional controls will need to be applied to individual devices. The privacy of user data should be considered. A user policy is essential.

**21.4.10.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies may identify additional policy provisions and controls that are required, based on their assessment of risk. Agencies MUST implement the additional controls and protocols before implementing BYOD.

**21.4.10.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST implement a BYOD acceptable use policy, agreed and signed by each person using a BYOD device.

**21.4.10.C.03. Control:** System Classification(s): All Classifications; Compliance: MUST

The agency's policy MUST clearly establish eligibility of personnel for participation in the agency BYOD scheme.

**21.4.10.C.04. Control:** System Classification(s): All Classifications; Compliance: MUST

Personnel MUST have written authorisation (usually managerial approval) before a connection is enabled (on-boarding).

**21.4.10.C.05. Control:** System Classification(s): All Classifications; Compliance: MUST

Written authorisation MUST include the nature and extent of agency access approved, considering:

- time, day of the week;
- location; and
- local or roaming access.

**21.4.10.C.06. Control:** System Classification(s): All Classifications; Compliance: MUST

Procedures MUST be established for removal of agency installed software and any agency data when the user no longer has a need to use BYOD, is redeployed or ceases employment (off-boarding).

**21.4.10.C.07.** **Control:** System Classification(s): All Classifications; Compliance: MUST

Standard Operating Procedures for the agency's BYOD network MUST be established.

**21.4.10.C.08.** **Control:** System Classification(s): All Classifications; Compliance: MUST

Provision MUST be made for contractors and other authorised non-employees. It is at the agency's discretion whether this activity is permitted. The risk assessment MUST reflect this factor.

**21.4.10.C.09.** **Control:** System Classification(s): All Classifications; Compliance: MUST

Ownership of data on BYOD devices MUST be clearly articulated and agreed.

**21.4.10.C.010.** **Control:** System Classification(s): All Classifications; Compliance: MUST

Agency policies MUST clearly articulate the separation between corporate support and where individuals are responsible for the maintenance and support of their own devices.

**21.4.10.C.011.** **Control:** System Classification(s): All Classifications; Compliance: MUST

Agency policies MUST clearly articulate the acceptable use of any GPS or other tracking capability.

**21.4.10.C.012.** **Control:** System Classification(s): All Classifications; Compliance: MUST

Individual responsibility for the cost of any BYOD device and its accessories MUST be agreed.

**21.4.10.C.013.** **Control:** System Classification(s): All Classifications; Compliance: MUST

Individual responsibility for replacement in the event of loss or theft MUST be agreed.

**21.4.10.C.014.** **Control:** System Classification(s): All Classifications; Compliance: MUST

Individuals MUST be responsible for the installation and maintenance of any mandated BYOD-based firewalls and anti-malware software and for implementing operating system updates and patches on their device.

**21.4.10.C.015.** **Control:** System Classification(s): All Classifications; Compliance: MUST

The procedures for purchasing and installing business related applications on the mobile devices MUST be specified and agreed.

**21.4.10.C.016.** **Control:** System Classification(s): All Classifications; Compliance: MUST

The responsibility for payment of voice and data plans and roaming charges MUST be specified and agreed.

### 21.4.11. BYOD Infrastructure and System Controls

**21.4.11.R.01. Rationale**

The use of BYOD presents increased risk and threat to agency systems. Changes to an agency's security architecture are necessary in order to minimise and manage the increased risk and threat to agency systems, information and information privacy.

**21.4.11.R.02. Rationale**

It is important that the principles of separation and segregation are applied to any system architecture or design to assist in the management of risk in BYOD systems.

**21.4.11.R.03. Rationale**

BYOD devices will seek to establish multiple connections through Wi-Fi "hot spots", Bluetooth connection and simultaneous internet and cellular connections. This behaviour creates multiple simultaneous "back channels" which can provide attack vectors for malicious activities and is considered to be high risk.

**21.4.11.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

A security architectural review MUST be undertaken by the agency before allowing BYOD devices to connect to agency systems.

**21.4.11.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

The BYOD network segment MUST be segregated from other elements of the agency's network.

**21.4.11.C.03. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST architecturally separate guest and public facing networks from BYOD networks.

**21.4.11.C.04. Control:** System Classification(s): All Classifications; Compliance: MUST

Network configuration policies and authentication mechanisms MUST allow access to agency resources ONLY through the BYOD network segment.

**21.4.11.C.05. Control:** System Classification(s): All Classifications; Compliance: MUST

Access to internal resources and servers MUST be carefully managed and confined to only those services for which there is a defined and properly authorised business requirement.

**21.4.11.C.06. Control:** System Classification(s): All Classifications; Compliance: MUST

Wireless accesses points used for access to agency networks MUST be implemented and secured in accordance with the directions in this manual (See Section 18.2 – Wireless Local Area Networks).

**21.4.11.C.07. Control:** System Classification(s): All Classifications; Compliance: MUST

Bluetooth on BYOD devices MUST be disabled while within designated secure areas on agency premises.

**21.4.11.C.08.** **Control:** System Classification(s): All Classifications; Compliance: MUST

Access Controls MUST be implemented in accordance with Chapter 16 – Access Control.

**21.4.11.C.09.** **Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST maintain a list of permitted operating systems, including operating system version numbers, for BYOD devices.

**21.4.11.C.010.** **Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST check each BYOD device for malware and sanitise the device appropriately before installing agency software or operating environments.

**21.4.11.C.011.** **Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST check each BYOD device for malware and sanitise the device appropriately before permitting access to agency data.

**21.4.11.C.012.** **Control:** System Classification(s): All Classifications; Compliance: MUST

BYOD MUST have a Mobile Device Management (MDM) solution implemented with a minimum of the following enabled:

- The MDM is enabled to "wipe" devices of any agency data if lost or stolen;
- If the MDM cannot discriminate between agency and personal data, all data, including personal data, is deleted if the device is lost or stolen;
- The MDM is capable of remotely applying agency security configurations for BYOD devices;
- Mobile device security configurations are validated (health check) by the MDM before a device is permitted to connect to the agency's systems;
- "Jail-broken", "rooted" or settings violations MUST be detected and isolated;
- "Jail-broken" devices are NOT permitted to access agency resources;
- Access to agency resources is limited until the device and user is fully compliant with policy and SOPs;
- Auditing and logging is enabled; and
- Changes of Subscriber Identity Module (SIM) card are monitored to allow remote blocking and wiping in the event of theft or compromise.

**21.4.11.C.013. Control:** System Classification(s): All Classifications; Compliance: MUST

Intrusion detection systems MUST be implemented.

**21.4.11.C.014. Control:** System Classification(s): All Classifications; Compliance: MUST

Continuous monitoring MUST be established to detect actual or potential security compromises or incidents from BYOD devices. Refer also to Chapter 6.

**21.4.11.C.015. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST maintain a list of approved cloud applications that may be used on BYOD devices.

**21.4.11.C.016. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST block the use of unapproved cloud applications for processing any agency or organisational data.

**21.4.11.C.017. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

BYOD devices MUST NOT be permitted direct connection to internal hosts, including all other devices on the local network.

**21.4.11.C.018. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

BYOD devices connecting to guest and public facing networks MUST NOT be permitted access to the corporate network other than through a VPN over the Internet.

**21.4.11.C.019. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Bluetooth on BYOD devices SHOULD be disabled while within agency premises and while accessing agency systems and data.

**21.4.11.C.020. Control:** System Classification(s): All Classifications; Compliance: SHOULD

BYOD devices and systems SHOULD use Multifactor (at least two-factor) authentication to connect to agency systems and prior to being permitted access to agency data.

### 21.4.12. Wireless IDS / IPS systems

**21.4.12.R.01. Rationale**

Devices will automatically associate with the strongest signal and associated Access Point (AP). A rogue AP may belong to another organisation in an adjacent building, contractor, customer, supplier or other visitor. Association with a rogue AP can provide a means for the installation of malware.

**21.4.12.R.02. Rationale**

Wireless IDS / IPS systems have the ability to detect rogue wireless AP's by channel, MAC address, frequency band and SSID. They can continuously monitor wireless networks and detect and block denial-of-service and man-in-the-middle wireless attacks. Establishing baselines of known authorised and unauthorised devices and AP's will assist in detecting and isolating any rogue devices and AP's.

**21.4.12.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST implement a wireless IDS /IPS on BYOD wireless networks.

**21.4.12.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST implement rogue AP and wireless "hot spot" detection and implement response procedures where detection occurs.

**21.4.12.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD conduct a baseline survey to identify:

- All authorised devices and AP's; and
- Any unauthorised devices and AP's.

### 21.4.13. BYOD Device Controls

**21.4.13.R.01. Rationale**

Mobile devices are susceptible to loss, theft and being misplaced. These devices can be easily compromised when out of the physical control of the authorised user or owner. To protect agency systems it is important that BYOD devices are also secured and managed on an ongoing basis.

**21.4.13.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Any agency data exchanged with the mobile device MUST be encrypted in transit (See Chapter 17 – Cryptography).

**21.4.13.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Any agency data stored on the device MUST be encrypted (including keys, certificates and other essential session establishment data).

**21.4.13.C.03. Control:** System Classification(s): All Classifications; Compliance: MUST

The use of virtual containers, sandboxes, wraps or similar mechanisms on the mobile device MUST be established for each authorised session for any organisational data. These mechanisms MUST be non-persistent and be removed at the end of each session.

**21.4.13.C.04. Control:** System Classification(s): All Classifications; Compliance: MUST

Any sensitive agency data MUST be removed and securely deleted, or encrypted at the end of a session.

**21.4.13.C.05. Control:** System Classification(s): All Classifications; Compliance: MUST

Connections to the agency network MUST be time limited to avoid leaving a session "logged on".

**21.4.13.C.06. Control:** System Classification(s): All Classifications; Compliance: MUST

Communications between the mobile device and the agency network MUST be established through a Virtual Private Network (VPN).

**21.4.13.C.07. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST disable split-tunnelling when using a BYOD device to connect to an agency network (See Section 21.1 – Agency Owned Mobile Devices).

**21.4.13.C.08. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST disable the ability for a BYOD device to establish simultaneous connections (e.g. wireless and cellular) when connected to an agency's network.

**21.4.13.C.09. Control:** System Classification(s): All Classifications; Compliance: MUST

The use of passwords or PINs to unlock the BYOD device MUST be enforced in addition to all other agency authentication mechanisms.

**21.4.13.C.010. Control:** System Classification(s): All Classifications; Compliance: MUST

BYOD device passwords MUST be distinct from any agency access and authentication passwords.

**21.4.13.C.011. Control:** System Classification(s): All Classifications; Compliance: MUST

BYOD passwords MUST be distinct from other fixed or mobile agency network passwords (See Section 16.1 – Identification and Authentication for details on password requirements).

### 21.4.14. Additional Controls

**21.4.14.R.01. Rationale**

There are many new devices and operating system versions being frequently released. It may not be feasible or cost-effective for an agency to support all combinations of device and operating system.

**21.4.14.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD compile a list of approved BYOD devices and operating systems for the guidance of staff.

**21.4.14.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider the implementation of Data Loss Prevention (DLP) technologies.

**21.4.14.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD consider the use of bandwidth limits as a means of controlling data downloads and uploads.

**21.4.14.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD take legal advice on the provisions in their BYOD policy.

# 22. Enterprise systems security

## 22.1. Cloud Computing

### Objective

22.1.1. Cloud systems risks are identified and managed and that Official Information and agency information systems are protected in accordance with Cabinet Directives, the NZISM, the New Zealand Classification System and with other government security requirements and guidance.

### Context

#### Terminology

22.1.2. Terminology and definitions of cloud models and services used in this section are consistent with NIST Special Publication 800-145, The NIST Definition of Cloud Computing, dated September 2011 (see table of References below).

22.1.3. A fundamental construct in the management of risk in cloud environment is that of Trust Zones and Trust Boundaries. A Trust Zone is a zoning construct based on levels of trust, classification, information asset value and essential information security. A Trust Boundary is the interface between two or more Trust Zones. Trust Zones use the principles of separation and segregation to manage sensitive information assets and ensure security policies are consistently applied to all assets in a particular trust Zone. Refer also to Section 22.2 – Virtualisation.

#### Separation and Segregation

22.1.4. Separation and Segregation is determined by system function and the sensitivity of the data the system stores, processes and transmits. One common example is placing systems that require a connection to the Internet into a demilitarized zone (DMZ) that is separated and segregated (isolated) from more sensitive systems.

22.1.5. Separation and Segregation limits the ability of an intruder to exploit a vulnerability with the intent of elevating privileges to gain access to more sensitive systems on the internal network. VLANs may be used to further separate systems by controlling access and providing segregation thus giving additional protection.

#### Mandates and Requirements

22.1.6. In August 2013, the Government introduced their approach to cloud computing, establishing a 'cloud first' policy and an All-of-Government direction to cloud services development and deployment. This is enabled by the Cabinet Minute [CAB Min (13) 37/6B].

22.1.7. Under the 'cloud first' policy state service agencies are expected to adopt approved cloud services either when faced with new procurements, or an upcoming contract extension decision.

22.1.8. In October 2013 the Government approved the GCIO risk and assurance framework for cloud computing, which agencies must follow when they are considering using cloud services [CAB Min (13) 37/6B]. It also directs that no data classified above RESTRICTED should be held in a *public* cloud, whether it is hosted onshore or offshore.

22.1.9. It is important to note that although agencies can outsource **responsibility** to a service provider for implementing, managing and maintaining security controls, they cannot outsource their **accountability** for ensuring their data is appropriately protected.

**Background**

22.1.10. The adoption of cloud technologies and services, the hosting of critical data in the cloud and the risk environment requires that agencies exercise caution. Many cloud users are driven by the need for performance, scalability, resource sharing and cost saving so a comprehensive risk assessment is essential in identifying and managing jurisdictional, sovereignty, governance, technical and security risks.

22.1.11. Typically agencies and other organisations start with a small, private cloud, allowing technical and security architectures, management processes and security controls to be developed and tested and gain some familiarity with cloud technologies and processes. These organisations then progress by using non-critical data, for example email, and other similar applications, in a hybrid, private or public cloud environment.

22.1.12. There are a number of technical risks associated with cloud computing, in addition to the existing risks inherent in organisational systems. Attention must also be paid to the strategic, governance and management risks of cloud computing. Security architecture and security controls also require careful risk assessment and consideration.

22.1.13. Cloud service providers will invariably seek to limit services, liability, compensation or penalties through carefully worded service contracts, which may present particular risks.

22.1.14. Much has been made of the operational cost savings related to cloud technologies, particularly a lower cost of operating. Less obvious are the risks and related cost of managing risk to an acceptable level. It is important to note that short term overall cost increases may, in some cases, be attributed to the adoption of cloud technologies and architectures.

22.1.15. Some valuable work in mapping the cloud risk landscape has been undertaken by such organisations as the Cloud Security Alliance, the US National Institute of Standards and Technology (NIST), the UK's Cloud Industry Forum and the European Network and Information Security Agency (ENISA). It is important to note that the extent of the risk landscape continues to evolve and expand.

**Scope**

22.1.16. This section provides information and some guidance on the risks associated with cloud computing, its implementation and ongoing use. Some controls are specified but agencies will necessarily undertake their own comprehensive risk assessment and select controls to manage those risks.

## References - Guidance

22.1.17. While NOT an exhaustive list, further information on Cloud can be found at:

| Title | Publisher | Source |
|---|---|---|
| **Cabinet Minute of Decision – CAB Min (12) 29/8A – 'Cloud First' Policy** | Cabinet Office | http://ict.govt.nz/assets/Uploads/Documents/CabMin12-cloud-computing.pdf |
| **Cabinet Minute of Decision – CAB Min (13) 37/6B – Cloud Computing Risk and Assurance Framework** | Cabinet Office | http://ict.govt.nz/assets/Cabinet-Papers/Cab-Minute-Cloud-Computing-Risk-and-Assurance-Framework-Oct-2013.pdf |
| **All-of-Government cloud computing approach** | Government Chief Information Officer | http://ict.govt.nz/programmes/government-approach |
| **Requirements for Cloud Computing** | Government Chief Information Officer | https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/ |
| **Cloud Computing: Security and Privacy Considerations** | Government Chief Information Officer | http://ict.govt.nz/assets/ICT-System-Assurance/Cloud-Computing-Information-Security-and-Privacy-Considerations-FINAL2.pdf |
| **Risk Assessment Process: Information Security** | Government Chief Information Officer | http://ict.govt.nz/assets/ICT-System-Assurance/Risk-Assessment-Process-Information-Security.pdf |
| **Government Use of Offshore Information and Communication Technologies (ICT) Service Providers – Advice on Risk Management April 2009** | State Services Commission | http://ict.govt.nz/assets/ICT-System-Assurance/offshore-ICT-service-providers-april-2009.pdf |
| **Cloud Computing a Guide to Making the Right Choices – February 2013** | Office of the Privacy Commissioner (OPC) | http://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/OPC-Cloud-Computing-guidance-February-2013.pdf |
| **Cloud Computing Security Considerations** | Australian Signals Directorate (ASD) | http://www.dsd.gov.au/infosec/cloudsecurity.htm |
| **Cloud Computing Policy and Guidance** | Australian Government Information Management Office (AGIMO) | http://www.finance.gov.au/agict//policy-guides-procurement/cloud |
| **Cloud Control Matrix V3.0.1** | Cloud Security Alliance (CSA) | https://cloudsecurityalliance.org/articles/csas-cloud-control-matrix-ccm-releases-minor-update-to-version-3-0-1/ |
| **Security Guidance for Critical Areas of Focus in Cloud Computing V3.0** | CSA | http://www.cloudsecurityalliance.org/guidance |
| **Top Threats to Cloud Computing** | CSA | http://www.cloudsecurityalliance.org/topthreats.html |
| **Governance, Risk Management and Compliance Stack** | CSA | http://www.cloudsecurityalliance.org/grcstack.html |

| Title | Publisher | Source |
|---|---|---|
| **Security & Resilience in Governmental Clouds - Making an informed decision** | The European Network and Information Security Agency (ENISA) | http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds |
| **Cloud Computing Information Assurance Framework** | ENISA | http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework |
| **Cloud Computing Security Risk Assessment** | ENISA | http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment |
| **Critical Cloud Computing – A CIIP perspective on cloud computing services** | ENISA | www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing/at_download/fullReport |
| **Guidelines on Security and Privacy in Public Cloud Computing ,Special Publication 800-144** | Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (NIST) | http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf |
| **Enterprise Risk Management for Cloud Computing** | The Committee of Sponsoring Organizations of the Treadway Commission (COSO) | http://www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf |
| **Cloud Security** | Cloud Industry Forum | http://www.cloudindustryforum.org/content/cloud-security |
| **OASIS – various reference and guidance documents** | Organization for the Advancement of Structured Information Standards (OASIS) | https://www.oasis-open.org/committees/tc_cat.php?cat=cloud |

## References – Standards

22.1.18. Further standards on Cloud can be found at:

| Title | Publisher | Source |
|---|---|---|
| **The NIST Definition of Cloud Computing , Special Publication 800-145, September 2011** | NIST | http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf |
| **Cloud Computing Synopsis and Recommendations, NIST Special Publication 800-146** | NIST | http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf |
| **Cloud Computing Standards Roadmap, NIST Special Publication 500-291** | NIST | http://www.nist.gov/itl/cloud/upload/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf |
| **Cloud Computing Reference Architecture NIST Special Publication 500-292** | NIST | http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505 |
| ISO/IEC 17788:2014 Information technology -- Cloud computing -- Overview and vocabulary | ISO / IEC | http://www.iso.org |
| ISO/IEC 17789:2014 Information technology -- Cloud computing -- Reference architecture | ISO / IEC | http://www.iso.org |
| ISO/IEC 17826:2012 Information technology -- Cloud Data Management Interface (CDMI) | ISO / IEC | http://www.iso.org |
| ISO/IEC CD 19086-1 Information technology -- Cloud computing -- Service level agreement (SLA) framework and Technology -- Part 1: Overview and concepts | ISO / IEC | http://www.iso.org |
| ISO/IEC NP 19086-2 Information technology -- Cloud computing -- Service level agreement (SLA) framework and Technology -- Part 2: Metrics | ISO / IEC | http://www.iso.org |
| ISO/IEC NP 19086-3 Information technology -- Cloud computing -- Service level agreement (SLA) framework and Technology -- Part 3: Core requirements | ISO / IEC | http://www.iso.org |
| ISO/IEC AWI 19941 Information Technology -- Cloud Computing -- Interoperability and Portability | ISO / IEC | http://www.iso.org |
| ISO/IEC AWI 19944 Information Technology - Cloud Computing - Data and their Flow across Devices and Cloud Services | ISO / IEC | http://www.iso.org |
| ISO/IEC DIS 27017 (In Draft) Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services | ISO / IEC | http://www.iso.org |

| Title | Publisher | Source |
|---|---|---|
| ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors | ISO / IEC | http://www.iso.org |

## PSR references

22.1.19. Relevant PSR requirements can be found at:

| Reference | Title | Source |
|---|---|---|
| **PSR Mandatory Requirements** | GOV2, GOV5, GOV6, INFOSEC1, INFOSEC2, INFOSEC3 and INFOSEC4 | http://www.protectivesecurity.govt.nz |
| **PSR content protocols** | Management protocol for information security | http://www.protectivesecurity.govt.nz |
| **PSR requirements sections** | Handling requirements for protectively marked information and equipment<br>Supply chain security<br>Classify and assign protective markings<br>Assess the risks to your information security | http://www.protectivesecurity.govt.nz |
| **Managing specific scenarios** | Cloud computing<br>Outsourced ICT facilities<br>Outsourcing, Offshoring and supply chains<br>Transacting online with the public | http://www.protectivesecurity.govt.nz |

## Rationale & Controls

### 22.1.20. Applicability

**22.1.20.R.01. Rationale**

Security controls may not be available, cost effective or appropriate for all information classification levels. Much will depend on the cloud computing deployment model adopted. It is important that agencies understand when it is appropriate to use cloud services and how to select appropriate cloud services and service models, based on the classification of the information, any special handling endorsements and associated confidentiality, availability and integrity risks.

**22.1.20.R.02. Rationale**

Systems and information classified CONFIDENTIAL and above require higher levels of protection. This applies in all types of cloud models including private, community, hybrid and public cloud models and deployments.

**22.1.20.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

The use of cloud services and infrastructures for systems and data classified CONFIDENTIAL, SECRET or TOP SECRET MUST be approved by the GCSB.

**22.1.20.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies intending to adopt cloud technologies or services MUST ensure cloud service providers apply the controls specified in this manual to any systems hosting, processing or storing agency data and systems.

**22.1.20.C.03. Control:** System Classification(s): C, S, TS; Compliance: MUST NOT

Agencies MUST NOT use public, hybrid (incorporating a public element), or other external cloud services for systems and data classified CONFIDENTIAL, SECRET or TOP SECRET.

**22.1.20.C.04. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT use public or hybrid (incorporating a public element) cloud services to host, process, store or transmit NZEO endorsed information.

**22.1.20.C.05. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies intending to adopt cloud technologies or services SHOULD obtain formal assurance cloud service providers will apply the controls specified in this manual to any cloud service hosting, processing or storing agency data and systems.

## 22.1.21. Risk Assessment

**22.1.21.R.01. Rationale**

The adoption of cloud technologies will introduce a wide range of technology and information system risks *in addition* to the risks that already exist for agency systems. It is vital that these additional risks are identified and assessed in order to select appropriate controls and countermeasures. Trust boundaries must be defined to assist in determining effective controls and where these controls can best be applied.

**22.1.21.R.02. Rationale**

The **responsibility** for the implementation, management and maintenance of controls will depend on the service model and deployment model (refer to NIST SP800-145) used in the delivery of cloud services.

**22.1.21.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies intending to adopt cloud technologies or services MUST conduct a risk assessment *before* implementation or adoption.

**22.1.21.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies intending to adopt cloud technologies or services MUST determine trust boundaries *before* implementation.

**22.1.21.C.03. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies intending to adopt cloud technologies or services MUST determine where the responsibility (agency or cloud service provider) for implementing, managing and maintaining controls lies in accordance with agreed trust boundaries.

**22.1.21.C.04. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure cloud risks for any cloud service adopted are understood and formally accepted by the Agency Head or Chief Executive (or their formal delegate) and the agency's Accreditation Authority.

**22.1.21.C.05. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST consult with the GCIO to ensure the strategic and other cloud risks are comprehensively assessed.

**22.1.21.C.06. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies procuring or using cloud services to be used by multiple agencies MUST ensure all interested parties formally agree the risks, controls and any residual risks of such cloud services.

**22.1.21.C.07. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies using cloud services MUST ensure they have conducted a documented risk assessment, accepted any residual risks, and followed the endorsement procedure required by the GCIO.

### 22.1.22. Offshore Services

**22.1.22.R.01. Rationale**

Cloud services hosted offshore introduce several additional risks, in particular, jurisdictional, sovereignty and privacy risks. Foreign owned cloud service providers operating in New Zealand, are subject to New Zealand legislation and regulation. They may, however, also be subject to a foreign government's privacy, lawful access and data intercept legislation.

**22.1.22.R.02. Rationale**

The majority of these jurisdictional, sovereignty and privacy risks cannot be adequately managed with controls available today. They must therefore be carefully considered and accepted by the Agency Head or Chief Executive before the adoption of such cloud services.

**22.1.22.R.03. Rationale**

Some cloud services hosted within New Zealand may be supported by foreign based technical staff. This characteristic introduces a further risk element to the use of foreign-owned cloud service providers.

**22.1.22.R.04. Rationale**

Further complexity can be introduced when All-of-Government or multi-agency systems are deployed or integrated with cloud services. Any security breach can affect several agencies and compromise large or aggregated data sets.

**22.1.22.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies using cloud services hosted offshore MUST ensure jurisdictional, sovereignty and privacy risks are fully considered and formally accepted by the Agency Head or Chief Executive and the agency's Accreditation Authority.

**22.1.22.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies using cloud services hosted offshore MUST ensure that the agency retains ownership of its information in any contract with the cloud service provider.

**22.1.22.C.03. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies using cloud services hosted offshore and connected to All-of-Government systems MUST ensure they have conducted a risk assessment, accepted any residual risks, and followed the endorsement procedure required by the GCIO.

**22.1.22.C.04. Control:** System Classification(s): C, S, TS; Compliance: MUST NOT

Agencies MUST NOT use cloud services hosted offshore for information or systems classified CONFIDENTIAL, SECRET or TOP SECRET.

**22.1.22.C.05. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT use cloud services hosted offshore for information with an NZEO endorsement.

**22.1.22.C.06. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT use cloud services hosted offshore *unless:*

- privacy, information sensitivity and information value has been fully assessed by the agency;
- a comprehensive risk assessment is undertaken by the agency;
- controls to manage identified risks have been specified by the agency; and
- the cloud service provider is able to provide adequate assurance that these controls have been properly implemented *before* the agency uses the cloud service.

## 22.1.23. System Availability

**22.1.23.R.01. Rationale**

The availability of agency systems, business functionality and any customer or client online services, is subject to additional risks in an outsourced cloud environment. A risk assessment will include consideration of business requirements on availability in a cloud environment.

**22.1.23.R.02. Rationale**

Risks to business functionality may include service outages, such as communications, data centre power, back and other failures or interruptions. Entity failures such the merger, acquisition or liquidation of the cloud service provider may also present a significant business risk to availability.

**22.1.23.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies intending to adopt cloud technologies or services MUST consider the risks to the availability of systems and information in their design of cloud systems architectures and supporting controls and governance processes.

**22.1.23.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Any contracts for the provision of cloud services MUST include service level, availability, recoverability and restoration provisions.

**22.1.23.C.03. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST ensure contracts with cloud service providers include provisions to manage risks associated with the merger, acquisition, liquidation or bankruptcy of the service provider and any subsequent termination of cloud services.

### 22.1.24. Unauthorised Access

**22.1.24.R.01. Rationale**

Cloud service providers may not provide adequate physical security and physical and logical access controls to meet agencies requirements. An assessment of cloud service risks will include physical and systems security. Refer also to Chapter 19 – Gateway Security, Section 22.2 – Virtualisation and Section 22.3 – Virtual Local Area Networks.

**22.1.24.R.02. Rationale**

Some cloud services hosted within New Zealand may be supported by technical staff, presenting additional risk. In some cases the technical staff are based offshore. The use of encryption can provide additional assurance against unauthorised access – refer to Chapter 17 – Cryptography.

**22.1.24.R.03. Rationale**

Data Loss Prevention (DLP) technologies and techniques are implemented to safeguard sensitive or critical information from leaving the organisation. They operate by identifying unauthorised access and data exfiltration and take remedial action by monitoring, detecting and blocking unauthorised attempts to exfiltrate data. For DLP to be effective, all data states (processing, transmission and storage) are monitored.

**22.1.24.C.01. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies intending to adopt cloud technologies or services SHOULD ensure cloud service providers apply the physical, virtual and access controls specified in this manual for agency systems and data protection.

**22.1.24.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies intending to adopt cloud technologies or services SHOULD apply separation and access controls to protect data and systems where support is provided by offshore technical staff.

**22.1.24.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies intending to adopt cloud technologies or services SHOULD apply controls to detect and prevent unauthorised data transfers and multiple or large scale data transfers to offshore locations and entities.

**22.1.24.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies intending to adopt cloud technologies or services SHOULD consider the use of encryption for data in transit and at rest.

### 22.1.25. Incident Handling and Management

**22.1.25.R.01. Rationale**

Cloud service providers may not provide the same level of incident identification and management as provided by agencies. In some cases, these services will attract additional costs. Careful management of contracts is required to ensure agency requirements for incident detection and management are fully met when adopting cloud services.

**22.1.25.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST include incident handling and management services in contracts with cloud service providers.

**22.1.25.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop and implement incident identification and management processes in accordance with this manual (See Chapter 6 – Information Security Monitoring, Chapter 7 – Information Security Incidents, Chapter 9 – Personnel Security and Chapter 16 – Access Control).

### 22.1.26. Backup, Recovery Archiving and Data Remanence

**22.1.26.R.01. Rationale**

Cloud service providers will invariably provide some business continuity and disaster recovery plans, including system and data backup, for their own operational purposes. These plans may not include customer data or systems. Where cloud service providers do not adequately meet agency business requirements, an agency defined backup and recovery plan may be necessary.

**22.1.26.R.02. Rationale**

Residual information remaining on a device or storage media after clearing or sanitising the device or media is described as data remanence. This characteristic is sometimes also described as data persistence, although this description may include the wider implication of multiple copies.

**22.1.26.R.03. Rationale**

Full consideration of risks associated with data remanence and data persistence is required to ensure agency requirements for backup, recovery, archiving and data management is included in any cloud service contract.

**22.1.26.R.04. Rationale**

In addition to backups, cloud service providers may also archive data. Multi-national or foreign based cloud service providers may have established data centres in several countries. Backup and archiving is invariably automated and there may be no feasible method of determining where and in what jurisdiction the data have been archived. This can create an issue of data remanence and persistence where cloud service contracts are terminated but not all agency data can be effectively purged or deleted from the provider's systems.

**22.1.26.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop and implement a backup, recovery and archiving plan and supporting procedures (See Section 6.4 – Business Continuity and Disaster Recovery).

**22.1.26.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST include a data purge or secure delete process in any cloud service contracts.

**22.1.26.C.03. Control:** System Classification(s): All Classifications; Compliance: MUST

Any data purge or secure delete process in any cloud service contracts MUST be independently verifiable.

### 22.1.27. User Awareness and Training

**22.1.27.R.01. Rationale**

The introduction of cloud services will introduce change to the appearance and functionality of systems, how users access agency systems and types of user support. It is essential that users are aware of information security and privacy concepts and risks associated with the services they use.

Support provided by the cloud service provider may attract additional charges.

**22.1.27.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST develop and implement user awareness and training programmes to support and enable safe use of cloud services (See Section 9.1 – Information Security Awareness and Training).

# 22.2. Virtualisation

## Objective

22.2.1. To identify virtualisation specific risks and apply mitigations to minimise risk and secure the virtual environment.

## Context

22.2.2. Virtualisation is the software simulation of the components of an information system and may include the simulation of hardware, operating systems, applications, infrastructure and storage. Underlying the simulation is hardware and control or simulation software, often described as a virtual machine (VM).

22.2.3. A Hypervisor is a fundamental component of a virtual environment and provides a supervisory function and framework that enables multiple operating systems, often described as "Guest Operating Systems", to run on a single physical device.

22.2.4. A fundamental construct in the management of risk in virtual environments is that of Trust Zones and Trust Boundaries. A Trust Zone is a zoning construct based on levels of trust, classification, information asset value and essential information security. A Trust Boundary is the interface between two or more Trust Zones. Trust Zones use the principles of separation and segregation to manage sensitive information assets and ensure security policies are consistently applied to all assets in a particular trust Zone. As assets are added to a Trust Zone, they inherit the security policies set for that Trust Zone.

22.2.5. Trust Zones will also apply the Principal of Least Privilege, which requires that each element in the network is permitted to access only those other network elements that are required for the node to perform its business function.

22.2.6. Virtualisation is radically changing how agencies and other organisations select, deploy implement and manage ICT. While offering significant benefits in efficiency, resource consolidation and utilisation of CIT assets, virtualisation can add risks to the operation of a system and the security of the data processed and managed by that system.

22.2.7. Virtualisation adds layers of technology and can combine many, traditionally discrete and physically separate components, into a single physical system. This consolidation invariably creates greater impact if faults occur or the system is compromised. Virtual systems are designed to be dynamic and to facilitate the movement and sharing of data. This characteristic is also a prominent attack vector and can make the enforcement and maintenance of security boundaries much more complex.

22.2.8. Virtualisation is susceptible to the same threats and vulnerabilities as traditional ICT assets but traditional security offers limited visibility of virtualised environments where the assets configurations and security postures are constantly changing. Incidents in virtualised environments can rapidly escalate across multiple services, applications and data sets, causing significant damage and making recovery complex.

### Virtualisation risks

22.2.9. Virtualisation risks can be considered in four categories:

- Risks directly related to virtualisation technologies;
- Systems architecture; implementation and management;
- The usage and business models; and
- Generic technology risks.

### Mitigations

22.2.10. The controls described elsewhere in this manual deal with generic technology risks. Important steps in risk mitigation for virtual environments include:

- Identify and accurately characterise all deployed virtualisation and security measures beyond built-in hypervisor controls on VMs.
- Comparing security controls against known threats and industry standards to determine gaps and select appropriate controls.
- Identify and implement anti-malware tools, intrusion prevention and detection, active vulnerability scanning and systems security management and reporting tools.

## References

22.2.11. Further references can be found at:

| Title | Publisher | Source |
|---|---|---|
| **NIST Special Publication 800-125, Guide to Security for Full Virtualisation Technologies** | NIST | http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf |
| **The Security Technical Implementation Guides,** | Defense Information Systems Agency, | http://iase.disa.mil/stigs/Pages/index.aspx |
| **Virtualization Security Checklist** | ISACA | http://www.isaca.org/Knowledge-Center/Research/Documents/Virtualization-Security-Checklist-26Oct2010-Research.pdf |
| **A Guide to Virtualization Hardening Guides** | SANS | http://www.sans.org/reading_room/analysts_program/vmware-guide-may-2010.pdf |
| **Virtual Machine Security Guidelines** | The Center for Internet Security | http://benchmarks.cisecurity.org/tools2/vm/CIS_VM_Benchmark_v1.0.pdf |
| **Software-Defined Networking (SDN) Definition** | Open Networking Foundation | https://www.opennetworking.org/sdn-resources/sdn-definition |
| **Network segmentation and segregation** | ASD | http://www.asd.gov.au/publications/csocprotect/Network_Segmentation_Segregation.pdf |

## Rationale & Controls

### 22.2.12. Functional segregation between servers

#### 22.2.12.R.01. Rationale

Agencies may implement segregation through the use of techniques to restrict a process to a limited portion of the file system, but this is often less effective. Virtualisation technology MUST be carefully architected to avoid cascade failures.

#### 22.2.12.R.02. Rationale

The key element in separating security domains of differing classifications is physical separation. Current virtualisation technology cannot guarantee separation.

#### 22.2.12.R.03. Rationale

The use of virtualisation technology within a security domain is a recognised means of efficiently architecting a system.

#### 22.2.12.C.01. Control: System Classification(s): All Classifications; Compliance: MUST NOT

Virtualisation technology MUST NOT be used for functional segregation between servers of different classifications.

#### 22.2.12.C.02. Control: System Classification(s): C, S, TS; Compliance: MUST NOT

Virtualisation technology MUST NOT be used for functional segregation between servers in different security domains at the same classification.

#### 22.2.12.C.03. Control: System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure that functional segregation between servers is achieved by:

- physically, using single dedicated machines for each function; or
- using virtualisation technology to create separate virtual machines for each function within the same security domain.

#### 22.2.12.C.04. Control: System Classification(s): All Classifications; Compliance: SHOULD NOT

Virtualisation technology SHOULD NOT be used for functional segregation between servers in different security domains at the same classification.

### 22.2.13. Risk Management

**22.2.13.R.01. Rationale**

Where virtualisation technologies are to be used, risk identification, assessment and management are important in order to identify virtualisation specific risks, threats and treatments.

**22.2.13.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST undertake a virtualisation specific risk assessment in order to identify risks, related risk treatments and controls.

**22.2.13.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD undertake a virtualisation specific risk assessment in order to identify risks and related risk treatments.

### 22.2.14. Systems Architecture

**22.2.14.R.01. Rationale**

It is important to include virtualisation specific concepts, constraints, mitigations and controls in the design of systems architectures that propose using virtualisation technologies, in order to gain maximum advantage from the use of these technologies and to ensure security of systems and data is maintained.

**22.2.14.R.02. Rationale**

Virtual environments enable a small number of technical specialists to cover a wide range of activities such as network, security, storage and application management. Such activities are usually undertaken as discrete activities by a number of individuals in a physical environment. To remain secure and correctly and safely share resources, VMs must be designed following the principles of separation and segregation through the establishment of trust zones.

**22.2.14.R.03. Rationale**

Software-defined networking (SDN) is an approach to networking in which control is decoupled from hardware and managed by a separate application described as a controller. SDNs are intended to provide flexibility by enabling network engineers and administrators to respond to rapidly changing business requirements. Separation and segregation principles also apply to SDNs.

**22.2.14.R.04. Rationale**

In addition to segregation of key elements, VM security can be strengthened through functional segregation. For example, the creation of separate security zones for desktops and servers with the objective of minimising intersection points.

**22.2.14.R.05. Rationale**

Poor control over VM deployments can lead to breaches where unauthorised communication and data exchange can take place between VMs. This can create opportunity for attackers to gain access to multiple VMs and the host system.

**22.2.14.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST architect virtualised systems and environments to enforce the principles of separation and segregation of key elements of the system using trust zones or security domains.

**22.2.14.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST NOT

Agencies MUST NOT permit the sharing of files or other operating system components between host and guest operating systems.

**22.2.14.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD architect virtualised systems and environments to enforce the principles of separation and segregation of key elements of the system using trust zones.

**22.2.14.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD design virtualised systems and environments to enable functional segregation within a security domain.

**22.2.14.C.05. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD harden the host operating systems following an agency or other approved hardening guide.

**22.2.14.C.06. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD separate production from test or development virtual environments.

**22.2.14.C.07. Control:** System Classification(s): All Classifications; Compliance: SHOULD NOT

Agencies SHOULD NOT permit the sharing of files or other operating system components between host and guest operating systems.

### 22.2.15. Systems Management

**22.2.15.R.01. Rationale**

VMs are easy to deploy, often without formal policies or controls to manage the creation, management and decommissioning of VMs. This is sometimes described as "VM sprawl", which is the unplanned proliferation of VMs. Attackers can take advantage of poorly managed and monitored resources. More deployments also mean more failure points, so VM sprawl can create operational difficulties even if no malicious activity is involved.

**22.2.15.R.02. Rationale**

A related difficulty occurs with **unsecured VM migration** when a VM is migrated to a new host, and security policies and configuration are not updated. VMs may also be migrated to other physical servers with little or no indication to users that a migration has occurred. Unsecured migration can introduce vulnerabilities through poor configuration and incomplete security and operational monitoring.

**22.2.15.R.03. Rationale**

Denial of service attacks can be designed specifically to exploit virtual environments. These attacks range from traffic flooding to the exploit of the virtual environment host's own resources.

**22.2.15.R.04. Rationale**

The ability to monitor VM backbone network traffic is vital to maintain security and operations. Conventional methods for monitoring network traffic are generally not effective because the traffic is largely contained and controlled within the virtual environment. Careful selection and implementation of hypervisors will ensure effective monitoring tools are enabled, tested and monitored.

**22.2.15.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST ensure a VM migration policy and related SOPs are implemented.

**22.2.15.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST implement controls to prohibit unauthorised VM migrations within a virtual environment or between physical environments.

**22.2.15.C.03. Control:** System Classification(s): C, S, TS; Compliance: MUST

Agencies MUST implement controls to safely decommission VMs when no longer required, including elimination of images, snapshots, storage, backup, archives and any other residual data.

**22.2.15.C.04. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD ensure a VM migration policy and related SOPs are implemented.

**22.2.15.C.05. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD implement controls to prohibit unauthorised VM migrations within a virtual environment or between physical environments.

**22.2.15.C.06. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD implement controls to safely decommission VMs when no longer required.

**22.2.15.C.07. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD implement security and operational management and monitoring tools which include the following minimum capabilities:

- Identify VMs when initiated;
- Validate integrity of files prior to installation;
- Scan new VMs for vulnerabilities and misconfigurations;
- Load only minimum operating system components and services;
- Set resource usage limits;
- Establish connections to peripherals only as required;
- Ensure host and guest time synchronisation;
- Detect snapshot rollbacks and scans after restores;
- Track asset migration; and
- Monitor the security posture of migrated assets.

### 22.2.16. Authentication and Access

**22.2.16.R.01. Rationale**

VM sprawl can compromise authentication and access procedures, identity management, and system logging. This can be complicated with the use of customer-facing interfaces, such as websites.

**22.2.16.R.02. Rationale**

Host and guest interactions and their system vulnerabilities can magnify virtual system vulnerabilities. The co-hosting and multi-tenancy nature of virtual systems and the existence of multiple data sets can make a serious attack on a virtual environment particularly damaging.

**22.2.16.R.03. Rationale**

A guest OS can avoid or ignore its VM encapsulation to interact directly with the hypervisor either as a direct attack or through poor design, configuration and control. This can give the attacker access to all VMs in the virtual environment and potentially, the host machine. Described as a "VM escape", it is considered to be one of the most serious threats to virtual systems.

**22.2.16.R.04. Rationale**

Hyperjacking is a form of attack that takes direct control of the hypervisor in order to gain access to the hosted VMs and data. This attack typically requires direct access to the hypervisor. While technically challenging, hyperjacking is considered a real-world threat.

**22.2.16.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST maintain strong physical security and physical access controls.

**22.2.16.C.02. Control:** System Classification(s): All Classifications; Compliance: MUST

Agencies MUST maintain strong authentication and access controls.

**22.2.16.C.03. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Agencies SHOULD maintain strong data validation checks.

# 22.3. Virtual Local Area Networks

## Objective

22.3.1. Virtual local area networks (VLANs) are deployed in a secure manner that does not compromise the security of information and systems.

## Context

### Scope

22.3.2. This section covers information relating to the use of VLANs within agency networks.

### Multiprotocol Label Switching

22.3.3. For the purposes of this section Multiprotocol Label Switching (MPLS) is considered to be equivalent to VLANs and is subject to the same controls.

### Exceptions for connectivity

22.3.4. A single network, managed in accordance with a single SecPlan, for which some functional separation is needed for administrative or similar reasons, can use VLANs to achieve that functional separation.

22.3.5. VLANs can also be used to separate VTC and IPT traffic from data traffic at the same classification (See Section 18.3 – Video and Telephony Conferencing and Internet Protocol Telephony).

### Software Defined Networking (SDN)

22.3.6. Software-defined networking (SDN) is an approach to networking in which control is decoupled from hardware and managed by a separate application described as a controller. SDNs are intended to provide flexibility by enabling network engineers and administrators to respond to rapidly changing business requirements.

22.3.7. Separation and Segregation principles also apply to SDNs. Refer to Section 22.2 – Virtualisation.

## References

22.3.8. Further references can be found at:

| Title | Publisher | Source |
|---|---|---|
| **IEEE 802.1Q-2011 IEEE Standard for Local and Metropolitan area networks – Media Access Control (MAC) Bridges, and Virtual Bridged Local Area Networks.** | Institute of Electrical and Electronics Engineers (IEEE) | http://standards.ieee.org |
| **Inter-Switch Link and IEEE 802.1Q Frame Format** | CISCO | http://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.html |
| **Dynamic Trunking Protocol (DTP)** | CISCO | http://www.cisco.com/c/en/us/tech/lan-switching/dynamic-trunking-protocol-dtp/index.html |

## Rationale & Controls

### 22.3.9. Using VLANs

**22.3.9.R.01. Rationale**

Limiting the sharing of a common (physical or virtual) switch between VLANs of differing classifications reduces the chance of data leaks that could occur due to VLAN vulnerabilities. Furthermore, disabling trunking on physical switches that carry VLANs of differing security domains will reduce the risk of data leakage across the VLANs. The principles of separation and segregation must be applied to all network designs and architectures.

**22.3.9.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

The principles of separation and segregation MUST be applied to the design and architecture of VLANs.

**22.3.9.C.02. Control:** System Classification(s): C, S, TS; Compliance: MUST NOT

Agencies MUST NOT use VLANs between classified networks and any other network of a lower classification.

**22.3.9.C.03. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

Agencies MUST NOT use VLANs between any classified network and any unclassified network.

**22.3.9.C.04. Control:** System Classification(s): All Classifications; Compliance: MUST NOT

VLAN trunking MUST NOT be used on switches managing VLANs of differing security domains.

### 22.3.10. Configuration and administration

**22.3.10.R.01. Rationale**

When administrative access is limited to originating from the highest classified network on a switch, the security risk of a data spill is reduced.

**22.3.10.C.01. Control:** System Classification(s): All Classifications; Compliance: MUST

Administrative access MUST be permitted only from the most trusted network.

### 22.3.11. Disabling unused ports

**22.3.11.R.01. Rationale**

Disabling unused ports on a switch will reduce the opportunity for direct or indirect attacks on systems.

**22.3.11.C.01. Control:** System Classification(s): C, S, TS; Compliance: MUST

Unused ports on the switches MUST be disabled.

**22.3.11.C.02. Control:** System Classification(s): All Classifications; Compliance: SHOULD

Unused ports on the switches SHOULD be disabled.

# 23. Supporting Information

## 23.1 Glossary of Abbreviations

| Abbreviation | Meaning |
|---|---|
| **3DES** | Triple Data Encryption Standard |
| **AES** | Advanced Encryption Standard |
| **AH** | Authentication Header |
| **AISEP** | Australasian Information Security Evaluation Program |
| **AoG** | All-of-Government |
| **AS** | Australian Standard |
| **ASD** | Australian Signals Directorate |
| **BYOD** | Bring Your Own Device |
| **BYOK** | Bring Your Own Keys |
| **CC** | Common Criteria |
| **CCRA** | Common Criteria Recognition Arrangement |
| **CDS** | Cross-Domain Solution |
| **CEO** | Chief Executive Officer |
| **CIO** | Chief Information Officer |
| **CISO** | Chief Information Security Officer |
| **COMSEC** | Communications Security |
| **CSO** | Chief Security Officer |
| **DdoS** | Distributed Denial-Of-Service |
| **DH** | Diffie-Hellman |
| **DIS** | Draft International Standard |
| **DKIM** | Domainkeys Identified Mail |
| **DoS** | Denial-Of-Service |
| **DSA** | Digital Signature Algorithm |
| **EAL** | Evaluation Assurance Level |
| **EAP-TLS** | Extensible Authentication Protocol-Transport Layer Security |
| **ECDH** | Elliptic Curve Diffie-Hellman |
| **ECDSA** | Elliptic Curve Digital Signature Algorithm |
| **EEPROM** | Electrically Erasable Programmable Read-Only Memory |
| **EPL** | Evaluated Products List |
| **EPLD** | Evaluated Products List – Degausser |
| **EPROM** | Erasable Programmable Read-Only Memory |
| **ESP** | Encapsulating Security Payload |
| **FIPS** | Federal Information Processing Standard |

| | |
|---|---|
| **FTL** | Flash Transition Layer |
| **GCIO** | NZ Government Chief Information Officer |
| **GCSB** | Government Communications Security Bureau |
| **GPU** | Graphics Processing Unit |
| **HA** | High Availability |
| **HB** | Handbook |
| **HGCE** | High Grade Cryptographic Equipment |
| **HGCP** | High Grade Cryptographic Products |
| **HMAC** | Hashed Message Authentication Code |
| **HSM** | Hardware Security Module |
| **HTTP** | Hypertext Transfer Protocol |
| **HTTPS** | Hypertext Transfer Protocol Secure |
| **HYOK** | Hold Your Own Keys |
| **ICT** | Information And Communications Technology |
| **IDS** | Intrusion Detection System |
| **IEC** | International Electrotechnical Commission |
| **IEEE** | Institute Of Electrical And Electronics Engineers |
| **IETF** | International Engineering Task Force |
| **IKE** | Internet Key Exchange |
| **IM** | Instant Messaging |
| **IMS** | IP Multimedia Subsystem |
| **IODEF** | Incident Object Description Exchange Format |
| **IP** | Internet Protocol |
| **IPSec** | Internet Protocol Security |
| **IR** | Infra-Red |
| **IRC** | Internet Relay Chat |
| **IPT** | Internet Protocol Telephony |
| **IRP** | Incident Response Plan |
| **ISAKMP** | Internet Security Association Key Management Protocol |
| **ISO** | International Organization For Standardization |
| **ITSEC** | Information Technology Security Evaluation Criteria |
| **ITSM** | Information Technology Security Manager |
| **IWF** | Inter-Working Function |
| **KMP** | Key Management Plan |
| **MDM** | Mobile Device Manager |
| **MFD** | Multifunction Device |
| **MMS** | Multimedia Message Service |
| **MSL** | (New Zealand) Measurement Standards Laboratory |

| | |
|---|---|
| **NAND** | Flash Memory Named After The NAND Logic Gate |
| **NAND** | NOT AND – A Binary Logic Operation |
| **NDPP** | Network Device Protection Profile |
| **NIST** | National Institute Of Standards And Technology |
| **NOR** | Flash Memory Named After The NOR Logic Gate |
| **NOR** | NOT OR – A Binary Logic Operation |
| **NTP** | Network Time Protocol |
| **NZCSI** | New Zealand Communications-Electronic Security Instruction |
| **NZCSS** | New Zealand Communications Security Standard |
| **NZ e-GIF** | New Zealand E-Government Interoperability Framework |
| **NZEO** | New Zealand Eyes Only |
| **NZISM** | New Zealand Information Security Manual |
| **NZS** | New Zealand Standard |
| **OTP** | One-Time Password |
| **PAM** | Privileged Access Mangement |
| **PBX** | Private Branch Exchange |
| **PED** | Portable Electronic Device |
| **PIN** | Personal Identification Number |
| **PKI** | Public Key Infrastructure |
| **PP** | Protection Profile |
| **PSR** | Protective Security Requirements |
| **PSTN** | Public Switched Telephone Network |
| **QoS** | Quality of Service |
| **RAM** | Random Access Memory |
| **RF** | Radio Frequency |
| **RFC** | Request For Comments |
| **RSA** | Rivest-Shamir-Adleman |
| **RTP** | Real-Time Transport Protocol |
| **SBC** | Session Border Controller |
| **SCEC** | Security Construction And Equipment Committee |
| **SCI** | Sensitive Compartmented Information |
| **SCIF** | Sensitive Compartmented Information Facility |
| **SDN** | Software Defined Networking |
| **SecPlan** | System Security Plan |
| **SecPol** | System Security Policy |
| **SitePlan** | System Site Plan |
| **SHA** | Secure Hashing Algorithm |
| **SIM** | Subscriber Identity Module |

| | |
|---|---|
| **SIP** | Session Initiation Protocol |
| **SLA** | Service Level Agreement |
| **S/MIME** | Secure Multipurpose Internet Mail Extension |
| **SMS** | Short Message Service |
| **SOE** | Standard Operating Environment |
| **SOP** | Standard Operating Procedure |
| **SP** | Special Publication |
| **SPF** | Sender Policy Framework |
| **SRMP** | Security Risk Management Plan |
| **SSD** | Solid State Drive |
| **SSH** | Secure Shell |
| **SSL** | Secure Sockets Layer |
| **TLS** | Transport Layer Security |
| **TOE** | Target of Evaluation (in Common Criteria) |
| **TOE** | Trusted Operating Environment |
| **UC** | Unified Communication |
| **UTC** | Co-ordinated Universal Time |
| **VLAN** | Virtual Local Area Network |
| **VoIP** | Voice Over Internet Protocol |
| **VPN** | Virtual Private Network |
| **WAP** | Wireless Access Point |
| **WEP** | Wired Equivalent Privacy |
| **WLAN** | Wireless Local Area Network |
| **WPA2** | Wi-Fi Protected Access 2 |
| **XAUTH** | Ike Extended Authentication |

## 23.2 Glossary of Terms

| Term | Meaning |
|---|---|
| **802.11** | The Institute of Electrical and Electronics Engineers standard defining WLAN communications. Formally titled IEEE 82.11. |
| **Access Gateway** | An architectural construct that provides the system user access to multiple security domains from a single device, typically a workstation. |
| **Accountable** | Required or expected to justify actions or decisions; being answerable and responsible for those actions & decisions. |
| **Accountable Material** | Accountable information, an accountable item or accountable material refers to the accountability controls applied to specified information, equipment or materials. Accountable information, items or materials are usually uniquely identifiable (usually a serial or identification number) and are tracked from acquisition or creation to final disposal. Safe custody is a fundamental and is achieved through:<br>• is easily to compute;<br>• will usually output a significantly different value, even for small changes made to the input; and<br>• can detect many types of data corruptions.<br>• allocation to a specific individual (issued or responsibility designated);<br>• allocation or designation of responsibility may also require a specific briefing related to the handling, care and protection of particular types of classified information and COMSEC equipment;<br>• the allocation, issue or designation being recorded;<br>• strict controls over access and movement (special handling requirements);<br>• maintenance of a register (manual or electronic); and<br>• regular audits to ensure accountability conditions continue to be adhered to and any briefings are current.<br>As a general rule, accountable information, items or materials are afforded physical security protection by specifying special handling and accountability conditions. Examples may include cryptographic or COMSEC equipment, other high value equipment, money, computers or information subject to privacy legislation and regulation.<br>Cryptographic or COMSEC equipment and any information classified as CONFIDENTIAL, SECRET or TOP SECRET is accountable by definition. |

| Term | Meaning |
|---|---|
| **Accountability** | Most contemporary definitions include two key elements:<br>• the conferring of responsibility and authority; and<br>• the answering for the use of that authority.<br><br>Accountability exists when the performance of tasks or functions by an individual or organisation, are subject to another's oversight, direction or request that they provide information or justification for their actions.<br><br>Answering for the use of authority means reporting, explaining actions, assuming obligations, and submitting to outside or external judgement. Having responsibility means having the authority to act, the power to control and the freedom to decide. It also means that one must behave rationally, reliably and consistently in exercising judgement. |
| **Accreditation** | A procedure by which an authoritative body gives formal recognition, approval and acceptance of the associated residual security risk with the operation of a system and issues a formal approval to operate the system. |
| **Accreditation Authority** | The authoritative body or individual responsible for systems accreditation. |
| **Agency** | New Zealand Government departments, authorities, agencies or other bodies established in relation to public purposes, including departments and authorities staffed under the Public Service Act. |
| **Agency Head** | The government employee with ultimate responsibility for the secure operation of agency functions, whether performed in-house or outsourced. |
| **All-of-Government** | Refers to the entire New Zealand state sector. |
| **Application Whitelisting** | An approach in which all executables and applications are prevented from executing by default, unless explicitly permitted. |
| **Asset** | Anything of value to an agency, such as IT equipment and software, information, personnel, documentation, reputation and public confidence. |
| **Attack Surface** | The IT equipment and software used in a system. The greater the attack surface the greater the chances are of an attacker finding an exploitable vulnerability. |
| **Audit** | A structured process of examination, review, assessment, testing and reporting against defined requirements or objectives. Auditors should be independent any IT system, business process, agency, function, site, supplier or other subject area being audited. |
| **Australasian Information Security Evaluation Program** | A program under which evaluations are performed by impartial companies against the Common Criteria. The results of these evaluations are then certified by ASD, which is responsible for the overall operation of the program. |
| **Authentication Header** | Part of the protocol used for authentication within IPSec, it provides authentication, integrity and anti-replay for the entire packet (both the header and data payload). |

| Term | Meaning |
|---|---|
| **Baseline** | Information and controls that are used as a minimum implementation or starting point to provide a consistent minimum standard of systems security and information assurance. |
| **Blacklist** | A set of items to be excluded, blocked or prevented from execution. It is the opposite of a whitelist which confirms that items are acceptable. |
| **Brute Force Attack** | A brute force attack is an automated continuous attack is conducted against a system or file to decrypt or discover passwords and data. Often used as an entry point for privilege escalation. |
| **Cascaded Connections** | Links to other systems that occur when connected systems are themselves connected to other systems. This may result in multiple indirect (cascaded) connections to systems with differing security implementations, data, equipment and other aspects important for the security and assurance of systems. |
| **Caveat** | A marking that indicates that the information has special requirements in addition to those indicated by the classification and any prescribed endorsement. The term covers codewords, source codewords, releasability indicators and special-handling caveats. See also Endorsements. |
| **Certification** | The process by which the controls and management of an information system is formally evaluated against any specific risks identified and the requirements of the NZISM. A key output is a formal assurance statement that the system conforms to the requirements of the NZISM. |
| **Certification Authority** | An official with the authority to assert that a system complies with prescribed controls within a standard. |
| **Certification Report** | A report generated by a certification body of a Common Criteria scheme that provides a summary of the findings of an evaluation. |
| **Characterisation** | In the NZISM "characterisation" is a synonym for "unique identifier".<br><br>This is typically applied to an operating system, programme, library or other programmatic element in the form of a checksum which can be calculated from a "known good" component and stored for comparison should there be any concern that components have been damaged or compromised.<br><br>Forensic methods may also provide characterisation indicators but are likely to require additional levels of expertise.<br><br>See also **Checksum** and **Hash.** |

| Term | Meaning |
|---|---|
| **Checksum** | A checksum verifies or **checks** the integrity of data.<br><br>A good checksum algorithm:<br>• is easily to compute;<br>• will usually output a significantly different value, even for small changes made to the input; and<br>• can detect many types of data corruptions.<br><br>Checksums are often used to verify the integrity of operating system, programme, library or other programmatic elements, images and firmware updates. Checksums typically range in length from one to 64-bits, depending on the intended usage and algorithm used to determine the checksum.<br><br>Checksums are related to hash functions, fingerprints, randomisation functions, and cryptographic hash functions. Note, however, each of those concepts are distinct, have different applications and therefore different design goals. Check digits and parity bits are special uses of checksums. It is important to recognise that, although related, a hash is not a checksum.<br><br>See also **Hash.** |
| **Chief Information Security Officer** | A senior executive with overall responsibility for the governance and management of information risks within an agency. This may include coordination between security, ICT and business functions to ensure risks are properly identified and managed. |
| **Classified Information** | Government information that requires protection from unauthorised disclosure. |
| **Classified Systems** | Systems that process, store or communicate classified information. |
| **Codewords** | A short (usually a single word) descriptions of a project, operation or activity, typically assigned used for reasons of reliability, clarity, brevity, or secrecy. Each **code word** is assembled in accordance with the specific rules of the code and assigned a unique meaning. Synonymous with *Codename*. |
| **Coercivity** | A measure of the resistance of a magnetic material to changes in magnetisation, equivalent to the field intensity necessary to demagnetise any magnetised material. The amount of coercive force required to reduce any residual magnetic induction to zero. Normally used in describing the characteristics of degaussing magnetic media (see Degausser). |
| **Common Criteria** | A formal, internationally-recognised scheme, defined in the ISO 15408 standard. This standard describes process to specify, design, develop, test, evaluate and certify as secure IT systems, where 'secure' is explicitly and formally defined. |
| **Common Criteria Recognition Arrangement** | An international agreement which facilitates the mutual recognition of Common Criteria evaluations by certificate producing schemes, including the Australian and New Zealand certification scheme. |

| Term | Meaning |
|---|---|
| **Communications Security** | Controls applied taken to deny unauthorised access to information derived from information and communication systems and to ensure the authenticity of related communications and data. |
| **Conduit** | A tube, duct or pipe used to protect cables. |
| **Connection Forwarding** | The use of network address translation to allow a port on a network node inside a local area network to be accessed from outside the network. Alternatively, using a Secure Shell server to forward a Transmission Control Protocol connection to an arbitrary port on the local host. |
| **ConOp** | **Concept of Operations,** a document describing the characteristics of an information systems and its intended use. It is used to communicate the intent and system characteristics to all stakeholders. |
| **Consumer Guide** | Product specific advice concerning evaluated products can consist of findings from mutually recognised information security evaluations. This may include the Common Criteria, findings from GCSB internal evaluations, any recommendations for use and references to relevant policy and other standards. |
| **Content Filtering** | The process of monitoring communications, including email and web pages, analysing them for any suspicious or unwanted content, and preventing the delivery of suspicious or unwanted content. |
| **Contract** | Contract means an agreement between two or more persons or entities, which is intended to be enforceable at law and includes a contract made by deed or in writing, |
| **Cross-Domain Solution** | A Cross-Domain Solution (CDS) is a controlled interface that enables secure manual and/or automatic access and/or information transfer between different security domains while protecting the confidentiality, integrity and availability of each domain.<br>There are several types of CDS including access, multi-level and transfer gateways. |
| **Cryptographic Hash** | An algorithm (the hash function) which takes as input a string of any length (the message), and generates a fixed length string (the message digest or fingerprint) as output. The algorithm is designed to make it computationally infeasible to find any input which maps to a given digest, or to find two different messages that map to the same digest. |
| **Cryptoperiod** | The useful life of the cryptographic key. |
| **Cryptographic Protocol** | Specified cryptographic algorithms, parameters (such as key length) and processes for managing, establishing and using encrypted communications. |
| **Cryptographic System** | A related set of hardware or software used for cryptographic communication, processing or storage, and the administrative framework in which it operates. |

| Term | Meaning |
|---|---|
| **Cryptographic System Material** | Material that includes, cryptographic key, equipment, devices, documents, firmware or software that contains or describes cryptographic logic. |
| **Data At Rest** | Information residing on media storage facility or a system that is not in use. |
| **Data In Transit** | Information that is being conveyed across a communication medium. |
| **Data In Use** | Information that has been decrypted for processing by a system. |
| **Data Diode** | A device that allows data to flow in only one direction. |
| **Data Remanence** | Residual information remaining on a device or storage media after clearing or sanitising the device or media. Sometimes described as data persistence. |
| **Data Spill** | An information security incident that occurs when information is transferred between two security domains by an unauthorised means. This can include from a classified network to a less classified network or between two areas with different need-to-know requirements. |
| **Declassification** | A process whereby information is reduced to an unclassified state. Subsequently an administrative decision can be made to formally authorise its release into the public domain. |
| **Degausser** | An electrical device or permanent magnet assembly which generates a coercive magnetic force to destroy magnetic storage patterns in order to sanitise magnetic media. |
| **Delegate** | A person or group of personnel who may authorise non-compliance with requirements in this manual on the specific authority of the agency head. |
| **Demilitarised Zone** | A small network with one or more servers that is kept separate from an agency's core network, either on the outside of the agency's firewall, or as a separate network protected by the agency's firewall. Demilitarised zones usually provide public domain information to less trusted networks, such as the Internet. |
| **Department** | Term used to describe Public Service Departments and Non-Public Service Departments within the state sector.<br>Refer State Services Commission list of Central Government Agencies – http://www.ssc.govt.nz/sites/all/files/guide-to-central-govt-agencies-30aug2013.pdf |
| **Device Access Control Software** | Software that can be installed to restrict access to communications ports such as USB, Serial HDMI and Ethernet Ports. Device access control software can either block all access to a communications port or allow access using a whitelisting approach based on device types, manufacturer's identification, or even unique device identifiers. |
| **Diffie-Hellman Groups** | A method used for specifying the modulus size used in the hashed message authentication code algorithms. Each DH group represents a specific modulus size. For example, group 2 represents a modulus size of 1024 bits. |
| **Dual-Stack Device** | A product that implements both IP version 4 and 6 protocol stacks. |

| Term | Meaning |
|---|---|
| **Emanation Security** | The counter-measures, techniques and processes employed to reduce classified emanations from a facility and its systems to an acceptable level. Emanations can be in the form of RF energy, sound waves or optical signals. |
| **Emergency Access** | The process of a system user accessing a system that they do not hold appropriate security clearances for due to an immediate and critical emergency requirement. |
| **Emergency Situation** | A situation requiring the evacuation of a site. Examples include fires and bomb threats. |
| **Encapsulating Security Payload** | A protocol used for encryption and authentication within IPSec. |
| **Endorsement** | Certain information may bear an endorsement marking in addition to a security classification.<br>Endorsement markings are not security classifications in their own right and must not appear without a security classification.<br>Endorsement markings are warnings that the information has special requirements in addition to those indicated by the security classification and should only be used when there is a clear need for special care.<br>Endorsement markings may indicate:<br>• the specific nature of information;<br>• temporary sensitivities;<br>• limitations on availability; or<br>• how recipients should handle or disclose information. |
| **Escort** | An individual who supervises visitors to secure areas to ensure uncleared visitors are not exposed to classified information, conversations equipment and other classified materials. Such visitors may include maintenance staff, IT contractors and building inspectors. |
| **Evaluation Assurance Level** | A numeric representation of the security functionality of a product gained from undertaking a Common Criteria evaluation. Each EAL comprises a number of assurance components, covering aspects of a product's design, development and operation. The range covers EAL0 (lowest) to EAL7 (highest). |
| **Exception** | The formal acknowledgement that a requirement of the NZISM cannot be met and that a dispensation from the particular compliance requirement is granted by the Accreditation Authority. This exception is valid for the term of the Accreditation Certificate or some lesser time as determined by the Accreditation Authority. |
| **Exceptions and Waivers** | An exception is NOT the same as a waiver. An exception means that the requirement need not be followed. A waiver means that some alternative controls or conditions are implemented. |
| **Facility** | An area that facilitates government business. For example, a facility can be a building, a floor of a building or a designated area on the floor of a building. |

| Term | Meaning |
|---|---|
| **Filter** | A device that manages or restricts the flow of data in accordance with a security policy. |
| **Firewall** | A network protection device that filters incoming and outgoing network data, based on a series of rules. |
| **Firmware** | Software embedded in a hardware device. |
| **Flash Memory Media** | A specific type of EEPROM. |
| **Fly Lead** | A cable that connects IT equipment to the fixed infrastructure of the facility. For example, the cable that connects a workstation to a network wall socket. |
| **Foreign National** | A person who is not a New Zealand citizen. |
| **Foreign System** | A system that is not owned and operated by the New Zealand Government. |
| **Functional Segregation** | Segregation based on the device function or intended function. |
| **Gateway** | Connections between two or more systems from different security domains to allow access to or transfer of information according to defined security policies. Some gateways can be automated through a combination of physical or software mechanisms. Gateways are typically grouped into three categories: access gateways, multilevel gateways and transfer gateways. |
| **General User** | A system user who can, with their normal privileges, make only limited changes to a system and generally cannot bypass system security. |
| **Government Chief Information Officer** | Government Chief Information Officer (GCIO) is a role undertaken by the Chief Executive of the Department of Internal Affairs in order to provide leadership on ICT matters within the NZ Government. |
| **Hardware** | A generic term for any physical component of information and communication technology, including peripheral equipment and media used to process information. |
| **Hardware Security Module** | Hardware Security Modules (HSMs) are a device, card or appliance usually installed inside of a PC or server to provide cryptographic functions. HSM's are usually physically and electronically hardened to reduce the possibility of tampering or other interference. |

| Term | Meaning |
|---|---|
| **Hash** | A hash is the result of a one-way, cryptographic function that converts a data string of any length into a unique fixed-length bit string. Typically applied to passwords and messages to protect against loss and/or add resistance to attacks.<br><br>Hashing algorithms or functions are designed as a one-way cryptographic transformation so that it's impossible to reverse the hash process and reconstitute the original string.<br><br>The values returned by a hash function are variously described as hash values, hash codes, digests, or simply hashes.<br><br>One common use of a hash is a data structure called a hash table, widely used in computer software for indexing and rapid retrieval of database elements.<br><br>Note that a hash is not the same as data encryption although it does utilise cryptographic functions.<br><br>See also Checksum. |
| **Hash Value** | See Hash. Also known as "message digest". |
| **Hashed Message Authentication Code Algorithms** | In cryptography, a keyed-hash message authentication code (HMAC) is a specific type of message authentication code (MAC) using a cryptographic hash function and a cryptographic key. |
| **High Assurance** | High Assurance is a generic term encompassing Common Criteria Evaluation Assurance Levels (EAL) 5, 6 and 7. Alternatively refers to the independent (unrelated) ASD High Assurance Evaluation Scheme. |
| **High Grade Cryptography** | The U.S. ranks cryptographic products and algorithms through a certification programme and categorising the products and algorithms into product types. Product types are defined in the US National Information Assurance Glossary (CNSSI No. 4009) which defines Type 1 and 2 products, and Type 3 and 4 algorithms. Type 1 products are used to protect systems requiring the most stringent protection mechanisms. |
| **High Grade Cryptographic Products & Equipment** | The equivalent to United States Type 1 cryptographic products & equipment. |
| **Hybrid Hard Drives** | Non-volatile magnetic media that use a cache to increase read and write speeds and reduce boot time. The cache is normally flash memory media or battery backed RAM. |
| **Incident Response Plan** | A plan for responding to information security incidents as defined by the individual agency. |
| **Information** | Any communication or representation of knowledge such as facts, data, and opinions in any medium or form, electronic as well as physical. Information includes any text, numerical, graphic, cartographic, narrative, or any audio or visual representation. |

| Term | Meaning |
|---|---|
| **Information Asset** | Information asset is any information or related equipment has value to an organisation. This includes equipment, facilities, patents, intellectual property, software and hardware. Information Assets also include services, information, and people, and characteristics such as reputation, brand, image, skills, capability and knowledge**.** |
| **Information and Communications Technology** | Information and Communications Technology (ICT) includes:<br>• Information management;<br>• Technology infrastructure; and<br>• Technology-enabled business processes and services. |
| **Information Security** | Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or any other means. |
| **Information Security Incident** | An occurrence or activity that may threaten the confidentiality, integrity or availability of a system or the information stored, processed or communicated by it or by any other process or system and processes. |
| **Information Security Policy** | A high-level document that describes how an agency protects its information. The CSP is normally developed to cover all systems and can exist as a single document or as a set of related documents. |
| **Information Technology Security Manager** | ITSMs are executives within an agency that act as a conduit between the strategic directions provided by the CISO and the technical efforts of systems administrators. The main responsibility of ITSMs is the administrative controls relating to information security within the agency. |
| **Infrared Device** | A device such as a mouse, keyboard, pointing device, laptop and smart phone that have an infrared communications capability. |
| **Internet Key Exchange Extended Authentication** | Used to provide an additional level of authentication by allowing IPSec gateways to request additional authentication information from remote users. As a result, users are forced to respond with credentials before being allowed access to the connection. |
| **Intrusion Detection System** | An automated system used to identify an infringement of security policy from an internal or external source. |
| **Intrusion Prevention System** | A security device or software which monitors system activities for malicious or unwanted behaviour and can react in real-time to block or prevent those activities. |
| **IP Security** | A suite of protocols for secure IP communications through authentication or encryption of IP packets including protocols for cryptographic key establishment. |
| **IP Telephony** | The management and transport of voice communications over IP networks. Also described as Voice Over IP (VOIP). |
| **IP Version 6** | A protocol used for communicating over a packet switched network. Version 6 is the successor to version 4 which is widely used on the Internet. The main change introduced in version 6 is a greater address space available for identifying network devices, workstations and servers. |

| Term | Meaning |
|---|---|
| **ISAKMP Aggressive Mode** | An IPSec protocol that uses a reduced Exchange to establish an IPSec connection. Connection negotiation is quicker but potentially less secure. |
| **ISAKMP Main Mode** | An IPSec protocol that offers improved security using additional negotiation to establish an IPSec connection. |
| **ISAKMP Quick Mode** | An IPSec protocol that is used for refreshing security association information. Similar to aggressive mode. |
| **Isolation** | Includes disconnection from other systems and any external connections. In some cases system isolation may not be possible for architectural or operational reasons. Isolation may also include the quarantine of suspected or known malware and unwanted content. |
| **IT Equipment** | Any equipment to support the acquisition, processing and storage of information. This may include servers, routers, switches, switch panels, UPSs, PCs, laptops printers, MFDs etc. |
| **Key Management** | The management of cryptographic keys and associated hardware and software. It includes their generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction. |
| **Key Management Plan** | Describes how cryptographic services are securely deployed within an agency. It documents critical key management controls to protect keys and associated material during their life cycle, along with other controls to provide confidentiality, integrity and availability of keys. |
| **Key Stretching** | A defence against brute force and similar system attacks by increasing the time required to complete hashing and making an attack more time-consuming. |
| **Limited Higher Access** | The process of granting a system user access to a system that they do not hold appropriate security clearances for, for a limited period of time. |
| **Lockable Commercial Cabinet** | A cabinet that is commercially available, of robust construction and is fitted with a commercial lock. |
| **Logging Facility** | A facility that includes the software component which records system events and associated details, the transmission (if necessary) of these records (logs) and how they are stored and secured. |
| **Malicious Code** | Any software that attempts to subvert the confidentiality, integrity or availability of a system. Types of malicious code include logic bombs, trapdoors, Trojans, viruses and worms. More usually as Malware. |
| **Malicious Code Infection** | An information security incident that occurs when malicious code is used to infect a system. Examples of malicious code infection viruses, worms and Trojans. |
| **Malware** | Malicious Software or Malicious Code. |
| **Management Traffic** | Communications generated by system administrators and processes over a network in order to manage and control a device. |

| Term | Meaning |
|---|---|
| **Mandatory Controls** | Controls within this manual with either a 'MUST' or a 'MUST NOT' compliance requirement. |
| **Media** | A generic term for hardware that is used to store information. |
| **Media Destruction** | The process of physically damaging the media with the objective of making the data stored on it inaccessible. To destroy media effectively, only the actual material in which the data is stored needs to be destroyed. |
| **Media Disposal** | The process of relinquishing control of media, or disposing of when no longer required, in a secure manner that ensures that no data can be recovered from the media. |
| **Media Sanitisation** | The process of securely erasing or overwriting data stored on media. |
| **Multifunction Devices** | The class of devices that combines printing, scanning, copying, faxing or voice messaging functionality within the one piece of equipment. These are often designed to connect to computer and communications networks simultaneously. |
| **Multilevel Gateway** | A gateway that enables access, based on authorisation, to data at many classification and releasability levels where each data unit is individually marked according to its domain. |
| **Need-To-Know** | The principle of telling a person only the information that they require to fulfil their role. |
| **Network Access Control** | Policies and processes used to control access to a network and actions on a network, including authentication checks and authorisation controls. |
| **Network Device** | Any device designed to facilitate the communication of information destined for multiple system users. For example: cryptographic devices, firewalls, routers, switches and hubs. |
| **Network Infrastructure** | The infrastructure used to carry information between workstations and servers or other network devices. For example: cabling, junction boxes, patch panels, fibre distribution panels and structured wiring enclosures. |
| **Network Protection Device** | A category of network device used specifically to protect a network. For example, a firewall, session border controller etc. |
| **NZ Eyes Only** | A caveat indicating that the information is not to be passed to or accessed by foreign nationals. |
| **NZ Government Information Security Manual** | National security policy that aims to provide a common approach to ensure that the implementation of information security reduces both agency specific, and whole of government, information security risks to an acceptable level. |
| **NZ Government Protective Security Manual** | The PSM was superseded by the Protective Security Requirements (PSR) in December 2014. |
| **No-Lone-Zone** | An area in which personnel are not permitted to be left alone such that all actions are witnessed by at least one other person. |
| **Non-Volatile Media** | A type of media which retains its information when power is removed. |

| Term | Meaning |
|---|---|
| **Off-Hook Audio Protection** | A method of mitigating the possibility of an active, but temporarily unattended handset inadvertently allowing discussions being undertaken in the vicinity of the handset to be heard by the remote party. This could be achieved through the use of a hold feature, mute feature, push-to-talk handset or equivalent. May not be effective on smart phones / cell phones. |
| **Official Information** | Any information held by a government department or agency. See the Official Information Act 1982 (as amended). |
| **OpenPGP** | An open-source implementation of Pretty Good Privacy (PGP), a widely available cryptographic toolkit. |
| **Oversight** | The term is used in this document in the following ways:<br>1. In the context of governance where the term is used to describe the responsibility and requirement to manage, govern, inspect or direct activities to ensure particular outcomes, e.g. the oversight of supply contracts.<br>2. In the physical security context to describe the ability to observe activity (surveillance) and/or read materials which should be protected and shared only under strict guidelines. It enables the systematic observation of places and people by visual, audio, electronic, photographic or other means. Typically this is caused by poor placing of computer screens and desks and proximity to windows, doors, corridors or other means of physical access and overview or oversight. Other physical factors may contribute. |
| **Patch Cable** | A metallic (usually copper) or fibre optic cable used for routing signals between two components in an enclosed container or rack or between adjacent containers or racks. |
| **Patch Panel** | A group of sockets or connectors that allow manual configuration changes, generally by means of connecting cables to the appropriate connector. Cables could be metallic (copper) or fibre optic. |
| **Perfect Forward Security** | Additional security for security associations in that if one security association is compromised subsequent security associations will not be compromised. |
| **Peripheral Switch** | A device used to share a set of peripherals between a number of computers. |
| **Principles of Separation and Segregation** | Systems architecture and design incorporating separation and segregation in order to establish trust zones, define security domains and enforce boundaries. |
| **Privacy Marking** | Privacy markings are used to indicate that official information has a special handling requirement or a distribution that is restricted to a particular audience. |

| Term | Meaning |
|---|---|
| **Private Network** | A private network is a network and infrastructure owned, managed and controlled by a single entity for its exclusive use.<br><br>This term includes networks used by private organisations, non-government organisations, state owned enterprises, or government department, agencies and ministries.<br><br>If any part of the transmission path utilises **any** element of a public network, such as telecommunications or data services from a service provider that utilise any component of local, regional or national infrastructure, then the network is defined as a public network. |
| **Privileged User** | A system user who can alter or circumvent system security protections. This can also apply to system users who could have only limited privileges, such as software developers, who can still bypass security precautions. A privileged user can have the capability to modify system configurations, account privileges, audit logs, data files or applications. |
| **Protective Marking** | A marking that is applied to unclassified or classified information to indicate the security measures and handling requirements that are to be applied to the information to ensure that it is appropriately protected. |
| **Protective Security Requirements** | The Protective Security Requirements (PSR) outlines the Government's expectations for managing personnel, physical and information security. |
| **Protective Security Requirements Framework** | The Protective Security Requirements Framework (PSRF) is a four-tier hierarchical approach to protective security. Strategic Security Directive (tier one); Core policies, strategic security objectives and the mandatory requirements (tier two); Protocols, standards and good practice requirements (tier three); Agency-specific policies and procedures (tier four). |
| **Public Domain Information** | Official information authorised for unlimited public access or circulation, such as agency publications and websites. |
| **Public Key Infrastructure** | The framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover and revoke public key certificates. SOURCE: CNSSI-4009 |
| **Public Network** | A public network contains components that are outside the control of the user organisation. These components may include telecommunications or data services from a service provider that utilise any component of local, regional or national infrastructure. |
| **Public Switched Telephone Network** | An historic term describing a public network where voice is communicated using analogue communications. Today almost all communication networks are substantially or entirely digital networks. |

| Term | Meaning |
|---|---|
| **Push-To-Talk** | Handsets that have a button which must be pressed by the user before audio can be communicated, thus improving off-hook audio protection. |
| **Quality Of Service** | A process to prioritise network traffic based on availability requirements. |
| **Radio Frequency Device** | Devices including mobile phones, wireless enabled personal devices and laptops. |
| **Reaccreditation** | A procedure by which an authoritative body gives formal recognition, approval and acceptance of the associated residual security risk with the continued operation of a system. |
| **Reclassification** | A change to the security measures afforded to information based on a reassessment of the potential impact of its unauthorised disclosure. The lowering of the security measures for media containing classified information often requires sanitisation or destruction processes to be undertaken prior to a formal decision to lower the security measures protecting the information. |
| **Remote Access** | Access to a system from a location not within the physical control of the system owner. |
| **Removable Media** | Storage media that can be easily removed from a system and is designed for removal. |
| **Residual Risk** | The risk remaining after management takes action to reduce the impact and likelihood of an adverse event, including control activities in responding to a risk (Institute of Internal Auditors). Also sometimes referred to as "net risk" or "controlled risk". |
| **Rogue Wireless Access Point** | An unauthorised Wireless Access Point operating outside of the control of an agency. |
| **Salt** | Salts are a random data string to the start or the end of a hash to strengthen its resistance to attack. Typically used in the generation of a password hash or checksums. |
| **Seconded Foreign National** | A representative of a foreign government on exchange or long-term posting to an agency. |
| **Secure Area** | An area that has been certified to physical security requirements as either a Secure Area; a Partially Secure Area; or an Intruder Resistant Area to allow for the processing of classified information. Refer to the PSR for more detail on Physical Security. |
| **Secure Multipurpose Internet Mail Extension** | A protocol which allows the encryption and signing of Multipurpose Internet Mail Extension-encoded email messages. |
| **Secure Shell** | A network protocol that can be used to securely log into a remote server or workstation, executing commands on a remote system and securely transfer file(s). |
| **Security Association** | A collection of connection-specific parameters containing information about a one-way connection within IPSec that is required for each protocol used. |
| **Security Association Lifetimes** | The duration for which security association information is valid. |

| Term | Meaning |
|---|---|
| **Security Domains** | A system or collection of systems operating under a security policy that defines the classification and releasability of the information processed within the domain. It can be defined by a classification, a community of interest or releasability within a certain classification.<br>This term is NOT synonymous with *Trust Zone*. |
| **Security Domain Owner** | The individual responsible for the secure configuration of the security domain throughout its life-cycle, including all connections to/from the domain. |
| **Security Risk Management Plan** | A plan that identifies the risks and appropriate risk treatments including controls needed to meet agency policy. |
| **Security Target** | An artefact of Common Criteria evaluations. It contains the information security requirements of an identified target of evaluation and specifies the functional and assurance security measures offered by that target of evaluation to meet the stated requirements. |
| **Segregation** | Segregation may be achieved by isolation, enforcing separation of key elements of a virtual system, removing network connectivity to the relevant device or applying access controls to prevent or limit access. |
| **Separation** | Separation is a physical distinction between elements of a network or between networks. This applies in both physical and virtual systems architectures |
| **Server** | A computer used to run programs that provide services to multiple users. For example, a file server, email server or database server. |
| **Session Border Controller** (**SBC**) | A device (physical or virtual) used in IP networks to control and manage the signalling and media streams of real-time UC and VoIP connections. It includes establishing, controlling, and terminating calls, interactive media communications or other VoIP connections. SBCs enable VoIP traffic to navigate gateways and firewalls and ensure interoperability between different SIP implementations. Careful selection of SBCs will provide such functionality as prevention of toll fraud, resistance to denial of service attacks and resistance to eavesdropping. |
| **Softphone** | A software application that allows a workstation to act as a VoIP phone, using either a built-in or an externally connected microphone and speaker. |
| **Software Component** | An element of a system, including but not limited to, a database, operating system, network or Web application. |
| **Solid State Drive** | Non-volatile media that uses flash memory media to retain its information when power is removed. |
| **SSH-Agent** | A programme storing private keys used for public key authentication thus enabling an automated or script-based Secure Shell session. |
| **Standard Operating Environment** | A standardised build of an operating system and associated software that is deployed on multiple devices. An SOE can be applied to servers, workstations, laptops and mobile devices. |

| Term | Meaning |
|---|---|
| **Standard Operating Procedures** | Procedures for the operation of system and complying with security requirements. |
| **System** | A related set of IT equipment and software used for the processing, storage or communication of information and the governance framework in which it operates. |
| **System Classification** | The highest classification of information for which the system is approved to store or process. |
| **System Owner** | The person responsible for the information resource. |
| **System Security Plan** | Documenting the controls for a system. |
| **System User** | A general user or a privileged user of a system. |
| **Target Of Evaluation** | The functions of a product subject to evaluation under the Common Criteria. |
| **Technical Surveillance Counter-Measures** | The process of surveying facilitates to detect the presence of technical surveillance devices and to identify technical security weaknesses that could aid in the conduct of a technical penetration of the surveyed facility. |
| **Telephone** | A device that converts between sound waves and electronic signals that can be communicated over a distance. |
| **Telephone System** | A system designed primarily for the transmission of voice traffic. |
| **TEMPEST** | A short name referring to investigations and studies of compromising emanations. |
| **TEMPEST Rated IT Equipment** | IT equipment that has been specifically designed to minimise TEMPEST emanations. |
| **TOP SECRET Area** | Any area certified to operate at TOP SECRET, containing TOP SECRET servers, workstations or associated network infrastructure. |
| **Traffic Flow Filter** | A device that has been configured to automatically filter and control the flow of network data. |
| **Transfer Gateway** | Facilitates the secure transfer of information, in one or multiple directions (i.e. low to high or high to low), between different security domains. |
| **Transport Mode** | An IPSec mode that provides a secure connection between two endpoints by encapsulating an IP payload. |
| **Trust Boundary** | The interface between two or more Trust Zones. |
| **Trust Zone** | A logical construct encompassing an area with a high degree of trust between the data, users, providers and the systems. It may include a number of capabilities such as secure boot, code-signing, trusted execution and Digital Rights Management (DRM).<br>This term is NOT synonymous with *Security Domain.* |
| **Trusted Source** | A person or system formally identified as being capable of reliably producing information meeting defined parameters, such as a maximum data classification and reliably reviewing information produced by others to confirm compliance with defined parameters. |

| Term | Meaning |
|---|---|
| **Tunnel Mode** | An IPSec mode that provides a secure connection between two endpoints by encapsulating an entire IP packet. The entire packet is encrypted and authenticated. |
| **UNCLASSIFIED Information** | Information that is assessed as not requiring a classification. |
| **UNCLASSIFIED Systems** | Systems that process, store or communicate information produced by the New Zealand Government that does not require a classification. |
| **Unified Communications** | The integration of real-time and near real time communication and interaction services in an organisation or agency. Unified Communications (UC) may integrate several communication systems including unified messaging, collaboration, and interaction systems; real-time and near real-time communications; and transactional applications. |
| **Unsecure Area** | An area that has not been certified to meet physical security requirements to allow for the processing of classified information. |
| **Virtual Private Network** | The tunnelling of a network's traffic through another network, separating the VPN traffic from the underlying network. A VPN can encrypt traffic if necessary. |
| **Virtual Private Network Split Tunnelling** | Functionality that allows personnel to access both a public network and a VPN connection at the same time, such as an agency system and the Internet. |
| **Virtualisation** | The software simulation of the components of an information system and may include the simulation of hardware, operating systems, applications, infrastructure and storage. |
| **Volatile Media** | A type of media, such as RAM, which gradually loses its information when power is removed. |
| **Waiver** | The formal acknowledgement that a particular compliance requirement of the NZISM cannot currently be met and that a waiver is granted by the Accreditation Authority on the basis that full compliance with the NZISM is achieved or compensating controls are implemented within a time specified by the Accreditation Authority. Waivers are valid in the short term only and full accreditation cannot be granted until all conditions of the waiver have been met. |
| **Waivers and Exceptions** | A waiver means that some alternative controls or conditions are implemented. An exception means that the requirement need not be followed. An exception is NOT the same as a waiver. |
| **Wear Levelling** | A technique used in flash memory that is used to prolong the life of the media. Data can be written to and erased from an address on flash memory a finite number of times. The wear levelling algorithm helps to distribute writes evenly across each memory block, thereby decreasing the wear on the media and increasing its lifetime. The algorithm ensures that updated or new data is written to the first available free block with the least number of writes. This creates free blocks that previously contained data. |
| **Whitelist** | A list that confirms items being analysed are acceptable. It is the opposite of a blacklist. |

| Term | Meaning |
|---|---|
| **Wi-Fi Protected Access** | Protocols designed to replace WEP. They refer to components of the 802.11i security standard. |
| **Wired Equivalent Privacy** | WEP, a deprecated 802.11 security standard. |
| **Wireless Access Point** | Typically also the device which connects the wireless local area network to the wired local area network. Also known as AP. |
| **Wireless Communications** | The transmission of data over a communications path using electromagnetic waves rather than a wired medium. |
| **Wireless Local Area Network** | A network based upon the 802.11 set of standards. Such networks are often referred to as wireless networks. |
| **Workstation** | A stand-alone or networked single-user computer. |
| **X11 Forwarding** | X11, also known as the X Window System, is a basic method of video display used in a variety of operating systems. X11 forwarding allows the video display from one network node to be shown on another node. |

**END OF DOCUMENT**