22.1. Agency-owned Mobile Devices

Objective

22.1.1. Information on agency-owned mobile devices is protected from unauthorised disclosure.

Context

Scope

22.1.2. 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.

22.1.3. 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

22.1.4. 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.

22.1.5. 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

22.1.6. 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

22.1.7. 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

22.1.8. 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

22.1.9. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV2, GOV4, GOV6, INFOSEC1, INFOSEC2, INFOSEC3, INFOSEC4, PHYSEC1 and PHYSEC2	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements Physical security (PHYSEC) | Protective Security Requirements

Rationale & Controls

Mobile devices usage policy

22.1.10.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.

22.1.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4471]

Agencies MUST develop a policy governing the use of mobile devices.

22.1.10.C.02. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must Not** [CID:4472]

Agencies MUST NOT allow mobile devices to process or store TOP SECRET information unless explicitly approved by GCSB to do so.

22.1.10.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4473]

Agencies SHOULD implement a Mobile Device Management (MDM) solution.

Personnel awareness

22.1.11.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.

22.1.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4476]

Agencies MUST advise personnel of the maximum permitted classifications for data and voice communications when using mobile devices.

22.1.11.C.02. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:4477]

Agencies SHOULD NOT use Paging Services, SMS or MMS for sensitive or classified communications.

Non-agency owned and controlled mobile devices

22.1.12.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.

22.1.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4480]

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.

Agency owned mobile device storage encryption

22.1.13.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.

22.1.13.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.

22.1.13.R.03. **Rationale**

Refer to the PSR - Mobile and Remote working

Refer to the PSR - Handling Requirements for protectively marked information and equipment

22.1.13.C.01. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must** [CID:4483]

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.

22.1.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:4484]

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.

22.1.13.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4485]

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.

22.1.13.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4486]

Agencies SHOULD encrypt classified information on all mobile devices using an Approved Cryptographic Algorithm.

22.1.13.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4487]

Pool or shared devices SHOULD be reissued with unique passwords, passphrases, PINs or other access codes for each separate issue or deployment.

Mobile device communications encryption

22.1.14.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.

22.1.14.R.02. **Rationale**

Note: This applies to information and systems classified as RESTRICTED/SENSITIVE and any higher classification.

22.1.14.R.03. **Rationale**

Encryption does not change the classification level of the information or system itself but allows reduced handling requirements to be applied.

22.1.14.C.01. **Control System Classifications(s): Secret, Confidential, Top Secret, Restricted/Sensitive; Compliance: Must** [CID:4492]

Agencies MUST use encryption on mobile devices communicating over public infrastructure, the Internet or non-agency controlled networks.

22.1.14.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4493]

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.

Mobile device privacy filters

22.1.15.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.

22.1.15.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4496]

Agencies SHOULD apply privacy filters to the screens of mobile devices.

Disabling Bluetooth functionality

22.1.16.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.

22.1.16.C.01. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must Not** [CID:4499]

Agencies MUST NOT enable Bluetooth functionality on mobile devices.

22.1.16.C.02. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:4500]

Agencies SHOULD NOT enable Bluetooth functionality on mobile devices.

Configuration control

22.1.17.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.

22.1.17.C.01. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:4503]

Agency personnel MUST NOT disable security functions or security configurations on a mobile device once provisioned.

22.1.17.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4504]

Agencies SHOULD control the configuration of mobile devices in the same manner as devices in the agency's office environment.

22.1.17.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4505]

Agencies SHOULD prevent personnel from installing unauthorised applications on a mobile device once provisioned.

Maintaining mobile device security

22.1.18.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.

22.1.18.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4508]

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.

22.1.18.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4509]

Agencies SHOULD conduct policy checks as mobile devices connect to agency systems.

Connecting mobile devices to the Internet

22.1.19.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.

22.1.19.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.

22.1.19.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4513]

Agencies MUST disable split tunnelling when using a VPN connection from a mobile device to connect to an agency network.

22.1.19.C.02.

Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Should Not [CID:4514]

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.

Emergency destruction

22.1.20.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.

22.1.20.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.

22.1.20.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4519]

Agencies MUST develop an emergency destruction plan for mobile devices.

22.1.20.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:4520]

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.

22.1.20.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4521]

Agencies SHOULD ensure personnel are trained in emergency destruction procedures and are familiar with the emergency destruction plan.

Labelling

22.1.21.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.

22.1.21.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4524]

Agencies SHOULD use soft labelling for mobile devices when appropriate to reduce their attractiveness value.

Unauthorised use of mobile devices

22.1.22.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.

22.1.22.R.02. **Rationale**

Agencies must recognise the risks and costs associated with personal use of an agency device.

22.1.22.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:4530]

Agencies SHOULD develop a policy to manage the non-business or personal use of an agency owned device.

22.1.22.C.02. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:4531]

Mobile devices SHOULD NOT be used other than by personnel specifically authorised by the agency.