15.1. Email Applications

Objective

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

Context

Scope

15.1.2. 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

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

Exceptions for receiving unmarked email messages

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

References

15.1.5. Further references can be found at:

Reference	Title	Publisher	Source
SP 800-45	**NIST publication SP 800-45 v2, Guidelines on Electronic Mail Security**	NIST	https://csrc.nist.gov/publications/detail/sp/800-45/version-2/final
	Detecting socially engineered emails August 2012	ASD	Detecting Socially Engineered Messages | Cyber.gov.au

PSR references

15.1.6. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV2, GOV3, GOV4, 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

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 Classifications(s): All Classifications; Compliance: Must** [CID:1684]

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 Classifications(s): All Classifications; Compliance: Must** [CID:1687]

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 Classifications(s): All Classifications; Compliance: Must Not** [CID:1688]

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 Classifications(s): All Classifications; Compliance: Should** [CID:1691]

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 Classifications(s): All Classifications; Compliance: Must Not** [CID:1696]

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 Classifications(s): All Classifications; Compliance: Should Not** [CID:1697]

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 Classifications(s): All Classifications; Compliance: Should Not** [CID:1698]

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 Classifications(s): All Classifications; Compliance: Must** [CID:1702]

All classified and unclassified emails MUST have a protective marking.

15.1.11.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:1703]

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 Classifications(s): All Classifications; Compliance: Should** [CID:1704]

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 Classifications(s): All Classifications; Compliance: Must** [CID:1707]

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 Classifications(s): All Classifications; Compliance: Should Not** [CID:1711]

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 Classifications(s): All Classifications; Compliance: Should** [CID:1714]

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 Classifications(s): All Classifications; Compliance: Should** [CID:1717]

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 Classifications(s): All Classifications; Compliance: Should** [CID:1720]

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 Classifications(s): All Classifications; Compliance: Should Not** [CID:1723]

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 Classifications(s): All Classifications; Compliance: Must** [CID:1726]

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 Classifications(s): All Classifications; Compliance: Should** [CID:1729]

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

15.1.19.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:1730]

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 Classifications(s): All Classifications; Compliance: Should Not** [CID:1733]

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