Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

Guidelines for email management

Email usage

Email usage policy

There are many security risks associated with the non-secure nature of email that are often overlooked. Documenting these security risks, and associated mitigations, will inform personnel of appropriate actions and precautions to take when using email.

Security Control: 0264; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
A policy governing the use of email is developed and implemented.

Webmail services

Allowing personnel to access webmail services can pose a security risk if web content filtering controls in place to mitigate malicious webmail attachments are inadequate. Additionally, the organisation will be reliant upon the webmail provider implementing mitigations such as Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM).

Security Control: 0267; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Personnel cannot access non-organisation approved webmail services.

Marking emails

All electronic information needs to be marked with an appropriate protective marking. This ensures that appropriate security controls are applied to the information and helps prevent unauthorised information being released into the public domain. When a protective marking is applied to an email it is important that it reflects the sensitivity or classification of the information in the body of the email and in any attachments to the email.

Security Control: 0273; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
All emails have a protective marking that accurately reflects its contents, including any attachments.

Receiving emails without valid protective markings

If an email is received without a valid protective marking (e.g. without a protective marking or with an unknown protective marking), users have an obligation to determine the appropriate protective marking for the email if it is to be responded to, forwarded on or printed out. If unsure, personnel may wish to contact the originator to seek clarification. Alternatively, where the user receives unmarked emails as part of standard business practices, the application of protective markings may be automated.

Security Control: 0278; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
When an email without a valid protective marking is received, users assess the information and determine how it is to be handled.

Preventing unmarked or inappropriately marked emails

Unmarked or inappropriately marked emails can be blocked at two points, workstations or the email server. The email server is the preferred location to block emails as it is a single location under the control of system administrators and blocking activities can be enforced for the entire network.

While blocking at the email server is considered the preferred approach, there is still benefit in blocking at workstations. Blocking at workstations can add an extra layer of security and will also reduce the likelihood of a data spill occurring on the email server.

Security Control: 1368; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Unmarked emails or emails marked with an unrecognised or invalid protective marking are prevented from being sent to the intended recipients by blocking them at the email server.

Security Control: 1022; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Unmarked emails or emails marked with an unrecognised or invalid protective marking are prevented from being sent to intended recipients by blocking them at workstations.

Blocking inbound emails

Blocking an inbound email with a protective marking higher than the sensitivity or classification that the receiving system is authorised to process will prevent a data spill from occurring on the receiving system.

Security Control: 0565; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Email systems are configured to reject, log and report inbound emails with protective markings indicating that the content of the email exceeds the sensitivity or classification of the receiving system.

Security Control: 1023; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
The intended recipients of any blocked emails are notified.

Blocking outbound emails

Blocking an outbound email with a protective marking higher than the sensitivity or classification of the path over which it would be communicated stops data spills that could occur due to interception or storage of the email at any point along the path it would be communicated.

Organisations may remove protective markings from emails destined for private citizens and businesses once they have been approved for release from their gateways.

Security Control: 0563; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Systems are configured to block any outbound emails with a protective marking indicating that the content of the email exceeds the sensitivity or classification of the path over which the email would be communicated.

Security Control: 0564; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Systems are configured to log every occurrence of a blocked email.

Protective marking standard

Applying markings that reflect the protection requirements of an email informs the recipient about how to appropriately handle the email. The application of standardised protective markings can facilitate interoperability across organisations.

Security Control: 0270; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
The Australian Government's email protective marking standard is implemented.

Protective marking tools

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

Allowing users to choose only protective markings for which the system is authorised lessens the chance of a user inadvertently over-classifying an email. It also reminds users of the maximum sensitivity or classification of information permitted on the system.

Email gateway filters generally only check the most recent protective marking applied to an email. Therefore, when users are forwarding or responding to an email, forcing them to apply a protective marking which is at least as high as that of the email they received will help email gateway filters prevent emails being sent to systems that are not authorised to handle the original sensitivity or classification of the email.

Security Control: 0271; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Protective markings cannot be inserted into user-generated emails without their intervention.

Security Control: 0272; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Marking tools do not allow users to select protective markings that the system has not been authorised to process, store or communicate.

Security Control: 1089; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Marking tools do not allow users replying to or forwarding an email to select a protective marking that is lower than previously used for the email.

Email distribution lists

Often the membership and nationality of members of email distribution lists is unknown. Therefore, users sending emails with Australian Eyes Only (AUSTEO), Australian Government Access Only (AGAO) or nationality releasability information to distribution lists could accidentally cause a data spill.

Security Control: 1539; Revision: 0; Updated: Sep-18; Applicability: P, S, TS; Priority: Should
Emails containing nationality releasability information are only sent to named recipients and not to groups or distribution lists unless the nationality of all members of the distribution lists can be confirmed.

Security Control: 0269; Revision: 2; Updated: Sep-18; Applicability: S, TS; Priority: Must
Emails containing AUSTEO or AGAO information are only sent to named recipients and not to groups or distribution lists unless the nationality of all members of the distribution lists can be confirmed.

Further information

Further information on the Australian Government's email protective marking standard can be found in the Attorney-General's Department (AGD)'s ***Protective Security Policy Framework*** (PSPF), ***Sensitive and classified information*** policy, at https://www.protectivesecurity.gov.au/information/sensitive-classified-information/.

Email infrastructure

Undeliverable messages

Undeliverable or bounce emails are commonly sent by email servers to the original sender when the email cannot be delivered, usually because the destination address is invalid. Due to the common spamming practice of spoofing sender addresses, this often results in a large amount of bounce emails being sent to an innocent third party. Sending bounces

only to senders that can be verified via SPF, or other trusted means, avoids contributing to this problem and allows trusted parties to receive legitimate bounce messages.

Security Control: 1024; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Notification of undeliverable, bounced or blocked emails are only sent to senders that can be verified via SPF or other trusted means.

Automatic forwarding of emails

Automatic forwarding of emails, if left unsecured, can pose a security risk. For example, if a user setup a server-side rule to automatically forward all emails received on an internet-connected system to their personal email account outside work.

Security Control: 0566; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Security controls for blocking unmarked and outbound emails are also applied to automatically forwarded emails.

Open relay email servers

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.

Security Control: 0567; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Open email relaying is disabled such that email servers will only relay messages destined for their domains and those originating from inside the domain.

Email server maintenance activities

Email servers perform a critical business function. It is important that organisations perform regular email server auditing, security reviews and vulnerability analysis activities.

Security Control: 0568; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Regular email server auditing, security reviews and vulnerability analysis activities are performed.

Centralised email gateways

Without a centralised email gateway, it is exceptionally difficult to deploy SPF, DKIM and outbound email protective marking verification.

An adversary will almost invariably avoid using the primary email server when sending malicious emails. This is because backup or alternative email gateways are often poorly maintained in terms of patches, blacklists and content filtering.

Security Control: 0569; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Email is routed through a centralised email gateway.

Security Control: 0570; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Where backup or alternative email gateways are in place, they are maintained at the same standard as the primary email gateway.

Security Control: 0571; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Where users send email from outside their network, an authenticated and encrypted channel is configured to allow email to be sent via the centralised email gateway.

Email server transport encryption

Email can be intercepted anywhere between the originating email server and the destination email server. Enabling Transport Layer Security (TLS) on the originating and destination email server will defeat passive intrusions 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 Internet Engineering Task Force (IETF) Request for Comments (RFC) 3207 specifies the encryption as opportunistic.

Security Control: 0572; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Opportunistic TLS encryption, as defined in IETF RFC 3207, is enabled on email servers that make incoming or outgoing email connections over public network infrastructure.

Further information

Further information on opportunistic TLS encryption can be found in IETF RFC 3207, ***SMTP Service Extension for Secure SMTP over Transport Layer Security***, at https://tools.ietf.org/html/rfc3207.

Email content filtering

Filtering malicious and suspicious emails and attachments

Blocking specific types of emails reduces the likelihood of phishing emails and emails containing malicious code entering an organisation's network.

Security Control: 1234; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Content filtering controls are implemented for email attachments.

Security Control: 0561; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
All emails addressed to internal email aliases with source addresses located from outside the domain are blocked at the gateway.

Security Control: 1502; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
All emails arriving via an external connection where the source address uses an internal domain name are blocked at the gateway.

Active web addresses in emails

Spoofed emails often contain an active web address directing users to a malicious website to illicit information or infect their workstation with malicious code. To reduce the success rate of such intrusions, organisations can strip active web addresses from emails and replace them with non-active versions.

Security Control: 1057; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Email servers strip active web addresses from emails and replace them with non-active versions.

Sender Policy Framework

SPF, and alternative implementations such as Sender ID, aid in the detection of spoofed emails. This is achieved by SPF records specifying a list of Internet Protocol (IP) addresses or domains that are allowed to send emails from specific domains. If an email server that sends an email is not in the SPF record for that domain, verification will fail.

Security Control: 0574; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Email servers are specified using SPF or Sender ID.

Security Control: 1183; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
A hard fail SPF record is used when specifying email servers.

Security Control: 1151; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
SPF or Sender ID is used to verify the authenticity of incoming emails.

Security Control: 1152; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Incoming emails that fail SPF checks are blocked, marked or identified in a manner that is visible to the email recipient.

DomainKeys Identified Mail

DKIM enables the detection of spoofed email contents. This is achieved by DKIM records specifying a public key that signs the contents of an email. If the signed digest in the email header does not match the signed contents of the email, verification will fail.

Security Control: 0861; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
DKIM signing is enabled on all email originating from an organisation's domain.

Security Control: 1025; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
DKIM is used in conjunction with SPF.

Security Control: 1026; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
DKIM signatures on received emails are verified, taking into account that email distribution list software typically invalidates DKIM signatures.

Security Control: 1027; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Email distribution list software used by external senders is configured such that it does not break the validity of the sender's DKIM signature.

Domain-based Message Authentication, Reporting and Conformance

Domain-based Message Authentication, Reporting and Conformance (DMARC) enables a domain owner to specify what action receiving email servers should take if they receive an email that fails a SPF/Sender ID or DKIM check. This includes 'reject' (the email is rejected), 'quarantine' (the email is marked as spam) or 'none' (no action is taken).

DMARC also provides a reporting feature which enables a domain owner to receive reports on the actions taken by receiving email servers. While this feature does not mitigate malicious emails sent to the domain owner's organisation, it can give the domain owner some visibility of attempts by adversaries to spoof their organisation's domains.

Security Control: 1540; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
A DMARC record is configured specifying that emails from an organisation's domains be rejected if they fail SPF/Sender ID or DKIM checks.

Further information

Further information on content filtering can be found in the ***Content filtering*** section of the ***Guidelines for data transfers and content filtering***.

Further information on implementing SPF can be found in the Australian Cyber Security Centre (ACSC)'s ***Mitigating Spoofed Emails Using Sender Policy Framework*** publication at https://www.acsc.gov.au/publications/protect/Spoof_Email_Sender_Policy_Framework.pdf.

Further information on email attachment filtering can be found in the ACSC's ***Malicious Email Mitigation Strategies*** publication at https://www.acsc.gov.au/publications/protect/Malicious_Email_Mitigation.pdf.

Further information on email security-related topics is available from the following documents:

- IETF RFC 4406, ***Sender ID: Authenticating E-Mail***, at https://tools.ietf.org/html/rfc4406.
- IETF RFC 4408, ***Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1***, at https://tools.ietf.org/html/rfc4408
- IETF RFC 4686, ***Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)***, at https://tools.ietf.org/html/rfc4686
- IETF RFC 4871, ***DomainKeys Identified Mail (DKIM) Signatures***, at https://tools.ietf.org/html/rfc4871

- IETF RFC 5617, ***DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)***, at https://tools.ietf.org/html/rfc5617.
- IETF RFC 7489, ***Domain-based Message Authentication, Reporting, and Conformance (DMARC)***, at https://tools.ietf.org/html/rfc7489.

Further information on email server security can be found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-45 Rev. 2, ***Guidelines on Electronic Mail Security***, at https://csrc.nist.gov/publications/detail/sp/800-45/version-2/final.