Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

APRIL 2019

Guidelines for email management

Email usage

Email usage policy

There are many security risks associated with the use of email that are often overlooked by users. Documenting these security risks, and associated mitigations, will inform users of 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

When users access non-approved webmail services they are effectively bypassing email content filtering controls as well as other security controls that may have been implemented for an organisation's email gateways and servers. While web content filtering controls may mitigate some security risks (e.g. some forms of malicious attachments), they are unlikely to address specific security risks relating to emails (e.g. spoofed email contents).

Security Control: 0267; Revision: 7; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Access to non-approved webmail services is blocked.

Protective markings for emails

Implementing protective markings for emails ensures that appropriate security controls are applied to information, and also helps to prevent unauthorised information being released into the public domain. In doing so, it is important that protective markings accurately reflect the information in the subject, body and attachments of emails.

Security Control: 0270; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Protective markings are applied to emails and reflect the information in their subject, body and attachments.

Protective marking tools

Requiring user involvement in the marking of emails ensures a conscious decision by users, thereby lessening the chance of incorrectly marked emails. In addition, allowing users to select only protective markings for which a system is authorised to process, store or communicate lessens the chance of users inadvertently over-classifying an email. This also serves to remind users of the maximum sensitivity or classification of information permitted on a system.

Email content filters may only check the most recent protective marking applied to an email. Therefore, when users are responding to or forwarding an email, requiring a protective marking which is at least as high as that of the email they

received will help email content 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: 3; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Should
Protective marking tools do not automatically insert protective markings into emails.

Security Control: 0272; Revision: 4; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Should
Protective marking tools do not allow users to select protective markings that a system has not been authorised to process, store or communicate.

Security Control: 1089; Revision: 4; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Protective 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.

Handling emails with inappropriate, invalid or missing protective markings

It is important that email servers are configured to block emails with inappropriate protective markings. For example, blocking inbound and outbound emails with a protective marking higher than the sensitivity or classification of the receiving system will prevent a data spill from occurring. In doing so, it is important to inform recipients of blocked inbound emails, and the sender of blocked outbound emails, that this has occurred.

If an email is received with an invalid or missing protective marking it may still be passed to its intended recipients; however, the recipients will have an obligation to determine the appropriate protective marking for the email if it is to be responded to, forwarded or printed. If unsure, the sender of the original email should be contacted to seek clarification of handling requirements.

Security Control: 0565; Revision: 4; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Email servers are configured to block, log and report emails with inappropriate protective markings.

Security Control: 1023; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Should
The intended recipients of any blocked inbound emails, and the sender of any blocked outbound emails, are notified.

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: 1; Updated: Mar-19; Applicability: P, S, TS; Priority: Must
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 gateways and servers

Centralised email gateways

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

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: 0571; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
When users send email from outside their network, an authenticated and encrypted channel is configured to allow email to be routed via a centralised email gateway.

Email gateway maintenance activities

An adversary will often avoid using an organisation's primary email gateway when sending malicious emails. This is because backup and alternative email gateways are often poorly maintained in terms of patches and email content filtering controls. As such, it is important that extra effort is made to ensure that backup and alternative email gateways are maintained to the same standard as the primary 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.

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 that email server. Such configurations are highly undesirable as spammers and worms can exploit them.

Security Control: 0567; Revision: 4; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Email servers only relay emails destined for or originating from their domains.

Email server transport encryption

Emails can be intercepted anywhere between originating email servers and destination email servers. Enabling Transport Layer Security (TLS) on email servers will mitigate the compromise of email traffic, with the exception of cryptanalysis of email traffic.

Implementing Internet Engineering Task Force (IETF) Request for Comments (RFC) 3207 can protect email traffic while ensuring email servers remain compatible with other email servers due to the use of opportunistic TLS encryption.

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.

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: 3; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Incoming emails that fail SPF checks are blocked or marked in a manner that is visible to the recipients.

DomainKeys Identified Mail

DKIM enables the detection of spoofed email contents. This is achieved by DKIM records specifying the public key used to sign an email's contents. Specifically, if the signed digest in the email header does not match the signed contents of the email, verification will fail.

Security Control: 0861; Revision: 2; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Should
DKIM signing is enabled on emails originating from an organisation's domains.

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.

Email content filtering

Content filtering performed on email bodies and attachments provides a defence-in-depth approach to preventing malicious content being introduced into a network. Specific guidance on implementing email content filtering can be found in the Australian Cyber Security Centre (ACSC)'s ***Malicious Email Mitigation Strategies*** publication.

Security Control: 1234; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Email content filtering controls are implemented for email bodies and attachments.

Blocking suspicious emails

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

Security Control: 0561; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Emails addressed to internal email aliases where the source address is from outside the domain are blocked at the email gateway.

Security Control: 1502; Revision: 1; Updated: Mar-19; Applicability: O, P, S, TS; Priority: Must
Emails arriving via an external connection where the source address uses an internal domain name are blocked at the email gateway.

Undeliverable messages

Undeliverable or bounce emails are commonly sent by receiving email servers when an 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.

Further information

Further information on implementing SPF can be found in the ACSC's ***Mitigating Spoofed Emails Using Sender Policy Framework*** publication at https://www.cyber.gov.au/publications/mitigating-spoofed-emails-sender-policy-framework-explained.

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 email content filtering can be found in the ACSC's ***Malicious Email Mitigation Strategies*** publication at https://www.cyber.gov.au/publications/malicious-email-mitigation-strategies.

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

- IETF RFC 3207, ***SMTP Service Extension for Secure SMTP over Transport Layer Security***, at https://tools.ietf.org/html/rfc3207.
- 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.