



Information Security Manual

Published: 02 March 2023

Guidelines for Email

Email usage

Email usage policy

As there are many security risks associated with the use of email services, it is important that an organisation develops, implements and maintains an email usage policy governing its use.

Control: ISM-0264; Revision: 4; Updated: Dec-22; Applicability: All; Essential Eight: N/A

An email usage policy is developed, implemented and maintained.

Webmail services

When users access non-approved webmail services, they often bypass controls that have been implemented by an organisation, such as email content filtering. To mitigate this security risk, access to non-approved webmail services should be blocked.

Control: ISM-0267; Revision: 7; Updated: Mar-19; Applicability: All; Essential Eight: N/A

Access to non-approved webmail services is blocked.

Protective markings for emails

Implementing protective markings for emails helps to prevent data spills, such as unauthorised data being released into the public domain. In doing so, it is important that protective markings reflect the highest sensitivity or classification of the subject, body and attachments of emails.

Control: ISM-0270; Revision: 6; Updated: Jun-21; Applicability: All; Essential Eight: N/A

Protective markings are applied to emails and reflect the highest sensitivity or classification of the subject, body and attachments.

Protective marking tools

Requiring user involvement in the protective marking of emails ensures a conscious decision is made by users, thereby lessening the chance of incorrect protective markings being applied to 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 emails.

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

received will help email content filters prevent emails being sent to systems that are not authorised to handle their original sensitivity or classification.

Control: ISM-0271; Revision: 3; Updated: Mar-19; Applicability: All; Essential Eight: N/A
Protective marking tools do not automatically insert protective markings into emails.

Control: ISM-0272; Revision: 4; Updated: Mar-19; Applicability: All; Essential Eight: N/A
Protective marking tools do not allow users to select protective markings that a system has not been authorised to process, store or communicate.

Control: ISM-1089; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A
Protective marking tools do not allow users replying to or forwarding emails to select protective markings lower than previously used.

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 protective markings higher than the sensitivity or classification of the receiving system, as this will prevent a data spill from occurring. In doing so, it is important to inform the intended recipients of blocked inbound emails, and the senders of blocked outbound emails, that this has occurred.

If emails are received with invalid or missing protective markings they may still be passed to their intended recipients. However, the recipients will have an obligation to determine appropriate protective markings if emails are to be responded to, forwarded or printed. If unsure, original senders of emails should be contacted to provide guidance on appropriate protective markings.

Control: ISM-0565; Revision: 4; Updated: Mar-19; Applicability: All; Essential Eight: N/A
Email servers are configured to block, log and report emails with inappropriate protective markings.

Control: ISM-1023; Revision: 6; Updated: Mar-22; Applicability: All; Essential Eight: N/A
The intended recipients of blocked inbound emails, and the senders of blocked outbound emails, are notified.

Email distribution lists

In some cases, the membership and nationality of members of email distribution lists will be unknown. As such, emails containing Australian Eyes Only, Australian Government Access Only or Releasable To data that are sent to email distribution lists could accidentally cause a data spill.

Control: ISM-0269; Revision: 5; Updated: Mar-22; Applicability: S, TS; Essential Eight: N/A
Emails containing Australian Eyes Only, Australian Government Access Only or Releasable To data are not sent to email distribution lists unless the nationality of all members of email 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's [Protective Security Policy Framework](#), [Sensitive and classified information](#) policy.

Email gateways and servers

Centralised email gateways

When routing emails via centralised email gateways it will be easier for an organisation to deploy Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting and Conformance (DMARC) and protective marking checks.

Control: ISM-0569; Revision: 5; Updated: Jun-22; Applicability: All; Essential Eight: N/A

Emails are routed via centralised email gateways.

Control: ISM-0571; Revision: 7; Updated: Jun-22; Applicability: All; Essential Eight: N/A

When users send or receive emails, an authenticated and encrypted channel is used to route emails via their organisation's centralised email gateways.

Email gateway maintenance activities

As backup and alternative email gateways are often poorly maintained in terms of patches and email content filtering, an adversary will often seek to exploit this when sending malicious emails to an organisation. As such, it is important that backup and alternative email gateways are maintained at the same standard as an organisation's primary email gateway.

Control: ISM-0570; Revision: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A

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 an email server that is configured to allow anyone on the internet to send emails through it. Such configurations are highly undesirable as spammers and worms can exploit them.

Control: ISM-0567; Revision: 5; Updated: Sep-22; Applicability: All; Essential Eight: N/A

Email servers only relay emails destined for or originating from their domains (including subdomains).

Email server transport encryption

Emails can be intercepted anywhere between originating email servers and destination email servers. Implementing opportunistic Transport Layer Security (TLS) encryption can mitigate this security risk while ensuring email servers remain compatible with each other. However, opportunistic TLS encryption is susceptible to downgrade attacks. To mitigate this security risk, Mail Transfer Agent Strict Transport Security (MTA-STS) allows domain owners to indicate that email transfers should only occur if satisfactory TLS encryption is negotiated beforehand.

Implementing MTA-STS reduces the opportunity for downgrade attacks during email transfers, and provides visibility of when they are attempted. TLS reporting supports the implementation of MTA-STS by providing a mechanism for a domain owner to publish a location where reports can be submitted regarding the success or failure of attempts to initiate encrypted connections when sending emails to a specified domain.

Control: ISM-0572; Revision: 4; Updated: Sep-21; Applicability: All; Essential Eight: N/A

Opportunistic TLS encryption is enabled on email servers that make incoming or outgoing email connections over public network infrastructure.

Control: ISM-1589; Revision: 2; Updated: Sep-22; Applicability: All; Essential Eight: N/A

MTA-STS is enabled to prevent the unencrypted transfer of emails between complying servers.

Sender Policy Framework

SPF aids in the detection of spoofed emails by specifying a list of hosts or Internet Protocol (IP) addresses that are allowed to send emails on behalf of a specified domain or subdomain. If an email server is not in the SPF record for a domain or subdomain, SPF verification will not pass. In specifying SPF records, domain owners should ensure that they delegate the minimum necessary set of hosts or IP addresses necessary for sending emails. In addition, extra care should be taken when delegating to hosts or IP addresses not under an organisation's control.

Control: ISM-0574; Revision: 6; Updated: Sep-22; Applicability: All; Essential Eight: N/A

SPF is used to specify authorised email servers (or lack thereof) for all domains (including subdomains).

Control: ISM-1183; Revision: 2; Updated: Sep-22; Applicability: All; Essential Eight: N/A

A hard fail SPF record is used when specifying authorised email servers (or lack thereof) for all domains (including subdomains).

Control: ISM-1151; Revision: 3; Updated: Oct-19; Applicability: All; Essential Eight: N/A
SPF is used to verify the authenticity of incoming emails.

DomainKeys Identified Mail

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

Control: ISM-0861; Revision: 3; Updated: Sep-22; Applicability: All; Essential Eight: N/A
DKIM signing is enabled on emails originating from an organisation's domains (including subdomains).

Control: ISM-1026; Revision: 5; Updated: Jan-20; Applicability: All; Essential Eight: N/A
DKIM signatures on received emails are verified.

Control: ISM-1027; Revision: 4; Updated: Sep-18; Applicability: All; Essential Eight: N/A
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

DMARC enables a domain owner to specify what action receiving email servers should take as a result of domain alignment, SPF and DKIM checks. For emails that do not pass DMARC checks, this includes 'reject' (emails are rejected), 'quarantine' (emails are 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 an adversary to spoof their organisation's domains.

Control: ISM-1540; Revision: 2; Updated: Sep-22; Applicability: All; Essential Eight: N/A
DMARC records are configured for all domains (including subdomains) such that emails are rejected if they do not pass DMARC checks.

Control: ISM-1799; Revision: 0; Updated: Sep-22; Applicability: All; Essential Eight: N/A
Incoming emails are rejected if they do not pass DMARC checks.

Email content filtering

Content filtering performed on email bodies and attachments provides a defence-in-depth approach to preventing malicious code being introduced into networks.

Control: ISM-1234; Revision: 5; Updated: Dec-22; Applicability: All; Essential Eight: N/A
Email content filtering is implemented to filter potentially harmful content in email bodies and attachments.

Blocking suspicious emails

Blocking specific types of suspicious emails, such as where the email source address uses an internal domain, or internal subdomain, reduces the likelihood of phishing emails entering an organisation's network.

Control: ISM-1502; Revision: 2; Updated: Sep-22; Applicability: All; Essential Eight: N/A
Emails arriving via an external connection where the email source address uses an internal domain, or internal subdomain, are blocked at the email gateway.

Notifications of undeliverable emails

Notifications of undeliverable emails are commonly sent by receiving email servers when emails cannot be delivered, usually because destination addresses are invalid. Due to the common spamming practice of spoofing sender addresses, this often results in a large number of notifications of undeliverable emails being sent to innocent third parties. Sending notifications of undeliverable emails only to senders that can be verified via SPF, or other trusted means, avoids contributing to this problem while allowing legitimate senders to be notified.

Control: *ISM-1024; Revision: 5; Updated: Mar-22; Applicability: All; Essential Eight: N/A*

Notifications of undeliverable emails are only sent to senders that can be verified via SPF or other trusted means.

Further information

Further information on implementing opportunistic TLS encryption for email servers can be found in the Australian Cyber Security Centre (ACSC)'s [Implementing Certificates, TLS, HTTPS and Opportunistic TLS](#) publication.

Further information on implementing SPF, DKIM and DMARC can be found in the ACSC's [How to Combat Fake Emails](#) publication.

Further information on engaging the services of email service providers for marketing or filtering purposes can be found in the ACSC's [Marketing and Filtering Email Service Providers](#) publication.

Further information on email content filtering can be found in the content filtering section of the [Guidelines for Gateways](#).

Further information on email content filtering can be found in the ACSC's [Malicious Email Mitigation Strategies](#) publication.

Further information on email security can be found in the following National Institute of Standards and Technology (NIST) publications:

- NIST Special Publication (SP) 800-45 Rev. 2, [Guidelines on Electronic Mail Security](#)
- NIST SP 800-177 Rev. 1, [Trustworthy Email](#)
- NIST SP 1800-6, [Domain Name System-Based Electronic Mail Security](#).