Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

JUNE 2021

Guidelines for Email

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, in an email usage policy will inform users of precautions to take when using email.

Security Control: 0264; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS
An email usage policy 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
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 data, and also helps to prevent 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.

Security Control: 0270; Revision: 6; Updated: Jun-21; Applicability: O, P, S, TS
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 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 data 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
Protective marking tools do not automatically insert protective markings into emails.

Security Control: 0272; Revision: 4; Updated: Mar-19; Applicability: O, P, S, TS
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
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
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
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 Releasable To (REL) data to distribution lists could accidentally cause a data spill.

Security Control: 0269; Revision: 4; Updated: Jun-21; Applicability: S, TS
Emails containing AUSTEO, AGAO or REL data 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's ***Protective Security Policy Framework***, ***Sensitive and classified information*** policy, at https://www.protectivesecurity.gov.au/information/sensitive-classified-information/Pages/default.aspx.

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
Email is routed through a centralised email gateway.

Security Control: 0571; Revision: 5; Updated: Mar-19; Applicability: O, P, S, TS
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
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
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.

Opportunistic TLS for email is susceptible to downgrade attacks. Mail Transfer Agent Strict Transport Security (MTA-STS) allows domain owners to indicate to other email servers that emails should only be sent if satisfactory TLS encryption is negotiated prior to transfer.

Implementing IETF RFC 8461 reduces the opportunity for downgrade attacks during email transfer and provides email server operators with visibility when downgrade attacks are attempted. IETF RFC 8460 supports the implementation of IETF RFC 8461 by providing a mechanism for a domain owner to publish a location where other email server operators can submit reports about their success or failure trying to initiate encrypted sessions when sending email to the specified domain.

Security Control: 0572; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
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.

Security Control: 1589; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
MTA-STS, as defined in IETF RFC 8461, is enabled to prevent the transfer of unencrypted emails between complying servers.

Sender Policy Framework

SPF aids in the detection of spoofed emails by specifying a list of domains that are allowed to send emails. If an email server is not in the SPF record for a domain, SPF verification will fail.

Security Control: 0574; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
SPF is used to specify authorised email services (or lack thereof) for all domains.

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

Security Control: 1151; Revision: 3; Updated: Oct-19; Applicability: O, P, S, TS
SPF is used to verify the authenticity of incoming emails.

Security Control: 1152; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS
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
DKIM signing is enabled on emails originating from an organisation's domains.

Security Control: 1026; Revision: 5; Updated: Jan-20; Applicability: O, P, S, TS
DKIM signatures on received emails are verified.

Security Control: 1027; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
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 SPF or DKIM checks. 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: 1; Updated: Oct-19; Applicability: O, P, S, TS
DMARC records are configured for all domains such that emails are rejected if they fail SPF 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
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: 1502; Revision: 1; Updated: Mar-19; Applicability: O, P, S, TS
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
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 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 at https://www.cyber.gov.au/acsc/view-all-content/publications/malicious-email-mitigation-strategies.

Further information on implementing SPF, DKIM and DMARC can be found in the ACSC's ***How to Combat Fake Emails*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/how-combat-fake-emails.

Further information on implementing opportunistic TLS encryption for email servers can be found in the ACSC's ***Implementing Certificates, TLS, HTTPS and Opportunistic TLS*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-certificates-tls-https-and-opportunistic-tls.

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 at https://www.cyber.gov.au/acsc/view-all-content/publications/marketing-and-filtering-email-service-providers.

Further information on opportunistic TLS encryption can be found in IETF RFC 3207 and its related update:

- IETF RFC 3207, ***SMTP Service Extension for Secure SMTP over Transport Layer Security***, at https://tools.ietf.org/html/rfc3207
- IETF RFC 7817, ***Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols***, at https://tools.ietf.org/html/rfc7817.

Further information on MTA-STS and associated reporting can be found in IETF RFC 8461 and IETF RFC 8460:

- IETF RFC 8461, ***SMTP MTA Strict Transport Security (MTA-STS)***, at https://tools.ietf.org/html/rfc8461
- IETF RFC 8460, ***SMTP TLS Reporting***, at https://tools.ietf.org/html/rfc8460.

Further information on SPF can be found in IETF RFC 7208 and its related updates:

- IETF RFC 7208, ***Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1***, at https://tools.ietf.org/html/rfc7208
- IETF RFC 7372, ***Email Authentication Status Codes***, at https://tools.ietf.org/html/rfc7372
- IETF RFC 8553, ***DNS AttrLead Changes: Fixing Specifications That Use Underscored Node Names***, at https://tools.ietf.org/html/rfc8553
- IETF RFC 8616, ***Email Authentication for Internationalized Mail***, at https://tools.ietf.org/html/rfc8616.

Further information on DKIM can be found in IETF RFC 6376 and its related updates:

- IETF RFC 6376, ***DomainKeys Identified Mail (DKIM) Signatures***, at https://tools.ietf.org/html/rfc6376

- IETF RFC 8301, ***Cryptographic Algorithm and Key Usage Update to DomainKeys Identified Mail (DKIM)***, at https://tools.ietf.org/html/rfc8301
- IETF RFC 8463, ***A New Cryptographic Signature Method for DomainKeys Identified Mail (DKIM)***, at https://tools.ietf.org/html/rfc8463
- IETF RFC 8553, ***DNS AttrLead Changes: Fixing Specifications That Use Underscored Node Names***, at https://tools.ietf.org/html/rfc8553
- IETF RFC 8616, ***Email Authentication for Internationalized Mail***, at https://tools.ietf.org/html/rfc8616.

Further information on DMARC can be found in IETF RFC 7489 and its related updates:

- IETF RFC 7489, ***Domain-based Message Authentication, Reporting, and Conformance (DMARC)***, at https://tools.ietf.org/html/rfc7489
- IETF RFC 8553, ***DNS AttrLead Changes: Fixing Specifications That Use Underscored Node Names***, at https://tools.ietf.org/html/rfc8553
- IETF RFC 8616, ***Email Authentication for Internationalized Mail***, at https://tools.ietf.org/html/rfc8616.

Further information on email security is available from the National Institute of Standards and Technology (NIST):

- 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
- NIST SP 800-177 Rev. 1, ***Trustworthy Email***, at https://csrc.nist.gov/publications/detail/sp/800-177/rev-1/final
- NIST SP 1800-6, ***Domain Name System-Based Electronic Mail Security***, at https://www.nccoe.nist.gov/publication/1800-6/.