GOV.UK

1. Home (https://www.gov.uk/)

Guidance

Securing government email

Apply the government secure email policy.

Published 24 August 2016
Last updated 9 September 2019 — see all updates

From:
Government Digital Service (https://www.gov.uk/government/organisations/government-digital-service)

Contents

Print this page

This guidance applies to all email domains that public sector organisations run on the internet. You should follow this guidance if you're in a role responsible for making sure your organisation exchanges email securely with other public sector organisations.

All gsi-family domain names (https://www.gov.uk/government/publications/changing-government-email-migrating-from-gsi/changing-government-email-migrating-from-gsi) (gsi.gov.uk, gse.gov.uk, gcsx.gov.uk or gsx.gov.uk) must now be replaced with a government domain like gov.uk, gov.scot, llyw.cymru or gov.wales.

How to secure email

You must:

- encrypt and authenticate email in transit by supporting Transport Layer Security (TLS) (https://www.gov.uk/government/publications/email-security-standards/transport-layer-security-tls) and Domain-based Message Authentication, Reporting and Conformance (DMARC) (https://www.gov.uk/government/publications/email-security-standards/domain-based-message-authentication-reporting-and-conformance-dmarc) as a minimum
- use extra encryption if your data needs more protection
- make sure the recipient protects the data you send to them
- make email security invisible to end users as far as practically possible

Central government organisations should already have implemented encryption and authentication in line with the Minimum Cyber Security Standard (https://www.gov.uk/government/publications/the-minimum-cyber-security-standard).

Encrypt and authenticate email in transit

Protecting your email in transit makes it difficult to spoof your domain. Encryption and authentication only work if both the sender and the recipient use them.

To meet the Minimum Cyber Security Standard and protect email you must:

- support Transport Layer Security Version 1.2 (https://www.gov.uk/government/publications/email-security-standards/transport-layer-security-tls) (TLS v1.2) or later for sending and receiving email securely
- have Domain-based Message Authentication Reporting and Conformance (DMARC) (https://www.gov.uk/government/publications/email-security-standards/domain-based-message-authentication-reporting-and-conformance-dmarc), DomainKeys Identified Mail (DKIM) (https://www.gov.uk/government/publications/email-security-standards/domainkeys-identified-mail-dkim) and Sender Policy Framework (SPF) (https://www.gov.uk/government/publications/email-security-standards/sender-policy-framework-spf) records in place to make email spoofing difficult
- implement spam and malware filtering, and enforce DMARC on inbound email

The Government Digital Service recommends protecting email by:

- forcing TLS when sending to *.gov.uk
- forcing TLS when sending to any other domains you know support it if your local risk profile requires it
- making sure you know if a TLS connection fails and your users know what to do if there is a problem
- signing up to the NCSC Mail Check service (https://www.ncsc.gov.uk/mailcheck) to access your DMARC reports
- having rules in place to handle organisations that don't support TLS 1.2 - set up TLS Reporting (TLS-RPT) (https://www.hardenize.com/blog/smtp-tls-reporting-tls-rpt) and send reports to the NCSC Mail Check service at tls-rua@mailcheck.service.ncsc.gov.uk to make this easier in the future
- using extra encryption services if you need them

Read the how to set up government email services securely (https://www.gov.uk/guidance/set-up-government-email-services-securely) for detailed information on how to set up TLS, DMARC, SPF and DKIM.

Use extra encryption if your data needs more protection

If you need extra security for individual messages consider using an end-to-end email encryption tool or service from the Digital Marketplace (https://www.digitalmarketplace.service.gov.uk/g-cloud/search?q=email+encryption&lot=cloud-software). Choose a tool or service that does not place unnecessary burdens on the user receiving information.

If you routinely share bulk data with third parties consider using a secure web service or a secure bulk data transfer service.

Make sure the data you send is appropriately protected by the recipient

As an information owner, you're responsible for managing your organisation's security risks. You should consider the protection of your data at rest as well as in transit. There is no standard list of approved, secure email domains for government. Your organisation must decide what assurance you need based on your own data and your own risk profile.

You need to understand possible risks when sharing information with other organisations and take steps to help protect your data. There are a number of approaches you can take to protect data including:

- checking to make sure the recipient has independent accreditation that shows good security practice such as Cyber Essentials Plus (https://www.cyberessentials.ncsc.gov.uk/cert-search/) or ISO 27001 (https://www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-directory/)
- asking the recipient organisation about their cyber security practices using the 10 steps to cyber security guidance (https://www.ncsc.gov.uk/guidance/10-steps-executive-summary)
- creating a data-sharing agreement between your organisations
- relying on the reasonable expectation that the organisation you send data to will protect the data as required by legal or regulatory requirements like GDPR (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/) or the NIS Directive (https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive)
- using additional encryption methods described above to protect the data in transit and at rest so you do not have to get any security information from the recipient

Make email security invisible to end users

Email security should be invisible to the end user as far as possible. Users should have the option to mark sensitive information if needed but not have to make complex technical decisions about sending data.

Do not make security difficult for users as they may find less secure work-arounds. Provide guidance so users:

- can continue to work with minimal disruption
- understand and can act on error or bounce-back messages
- know who to contact if things go wrong
- know if they have permission to send information by an insecure route if a secure route fails

Further email security guidance

For more information about email security, see:

- Set up government email services securely (https://www.gov.uk/guidance/set-up-government-email-services-securely)
- Changing government email: migrating from .gsi (https://www.gov.uk/government/publications/changing-government-email-migrating-from-gsi/changing-government-email-migrating-from-gsi)
- NCSC guidance on TLS (https://www.ncsc.gov.uk/guidance/tls-external-facing-services)
- Government policy on email security (https://www.gov.uk/government/publications/government-network-policy-changes/government-network-policy-changes)
- Email security standards (https://www.gov.uk/government/publications/email-security-standards)

- Minimum Cyber Security Standard (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/719067/25062018_Minimum_Cyber_Security_Standard_gov.uk__3_.pdf)
- Sender Policy Framework (https://www.gov.uk/government/publications/email-security-standards/sender-policy-framework-spf)
- Technology Code of Practice (https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice)
- Protect domains that don't send email (https://www.gov.uk/guidance/protect-domains-that-dont-send-email)
- Sending emails from your service domain (https://www.gov.uk/service-manual/technology/how-to-email-your-users)

Published 24 August 2016
Last updated 9 September 2019 + show all updates

1. 9 September 2019
   Updated information about TLS.
2. 24 January 2019
   Updated information about encryption, authentication and protection of data at rest
3. 18 April 2018
   The approach to email security is changing and we have removed the need to pass an assessment.
4. 25 August 2016
   In this version of the guidance, CTS has: * changed and removed wording throughout the document to make it easier to understand * moved technical detail into the set up guide * changed the document title in line with GDS style * restructured the document around the three aspects of encryption, anti-spoofing, and assessment * removed references to ADSP as it is no longer used widely enough to be valuable
5. 24 August 2016
   First published.

Print this page

Brexit transition

31 days to go

Check you're ready for 2021

(https://www.gov.uk/transition)

Related content

- Protect domains that don't send email (https://www.gov.uk/guidance/protect-domains-that-dont-send-email)
- Secure email guidance (https://www.gov.uk/government/collections/secure-email-guidance)
- Email security standards (https://www.gov.uk/government/publications/email-security-standards)
- Set up government email services securely (https://www.gov.uk/guidance/set-up-government-email-services-securely)
- How Welsh public sector organisations migrated email from the PSN to the internet (https://www.gov.uk/government/case-studies/how-welsh-public-sector-organisations-migrated-email-from-the-psn-to-the-internet)

Collection

- Secure email guidance (https://www.gov.uk/government/collections/secure-email-guidance)