GOV.UK

1. Home (https://www.gov.uk/)
2. Government (https://www.gov.uk/government/all)
3. Government efficiency, transparency and accountability (https://www.gov.uk/government/government-efficiency-transparency-and-accountability)

Collection

Securing technology at OFFICIAL

Guidance on how organisations should secure their technology and services to protect UK government information classified as OFFICIAL.

Published 6 March 2015
Last updated 2 November 2015 — see all updates

From:
Cabinet Office (https://www.gov.uk/government/organisations/cabinet-office) and CESG (https://www.gov.uk/government/organisations/cesg)

Contents

The vast majority of UK government business is conducted at the OFFICIAL classification. This includes routine information supporting business operations and services, much of which would have damaging consequences if lost or stolen.

Security at OFFICIAL is achieved through following good commercial practices, using well configured commodity technologies and by people taking personal responsibility and using their judgement more actively.

Achieving Secure Technology

The Government Security Policy Framework (https://www.gov.uk/government/publications/security-policy-framework) describes government's overall approach to protective security. Security is achieved through understanding your true security needs and matching these requirements to technology available. It should be focused on meeting outcomes that have been clearly defined, rather than applying prescriptive controls.

Whilst technology risks must always be effectively managed, there are opportunities for organisations to develop innovative solutions and use modern, commodity technologies and tools. Security must be considered when making decisions about technology, and it should be balanced against other needs of the service.

Risk management at OFFICIAL

The links below, and our wider portfolio of risk management products, provide guidance on developing an effective approach to the assessment and management of information risk within technology projects. We also highlight common characteristics that we have observed in technology projects where risk is managed well and enables effective decision making about security.

Our portfolio of risk management guidance can be found at https://www.gov.uk/government/collections/risk-management-guidance (https://www.gov.uk/government/collections/risk-management-guidance). Or the following highlights are the best places to start.

- Security considerations for common enterprise IT decisions (https://www.gov.uk/guidance/security-considerations-for-common-enterprise-it-decisions)
  - 6 March 2015
  - Guidance

Securing data in transit at OFFICIAL

The items below should help with the design and implementation of controls to protect data as it transits across networks.

- Network principles (https://www.gov.uk/government/publications/network-principles)
  - 7 July 2015
  - Guidance

Published 6 March 2015
Last updated 2 November 2015 + show all updates

1. 2 November 2015
   Added guidance on Google Apps for Work and Microsoft Office 365 that was commissioned by a government department
2. 2 September 2015
   Added links to the recently published Network Principles and TLS configuration guidance.
3. 6 March 2015
   First published.

Brexit transition

39 days to go

Check you’re ready for 2021

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

Related content

- Security considerations for common enterprise IT decisions (https://www.gov.uk/guidance/security-considerations-for-common-enterprise-it-decisions)
- Network principles (https://www.gov.uk/government/publications/network-principles)

Explore the topic

- Government efficiency, transparency and accountability (https://www.gov.uk/government/government-efficiency-transparency-and-accountability)
- National security (https://www.gov.uk/government/national-security)