Information Security Manual

Published: 21 September 2023

September 2023 Changes

A summary of content changes for the latest update of the *Information Security Manual* (ISM) are covered below.

Guidelines for Cyber Security Roles

Contributing to business continuity and disaster recovery planning

The existing control relating to the Chief Information Security Officer (CISO) contributing to the development and maintenance of business continuity and disaster recovery plans was amended to include contributing to the implementation of these plans as well. [ISM-0734]

Communicating a cyber security vision and strategy

The existing control relating to the CISO developing, implementing and maintaining a cyber security communications strategy was amended to clarify that this is for the purpose of assisting them in the communication of the cyber security vision and strategy for their organisation. [ISM-0720]

Guidelines for Personnel Security

System usage policy

A new control was added covering the development, implementation and maintenance of system usage policies. Previously, such policies were only referenced in the control covering the use of logon banners for systems. [ISM-1864]

System access requirements

A new control was added covering personnel agreeing to abide by system usage policies before being granted access to systems and their resources. In doing so, such agreements should be in the form of a written acknowledgement, for example, personnel signing a copy of a system usage policy acknowledging that they have read its contents and agree to abide by them. [ISM-1865]

Privileged access to systems

The essential eight applicability marking for the existing control relating to privileged users being assigned a dedicated privileged account to be used solely for duties requiring privileged access was updated to reflect that it maps to the restrict administrative privileges mitigation strategy within the *Essential Eight Maturity Model*. [ISM-0445]

Recording authorisation for personnel to access systems

The existing control relating to maintaining a secure record of authorisations for personnel to access systems was amended to include the retention of signed copies of agreements by personnel to abide by system usage policies. [ISM-0407]

Guidelines for Enterprise Mobility

Privately-owned mobile devices and desktop computers

Existing controls relating to the use of privately-owned mobile devices were amended to include privately-owned desktop computers when used as part of working from home arrangements. [ISM-1297, ISM-1400, ISM-0694]

The existing control relating to the use of privately-owned mobile devices for accessing OFFICIAL: Sensitive or PROTECTED systems or data was amended to separate out the requirement for an approved mobile platform into its own control. [ISM-1400, ISM-1867]

A new control was added covering the prevention of OFFICIAL: Sensitive and PROTECTED data being stored on privately-owned mobile devices and desktop computers. [ISM-1866]

Organisation-owned mobile devices and desktop computers

The existing control relating to the use of organisation-owned mobile devices was amended to include organisation-owned desktop computers, when used as part of working from home arrangements, and with organisations either prohibiting the use of such devices for personal purposes or having enforced separation of work data from any personal data. [ISM-1482]

Connecting mobile devices and desktop computers to the internet

The existing control relating to users of mobile devices accessing the internet via a Virtual Private Network connection to their organisation's secure internet gateway was amended to include desktop computers when used as part of working from home arrangements. [ISM-0874]

Mobile device management policy

The existing control relating to Mobile Device Management (MDM) solutions being used to enforce mobile device management policy was amended to ensure that such MDM solutions have completed a Common Criteria evaluation against the *Protection Profile for Mobile Device Management*, version 4.0 or later. [ISM-1195]

Approved mobile platforms

The existing control relating to mobile devices not accessing OFFICIAL: Sensitive or PROTECTED systems or data unless using an ASD-approved platform was amended to ensure such mobile platforms have completed a Common Criteria evaluation against the *Protection Profile for Mobile Device Fundamentals*, version 3.2 or later. [ISM-1867]

The existing control relating to mobile devices not accessing SECRET or TOP SECRET systems or data unless approved by ASD was amended to clearly articulate that approval by ASD constitutes the issuing of an Approval for Use (AFU) by ASD and operation in accordance with the latest version of their associated Australian Communications Security Instruction. [ISM-0687]

Data storage

A new control was added covering ASD approval being required before any removal media is used with SECRET and TOP SECRET mobile devices. [ISM-1868]

Personnel awareness

The existing control relating to taking specific precautions when travelling overseas with mobile devices was amended to reflect that the advice is also applicable to using mobile devices domestically. In addition, the control was amended to discourage the use of gifted or unauthorised peripherals with mobile devices. [ISM-1299]

While travelling overseas with mobile devices

The existing control relating to travelling overseas with mobile devices was amended to note that stolen or lost mobile devices or removable media should still be reported as a potential compromise even if they are later returned or found. [ISM-1088]

Guidelines for ICT Equipment

Hardening ICT equipment configurations

The existing control covering hardening of ICT equipment was reworded to ensure consistency of language with similar controls. [ISM-1858]

ICT equipment registers

The existing control relating to an ICT equipment register being developed, implemented and maintained was split into two controls to allow for the optional implementation of separate registers for networked ICT equipment (i.e. those connected to a network and having an IP address) and non-networked ICT equipment (those disconnected from networks and not having an IP address). [ISM-0336, ISM-1869]

On-site maintenance and repairs

The existing controls relating to on-site maintenance and repairs of ICT equipment by uncleared technicians were amended to instead reference technicians that are not appropriately cleared (i.e. they either hold no security clearance or a security clearance lower than what is required). [ISM-0306, ISM-0307]

Guidelines for Media

Supervision of destruction

The existing control covering the destruction of media was slightly reworded to ensure consistency of language. [ISM-0370]

Supervision of accountable material destruction

The existing control covering the destruction of media storing accountable material was slightly reworded to ensure consistency of language. [ISM-0372]

Guidelines for System Hardening

Hardening operating system configurations

The existing control covering hardening of operating systems was reworded to ensure consistency of language with similar controls. [ISM-1409]

Application control

Two new controls were added covering locations on disk that application control should be implemented, i.e. 'user profiles and temporary folders used by operating systems, web browsers and email clients' and everywhere else. Organisations implementing Essential Eight Maturity Level One should implement the first control while organisations implementing Maturity Level Two or Maturity Level Three should implement both controls. [ISM-1870, ISM-1871]

Hardening user application configurations

The existing control covering the hardening of office productivity suites was amended to recommend the implementation of both ASD and vendor hardening guidance, noting that ASD hardening guidance should generally be given preference when conflicting guidance arises. [ISM-1859]

The existing control covering the hardening of web browsers was amended to recommend the implementation of both ASD and vendor hardening guidance, noting that ASD hardening guidance should generally be given preference when conflicting guidance arises. [ISM-1412]

The existing control covering the hardening of PDF software was amended to recommend the implementation of both ASD and vendor hardening guidance, noting that ASD hardening guidance should generally be given preference when conflicting guidance arises. [ISM-1860]

Hardening server applications configurations

The existing control covering hardening of server applications was reworded to ensure consistency of language with similar controls. [ISM-1246]

Multi-factor authentication

Three existing controls relating to using multi-factor authentication to authenticate users of online services were reworded to ensure consistency of language with similar controls. [ISM-1504, ISM-1679, ISM-1680]

The existing control relating to an organisation's non-organisational users using multi-factor authentication to authenticate to the organisation's online services (but being able to opt out) was rewritten to clearly articulate the underlying intent. Specifically, the use of multi-factor authentication by users of online customer services (e.g. citizen-facing services) that process, store or communicate sensitive data (e.g. personally identifiable information) – not, for example, non-organisational users, such as contractors and service providers, opting out of using multi-factor authentication for remote access to an organisation they are supporting. [ISM-1681]

A minor grammatical change was made to the existing control on the use of multi-factor authentication for authenticating users of important data repositories. [ISM-1505]

The existing control relating to the implementation of phishing-resistant multi-factor authentication was split into four separate controls reflecting the different scenarios in which it may be applied by an organisation as they progressively adopt the technology. Specifically, one control for users of systems (e.g. local authentication to workstations), one control for users of online services (e.g. use of cloud services) and two controls for users of online customer services. [ISM-1682, ISM-1872, ISM-1873, ISM-1874]

Protecting credentials

The existing control on implementing PPL for LSASS was amended to remove the requirement for an UEFI lock. Rather, organisations are encouraged to implement UEFI locks for security functionality such as PPL for LSASS, Windows Defender Credential Guard and Windows Defender Remote Credential guard where appropriate and supported by workstations. [ISM-1861]

A new control was added covering at least monthly scanning of networks to identify any credentials that are being stored in an unprotected manner on networks, such as passwords and API keys being kept in the clear in documents, on network file shares or in other data repositories. [ISM-1875]

Logon banner

The existing control relating to logon banners was amended to note that logon banners act as reminder for users of their security responsibilities rather than a legally binding acceptance of system usage policies by users. [ISM-0408]

The existing control requiring organisations to seeking legal advice on the exact wording of logon banners was rescinded. Rather, organisations should seek legal advice on any usage policies for systems, or any of their resources, whenever they deem it appropriate to do so. [ISM-0979]

Guidelines for System Management

Scanning for missing patches or updates

The existing control relating to using a vulnerability scanner to identify missing patches or updates for vulnerabilities in 'operating systems of internet-facing services' was amended to 'operating systems of internet-facing servers and internet-facing network devices' to reduce confusion as to its applicability. [ISM-1701]

The existing control relating to using a vulnerability scanner to identify missing patches or updates for vulnerabilities in 'operating systems of workstations, servers and network devices' was amended to 'operating systems of workstations, non-internet-facing servers and non-internet-facing network devices' to reduce confusion as to its applicability. [ISM-1702]

When to patch vulnerabilities

The existing controls relating to patching, updating or applying other vendor mitigations for vulnerabilities within two weeks of release, or 48 hours of release when working exploits exist, were all split into two separate controls to allow for separate assessment of standard patching practices (i.e. within two weeks) and quick response patching practices (i.e. within 48 hours). In addition, scenarios in which vulnerabilities are assessed as critical by vendors (e.g. they facilitate remote code exploitation without user interaction, or facilitate authentication bypasses that grant privileged access) have been included within the quick response patching window. Typically, vendors or ASD will release 'critical alerts' for situations that require a quick response. [ISM-1690, ISM-1694, ISM-1697, ISM-1751, ISM-1876, ISM-1877, ISM-1878, ISM-1879]

The existing control (now two controls) relating to applying patches, updates or other vendor mitigations to vulnerabilities in 'operating systems of internet-facing services' was amended to 'operating systems of internet-facing servers and internet-facing network devices' to reduce confusion as to its applicability. [ISM-1694, ISM-1877]

The existing controls relating to applying patches, updates or other vendor mitigations to vulnerabilities in 'operating systems of workstations, servers and network devices' was amended to 'operating systems of workstations, non-internet-facing servers and non-internet-facing network devices' to reduce confusion as to its applicability. [ISM-1695, ISM-1696]

Guidelines for Networking

Network access controls

The existing control relating to the implementation of network access controls to prevent the connection of unauthorised network devices was extended to include other ICT equipment. [ISM-0520]

A minor grammatical change was made to the existing control on the use of network access controls to limit the flow of network traffic between network segments. [ISM-1182]

Blocking anonymity network traffic

A minor grammatical change was made to the existing control on blocking inbound network connections from anonymity networks. [ISM-1627]

Guidelines for Cryptography

Communications security doctrine

A minor grammatical change was made to the existing control on compliance with all communications security doctrine produced by ASD. [ISM-0499]

Approved High Assurance Cryptographic Equipment

The existing control relating to the use of High Assurance Cryptographic Equipment (HACE) was amended to clearly articulate that approval by ASD constitutes the issuing of an AFU by ASD and operation in accordance with the latest version of their associated Australian Communications Security Instructions. [ISM-1802]

Encrypting data at rest

A minor language change was made to the existing control on encrypting media containing SECRET or TOP SECRET data. [ISM-0460]

Encrypting data in transit

A minor language change was made to the existing control on encrypting SECRET and TOP SECRET data in transit. [ISM-0467]

Guidelines for Gateways

System administrators for gateways

A minor grammatical change was made to the existing control on identifying suitable system administrators for gateways. [ISM-1520]

Various guidelines

Cyber security terminology

References to 'ACSC' were replaced with 'ASD'. [ISM-0043, ISM-0140, ISM-0247, ISM-0248, ISM-0249, ISM-0286, ISM-0290, ISM-0296, ISM-0300, ISM-0321, ISM-0499, ISM-0597, ISM-1079, ISM-1137, ISM-1246, ISM-1409, ISM-1412, ISM-1858, ISM-1859, ISM-1860]

References to 'an adversary' were replaced with 'malicious actors'. [ISM-1213]

References to 'incident management' were replaced with 'cyber security incident management'. [ISM-0576, ISM-1784]

References to 'incident response plan' were replaced with 'cyber security incident response plan'. [ISM-0043, ISM-0576, ISM-1784, ISM-1819]

References to 'internet-facing services' were replaced with 'online services'. [ISM-1504, ISM-1679, ISM-1680, ISM-1698, ISM-1690, ISM-1704]

References to 'security vulnerabilities' were replaced with 'vulnerabilities'. [ISM-0300, ISM-0402, ISM-1163, ISM-1606, ISM-1690, ISM-1691, ISM-1692, ISM-1693, ISM-1694, ISM-1695, ISM-1696, ISM-1697, ISM-1698, ISM-1699, ISM-1700, ISM-1701, ISM-1702, ISM-1703, ISM-1717, ISM-1751, ISM-1752, ISM-1754]

References to 'OFFICIAL systems', 'OFFICIAL mobile devices', 'OFFICIAL cables' and 'OFFICIAL wall outlet boxes' were replaced with OFFICIAL: Sensitive terminology (e.g. OFFICIAL: Sensitive mobile devices) to correctly reflect the highest sensitivity of data such systems, devices and infrastructure can process, store and communicate (i.e. up to Business Impact Level 2). [ISM-0248, ISM-0926, ISM-1107, ISM-1196, ISM-1198, ISM-1199, ISM-1200, ISM-1400]

References to sensitive and classified systems or data, where it now only relates to classified systems or data (i.e. OFFICIAL: Sensitive and above), have been replaced with references to classified systems or data. [ISM-0810, ISM-1053, ISM-1530]

Contact details

If you have any questions regarding this guidance you can write to us or call us on (02) 5130 0156.