Australian Government
Australian Signals Directorate

Information Security Manual

Published: 1 December 2023

December 2023 Changes

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

Guidelines for Cyber Security Incidents

Reporting cyber security incidents to customers or the public

A new control recommending cyber security incidents involving customer data be reported to customers and the public in a timely manner after they occur or are discovered was added. [ISM-1880]

A new control recommending cyber security incidents not involving customer data be reported to customers and the public in a timely manner after they occur or are discovered was added. [ISM-1881]

Enacting cyber security incident response plans

The existing control relating to enacting a cyber security incident response plan following the identification of cyber security incidents was reworded. [ISM-1819]

Guidelines for Procurement and Outsourcing

Cyber supply chain risk management activities

The existing control relating to applications, ICT equipment and services being chosen from suppliers that have a strong track record of transparency and maintaining the security of their own systems and cyber supply chains was split into two separate controls. [ISM-1632, ISM-1882]

Guidelines for Personnel Security

Unprivileged access to systems

The existing control relating to the centralised storage of unprivileged access event logs was merged into the existing control relating to collecting unprivileged access event logs. [ISM-1566, ISM-1714]

Privileged access to systems

The existing control relating to validating requests for privileged access to data repositories was merged into the existing control relating to validating requests for privileged access to systems and applications. [ISM-1507, ISM-1733]

The existing control relating to limiting privileged access to data repositories based on user duties was merged into the existing control relating to limiting access to systems and applications based on user duties. [ISM-1508, ISM-1853]

The existing controls relating to privileged user accounts and privileged service accounts being prevented from accessing the internet, email and web services were merged. Furthermore, the merged control was amended to include an exclusion to allow for explicitly authorised privileged accounts to access online services. [ISM-1175, ISM-1653]

A new control recommending privileged accounts explicitly authorised to access online services be strictly limited to only what is required for users and services to undertake their duties was added. [ISM-1883]

The existing control relating to the centralised storage of privileged access event logs was merged into the existing control relating to collecting privileged access event logs. [ISM-1509, ISM-1651]

The existing control relating to the centralised storage of privileged account and group management event logs was merged into the existing control relating to collecting privileged account and group management event logs. [ISM-1650, ISM-1652]

Suspension of access to systems

Existing controls relating to automatically disabling access to systems, applications and data repositories after 45 days of inactivity were amended to remove the requirement that it occur automatically, noting that in some cases supporting governance mechanisms may be required to assist in identifying when accounts have not been used within the last 45 days. [ISM-1404, ISM-1647, ISM-1648, ISM-1716]

The existing control relating to privileged access to data repositories being automatically disabled after 12 months unless revalidated was merged into the existing control relating to privileged access to systems and applications being disabled after 12 months unless revalidated. [ISM-1647, ISM-1734]

Emergency access to systems

The existing control relating to the centralised storage of break glass account event logs was merged into the existing control relating to collecting break glass account event logs. [ISM-1613, ISM-1715]

Guidelines for Communications Infrastructure

Emanation security doctrine

A new control recommending all emanation security doctrine produced by the Australian Signals Directorate (ASD) be complied with was added. [ISM-1884]

Emanation security threat assessments

The existing control relating to conducting emanation security threat assessments for SECRET or TOP SECRET systems within shared facilities was merged with the existing control relating to conducting emanation security threat assessments for SECRET or TOP SECRET systems that have radio frequency transmitters. Furthermore, the requirement to implement additional installation criteria derived from an emanation security threat assessment was split into a separate control. [ISM-0247, ISM-1137, ISM-1885]

The existing control relating to conducting emanation security threat assessments for OFFICIAL: Sensitive or PROTECTED systems that are co-located with SECRET or TOP SECRET systems was amended to clarify the requirement is only applicable when the systems are located within 20 meters of each other. [ISM-0248]

The existing control relating to conducting emanation security threat assessments for systems in military platforms, or when deployed overseas, was amended to clarify the requirement is applicable to SECRET or TOP SECRET systems in mobile platforms or that exist as a deployable capability. [ISM-0249]

The existing control relating to seeking emanation security threat assessments as early as possible in a system's life cycle was reworded. [ISM-0246]

Guidelines for Communications Systems

Logging multifunction device use

The existing control relating to the centralised storage of multifunction device (MFD) event logs was merged into the existing control relating to collecting MFD event logs. [ISM-1855, ISM-1856]

Guidelines for Enterprise Mobility

Maintaining mobile device security

A new control recommending mobile devices be operated in a supervised (or equivalent) mode was added. [ISM-1886]

A new control recommending mobile devices be configured with remote locate and wipe functionality was added. [ISM-1887]

A new control recommending mobile devices be configured with a secure lock screen was added. [ISM-1888]

The existing control relating to preventing personnel from installing or uninstalling non-approved applications was corrected to recommend that personnel be prevented from installing non-approved applications. [ISM-0863]

Before travelling overseas with mobile devices

The existing control relating to hardening mobile devices before overseas travel was amended to split out recommendations to configure remote locate and wipe functionality, as well as secure lock screens, as such measures are applicable to everyday use of mobile devices. [ISM-1555]

Guidelines for ICT Equipment

Hardening ICT equipment configurations

The existing control relating to ICT equipment being hardened using ASD and vendor hardening guidance was amended to recommend that the most restrictive guidance take precedence when conflicts occur. [ISM-1858]

Guidelines for System Hardening

Hardening operating system configurations

The existing control relating to operating systems being hardened using ASD and vendor hardening guidance was amended to recommend that the most restrictive guidance take precedence when conflicts occur. [ISM-1409]

Application control

The existing control relating to implementing Microsoft's 'recommended block rules' was reworded to 'recommended application blocklist'. [ISM-1544]

The existing control relating to implementing Microsoft's 'recommended driver block rules' was reworded to 'vulnerable driver blocklist'. [ISM-1659]

The existing controls relating to allowed and blocked application control events being logged where merged together. [ISM-1660, ISM-1661, ISM-1662]

The existing control relating to the centralised storage of application control event logs was merged into the newly merged control relating to collecting application control event logs. [ISM-1660, ISM-1663]

Command Shell

A new control recommending command line process creation events be centrally logged was added. [ISM-1889]

PowerShell

The existing controls relating to PowerShell event logs being captured and stored centrally were merged into the existing control relating to collecting PowerShell module logging, script block logging and transcription event logs. [ISM-1623, ISM-1664, ISM-1665]

Operating system event logging

The existing control relating to the centralised storage of operating system event logs was merged into the existing control relating to collecting operating system event logs. [ISM-0582, ISM-1747]

Hardening user application configurations

The existing control relating to office productivity suites being hardened using ASD and vendor hardening guidance was amended to recommend that the most restrictive guidance take precedence when conflicts occur. [ISM-1859]

The existing control relating to Internet Explorer 11 being blocked from processing content from the internet was rescinded while leaving the existing recommendation that it be disabled or removed. [ISM-1666]

The existing control relating to web browsers being hardened using ASD and vendor hardening guidance was amended to recommend that the most restrictive guidance take precedence when conflicts occur. [ISM-1412]

The existing control relating to Portable Document Format (PDF) software being hardened using ASD and vendor hardening guidance was amended to recommend that the most restrictive guidance take precedence when conflicts occur. [ISM-1860]

Microsoft Office macros

A new control recommending Microsoft Office macros be checked to ensure they are free of malicious code before being digitally signed or placed within Trust Locations was added. [ISM-1890]

The existing control relating to only privileged users responsible for checking that Microsoft Office macros are free of malicious code being able to write to and modify content within Trusted Locations was reworded. [ISM-1487]

A new control recommending Microsoft Office macros digitally signed by signatures other than V3 signatures be prevented from being enabled via the Message Bar or Backstage View was added. [ISM-1891]

The existing control relating to the centralised storage of macro execution event logs was merged into the existing control relating to collecting macro execution event logs. [ISM-1677, ISM-1678]

Hardening server application configurations

The existing control relating to server applications being hardened using ASD and vendor hardening guidance was amended to recommend that the most restrictive guidance take precedence when conflicts occur. [ISM-1246]

Microsoft Active Directory Domain Services domain controllers

The existing control relating to the centralised storage of security-related events for Microsoft Active Directory Domain Services (AD DS) was merged into the existing control relating to collecting security-related events for Microsoft AD DS. [ISM-1830, ISM-1831]

Multi-factor authentication

The existing control relating to multi-factor authentication being used to authenticate users to their organisation's online services was amended to clarify that it relates to their organisation's online services that process, store or communicate their organisation's sensitive data. [ISM-1504]

A new control recommending multi-factor authentication be used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data was added. [ISM-1892]

A new control recommending multi-factor authentication be used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data was added. [ISM-1893]

The existing control relating to multi-factor authentication being used to authenticate users to online customer services, but users being able to opt out, was amended to remove the opt out clause. This control was also reworded to reference customers authenticating to such services in order to access their own sensitive customer data. [ISM-1681]

The existing control relating to multi-factor authentication being used to authenticate users to important data repositories was expanded to all data repositories. [ISM-1505]

The existing control relating to phishing-resistant multi-factor authentication being used for online services was amended to reflect that it relates to users (but not customers). [ISM-1872]

The existing controls relating to phishing-resistant multi-factor authentication being used for online customer services were amended to reflect that they relate to customers (but not users). [ISM-1873, ISM-1874]

The existing control relating to phishing-resistant multi-factor authentication being used for systems was amended to reflect that it relates to users (but not customers). [ISM-1682]

A new control recommending multi-factor authentication used for authenticating users of data repositories be phishing-resistant was added. [ISM-1894]

The existing control relating to the centralised storage of multi-factor authentication event logs was merged into the existing control relating to collecting multi-factor authentication event logs. [ISM-1683, ISM-1684]

Single-factor authentication

A new control recommending successful and unsuccessful single-factor authentication events be centrally logged was added. [ISM-1895]

Protecting credentials

A new control recommending the use of memory integrity functionality in Microsoft Windows was added. [ISM-1896]

The existing control relating to the use of Protective Process Light for the Local Security Authority Subsystem Service in Microsoft Windows was reworded to refer to Local Security Authority protection functionality instead. [ISM-1861]

The existing control relating to Credential Guard and Remote Credential Guard in Microsoft Windows was reworded and split into two separate controls. [ISM-1686, ISM-1897]

Guidelines for System Management

Separate privileged operating environments

A new control recommending the use of Secure Admin Workstations for the performance of administrative activities was added. [ISM-1898]

Administrative infrastructure

The existing control relating to only privileged operating environments being able to communicate with jump servers, along with the existing control relating to only jump servers being able to communicate with assets requiring remote administration, were replaced with a new control recommending network devices that do not belong to administrative infrastructure be prevented from initiating connections with administrative infrastructure. [ISM-1381, ISM-1388, ISM-1899]

Scanning for missing patches or updates

The existing control relating to conducting vulnerability scanning to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices was relaxed from weekly scanning to fortnightly scanning. [ISM-1702]

The existing control relating to conducting vulnerability scanning to identify missing patches or updates for vulnerabilities in operating systems of ICT equipment other than workstations, servers and network devices was relaxed from weekly scanning to fortnightly scanning. [ISM-1752]

The existing control relating to conducting vulnerability scanning to identify missing patches or updates for vulnerabilities in drivers and firmware was relaxed from weekly scanning to fortnightly scanning and split into two separate controls. [ISM-1703, ISM-1900]

When to patch vulnerabilities

The existing control relating to applying patches, updates or other vendor mitigations for vulnerabilities in online services within two weeks of release was amended to note that this relates to situations where vulnerabilities are assessed as non-critical by vendors and no working exploits exist. [ISM-1690]

A new control recommending patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products be applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist was added. [ISM-1901]

The existing control relating to applying patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices within two weeks of release was amended to note that this relates to situations where vulnerabilities are assessed as non-critical by vendors and no working exploits exist. [ISM-1694]

The existing control relating to applying patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices was relaxed from within two weeks of release to within one month of release. [ISM-1695]

A new control recommending patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices be applied within one month of release where vulnerabilities are assessed as non-critical by vendors and no working exploits exist was added. [ISM-1902]

The existing control relating to applying patches, updates or other vendor mitigations for vulnerabilities in operating systems of ICT equipment other than workstations, servers and network devices within two weeks of release was relaxed to within one month of release. Furthermore, this control was amended to note that this relates to situations where vulnerabilities are assessed as non-critical by vendors and no working exploits exist. [ISM-1751]

The existing control relating to applying patches, updates or other vendor mitigations for vulnerabilities in drivers and firmware within 48 hours where vulnerabilities are assessed as critical by vendors or when working exploits exist was split into two separate controls. [ISM-1879, ISM-1903]

The existing control relating to applying patches, updates or other vendor mitigations for vulnerabilities in drivers and firmware within two weeks of release was relaxed to within one month of release and split into two separate controls. Furthermore, the controls were amended to note that this relates to situations where vulnerabilities are assessed as non-critical by vendors and no working exploits exist. [ISM-1697, ISM-1904]

Cessation of support

The existing control relating to removing online services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors was split into two separate controls to separate online services from desktop applications. [ISM-1704, ISM-1905]

The existing control relating to removing applications that are no longer supported by vendors was amended to address applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products. [ISM-0304]

Performing and retaining backups

The existing control relating to performing backups of data, applications and settings with a frequency and retention timeframe in accordance with business continuity requirements was amended to reflect that the business criticality of data and applications should also be considered. [ISM-1511]

The existing control relating to synchronising backups of data, applications and settings was reworded. [ISM-1810]

The existing control relating to storing backups of data, applications and settings in a secure and resilient manner was reworded. [ISM-1811]

Backup modification and deletion

The existing control relating to backup administrator accounts being prevented from modifying and deleting backups during their retention period was reworded. [ISM-1708]

Testing restoration of backups

The existing control relating to testing restoration of data, applications and settings was reworded. [ISM-1515]

Guidelines for System Monitoring

Centralised event logging facility

The existing control relating to protecting event logs from unauthorised modification and deletion was reworded. [ISM-1815]

Event log monitoring

A new control recommending event logs from internet-facing servers be analysed in a timely manner to detect cyber security events was added. [ISM-1906]

A new control recommending event logs from non-internet-facing servers be analysed in a timely manner to detect cyber security events was added. [ISM-1907]

The existing control relating to analysing event logs in a timely manner to detect cyber security events was scoped to event logs from workstations. [ISM-0109]

Guidelines for Software Development

Reporting and resolving vulnerabilities

A new control recommending vulnerabilities identified in applications be publicly disclosed (where appropriate to do so) by software developers in a timely manner was added. [ISM-1908]

A new control recommending that when software developers are resolving vulnerabilities they perform root cause analysis and to the greatest extent possible seek to remediate entire vulnerability classes was added. [ISM-1909]

Web application programming interfaces

A new control recommending event logs relating to specific web application programming interface calls be collected and centrally logged was added. [ISM-1910]

Web application interaction with databases

The existing control relating to the use of parameterised queries or stored procedures instead of dynamically generated queries was reworded. [ISM-1276]

The existing control relating to the centralised storage of web application event logs was merged into the existing control relating to collecting database-related web application event logs. [ISM-1536, ISM-1757]

Web application event logging

A new control recommending event logs relating to crashes and error messages for web applications be collected and centrally logged was added. [ISM-1911]

Guidelines for Databases

Database event logging

The existing control relating to the centralised storage of database event logs was merged into the existing control relating to collecting database event logs. [ISM-1537, ISM-1758]

Guidelines for Networking

Network documentation

The existing control on developing, implementing and maintaining network documentation was reworded. [ISM-0518]

A new control recommending network documentation include device settings for all critical servers, high-value servers, network devices and network security appliances was added. [ISM-1912]

Default settings

The existing control relating to hardening settings for wireless access points was reworded. [ISM-1710]

Guidelines for Gateways

System administration of gateways

The existing control relating to system administration activities for gateways between networks belonging to different security domains was reworded. [ISM-0629]

Gateway event logging

The existing control relating to the centralised storage of gateway event logs was merged into the existing control relating to collecting gateway event logs. [ISM-0634, ISM-1775]

Cross Domain Solution event logging

The existing control relating to the centralised storage of Cross Domain Solution event logs was merged into the existing control relating to collecting Cross Domain Solution event logs. [ISM-0670, ISM-1776]

Web proxy event logging

The existing control relating to the centralised storage of web proxy event logs was merged into the existing control relating to collecting web proxy event logs. [ISM-0261, ISM-1777]

Various guidelines

Essential Eight mapping

A number of existing controls had their Essential Eight mapping updated to reflect the latest release of the *Essential Eight Maturity Model*. A mapping to Maturity Level One requirements was also added. [ISM-0123, ISM-0140, ISM-0445, ISM-0843, ISM-0974, ISM-1175, ISM-1228, ISM-1380, ISM-1401, ISM-1405, ISM-1485, ISM-1486, ISM-1488, ISM-1489, ISM-1501, ISM-1504, ISM-1507, ISM-1511, ISM-1515, ISM-1544, ISM-1582, ISM-1585, ISM-1623, ISM-1654, ISM-1657, ISM-1671, ISM-1672, ISM-1677, ISM-1679, ISM-1680, ISM-1681, ISM-1682, ISM-1688, ISM-1689, ISM-1690, ISM-1691, ISM-1694, ISM-1695, ISM-1697, ISM-1698, ISM-1699, ISM-1701, ISM-1702, ISM-1703, ISM-1704, ISM-1807, ISM-1808, ISM-1810, ISM-1811, ISM-1812, ISM-1814, ISM-1815, ISM-1819, ISM-1861, ISM-1870, ISM-1872, ISM-1873, ISM-1876, ISM-1877, ISM-1879]

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).