



Information Security Manual: September 2022 Changes

Published: 15 September 2022

Summary of content changes

Changes for the September 2022 update of the [Information Security Manual](#) (ISM) are covered below.

Guidelines for Cyber Security Incidents

Incident management policy

Language associated with 'intrusion detection and prevention policy' was amended to 'incident management policy' (ISM-0576).

A new control was added covering exercising the incident management policy, including the associated incident response plan, at least annually (ISM-1784).

Guidelines for Procurement and Outsourcing

Cyber supply chain risk management

The cyber supply chain risk management recommendations covering components and services were amended to applications, ICT equipment and services (ISM-1452, ISM-1568, ISM-1631 and ISM-1632).

Language associated with 'suppliers and service providers' was amended to 'suppliers' noting that suppliers have now been defined within the glossary as encompassing application developers, ICT equipment manufacturers, service providers and other organisations involved in distribution channels (ISM-1452, ISM-1567, ISM-1632 and ISM-1569).

Language associated with cyber supply chain risk assessments for applications, ICT equipment and services 'relevant to the security of systems' was amended to 'associated with systems' noting that every part of a system can potentially impact its security risk profile (ISM-1452, ISM-1568, ISM-1631 and ISM-1632).

Supplier relationship management

A new control was added covering the development and implementation of a supplier relationship management policy (ISM-1785).

A new control was added covering the development and implementation of an approved supplier list (ISM-1786).

Purchasing of applications, ICT equipment and services

A new control was added covering purchasing applications, ICT equipment and services from approved suppliers (ISM-1787).

A new control was added covering identifying multiple potential suppliers for critical applications, ICT equipment and services (ISM-1788).

A new control was added covering purchasing and keeping in reserve sufficient spares of critical ICT equipment (ISM-1789).

Delivery of applications, ICT equipment and services

A new control was added covering maintaining the integrity of the delivery of applications, ICT equipment and services (ISM-1790).

A new control was added covering determining the integrity of applications, ICT equipment and services as part of acceptance of products and services (ISM-1791).

A new control was added covering determining the authenticity of applications, ICT equipment and services as part of acceptance of products and services (ISM-1792).

Managed service and cloud service registers

Existing controls were modified to ensure similar information is being recorded within managed service registers and cloud service registers. In addition, a new requirement was added to existing controls to ensure that copies of contractual arrangements for managed services and cloud services are kept with associated registers (ISM-1638 and ISM-1737).

The existing control recommending 24/7 contact details be recorded for managed services and cloud services (ISM-1433) was merged into existing controls for managed service registers and cloud service registers (ISM-1638 and ISM-1737).

Assessment of managed service providers

A new control was added covering managed service providers and their managed services being assessed by Infosec Registered Assessor Program (IRAP) assessors – as per recent changes to Policy 11 of the Attorney-General's Department's [Protective Security Policy Framework](#) (PSPF) (ISM-1793). The assessment timeframe for this control was set to 'at least every 24 months' to mirror recommendations for outsourced cloud service providers (ISM-1570).

Contractual security requirements

The existing control recommending that security requirements be documented in contractual arrangements with service providers was extended to recommend that such requirements be reviewed on a regular and ongoing basis to ensure they remain fit for purpose (ISM-0072).

The existing control recommending that service providers notify their customers of cyber security incidents was extended to recommend that such requirements be documented in contractual arrangements (ISM-0141).

A new control was added covering documenting in contractual arrangements a requirement for service providers to notify their customers of significant changes to their own service provider arrangements (ISM-1794).

Guidelines for Enterprise Mobility

Approval for Use

Language associated with 'approved for use by the ACSC' was amended to 'approved for use by ASD' noting that ASD issues 'approval for use' for cryptographic equipment (ISM-0687).

Use of mobile devices

The language for existing controls covering the use of privately-owned mobile devices and organisation-owned mobile devices was amended to ensure consistency, noting recommendations for securing their use have not changed (ISM-1400 and ISM-1482).

Guidelines for System Hardening

Protecting credentials

A new control was added covering minimum credential lengths (30 characters) for local administrator accounts and service accounts (ISM-1795).

Regularly restarting workstations

The existing control covering restarting workstations outside of business hours, after a suitable period of inactivity, was amended to clarify that this should be occurring on a daily basis (ISM-0853).

Guidelines for Software Development

Software supply chain security

A new control was added covering software developers digitally signing files containing executable content as part of application development (ISM-1796).

A new control was added covering software developers digitally signing or providing cryptographic checksums for installers, patches and updates as part of application development (ISM-1797).

A new control was added covering software developers providing secure configuration guidance for their applications (ISM-1798).

Guidelines for Email

Email subdomains

Existing controls covering 'domains' were amended to 'domains (including subdomains)' to avoid confusion as to whether subdomains were in scope or out of scope for these controls (ISM-0567, ISM-0574, ISM-0861, ISM-1183, ISM-1502 and ISM-1540).

Email server transport encryption

The existing control covering the use of MTA-STS was reworded to clarify that MTA-STS is used for 'preventing the unencrypted transfer of emails' rather than 'preventing the transfer of unencrypted emails' (ISM-1589).

Domain-based Message Authentication, Reporting and Conformance

The existing SPF control recommending that incoming emails that fail SPF checks be blocked or marked in a manner that is visible to recipients (ISM-1152) was replaced by a new DMARC control covering incoming emails being rejected if they do not pass DMARC checks (ISM-1799).

Guidelines for Networking

Flashing network devices with trusted firmware before first use

A new control was added covering flashing network devices with trusted firmware before first use (ISM-1800).

Regularly restarting network devices

A new control was added covering restarting network devices on at least a monthly basis (ISM-1801).

Guidelines for Cryptography

ASD-approved High Assurance Cryptographic Equipment

Language associated with 'High Assurance Cryptographic Equipment' was amended to 'ASD-approved High Assurance Cryptographic Equipment' noting that ASD is the sole authority for approving of cryptographic equipment as High Assurance Cryptographic Equipment (ISM-0460, ISM-0467 and ISM-0499).

A new control was added covering ASD approval for the use of High Assurance Cryptographic Equipment (ISM-1802).

Contact details

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