



Information Security Manual: December 2022 Changes

Published: 01 December 2022

Summary of content changes

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

Guidelines for Cyber Security Roles

Developing a cyber security communications strategy

The existing control relating to the development and maintenance of a cyber security communications strategy was amended to ensure it is implemented [ISM-0720].

Overseeing cyber security awareness raising

The existing control relating to overseeing the development and operation of a cyber security awareness raising program was amended to ensure it is also maintained [ISM-0735].

Guidelines for Cyber Security Incidents

Incident management policy

The existing control relating to the development and implementation of an incident management policy was amended to include the development and implementation of an associated incident response plan [ISM-0576].

Cyber security incident register

The existing control relating to cyber security incident registers, including their contents, was separated into two controls [ISM-0125, ISM-1803].

Trusted insider program

The existing control relating to the development and implementation of a trusted insider program was amended to ensure it is also maintained [ISM-1625].

Guidelines for Procurement and Outsourcing

Cyber supply chain risk management activities

The existing control relating to identifying and understanding all applications, ICT equipment and services associated with systems was amended to focus on identifying the suppliers of applications, ICT equipment and services associated with systems [ISM-1631].

Sourcing applications, ICT equipment and services

Language from existing controls relating to ‘purchasing’ was amended to ‘sourcing’ to avoid unintentionally excluding applications, ICT equipment and services that isn’t purchased (e.g. open source software) [ISM-1787, ISM-1788, ISM-1789].

Contractual security requirements with service providers

Language from existing controls relating to ‘contractual arrangements’ was amended to ‘contractual arrangements with service providers’ [ISM-0072, ISM-0141, ISM-1451, ISM-1571, ISM-1572, ISM-1573, ISM-1574, ISM-1757, ISM-1738, ISM-1794].

An existing control relating to service providers providing an appropriate level of protection for any data entrusted to them or their services was amended to capture subcontractors used by service providers [ISM-1395].

A new control was added covering the inclusion of a break clause in contractual arrangements with service providers where service providers, or any subcontractors, are unable to meet security requirements [ISM-1804].

The existing control relating to service providers providing notification of significant changes to their own service provider arrangements was amended to ensure a minimum notification period of one month is provided to customers [ISM-1794].

Guidelines for Communications Infrastructure

Denial of service response plan

The existing control relating to denial of service response plans for video conferencing and IP telephony, including their contents, was separated into two controls [ISM-1019, ISM-1805].

Guidelines for Enterprise Mobility

After travelling overseas with mobile devices

Existing controls relating to the handling of credentials following travelling overseas with mobile devices were amended to align with language used by controls within the authentication hardening section of the [Guidelines for System Hardening](#) [ISM-1300, ISM-1556].

Guidelines for System Hardening

Operating system releases and versions

Language from existing controls relating to operating systems was amended to clarify intent [ISM-1407]. This included the rescinding of one control that was no longer required [ISM-1744].

Language from an existing control relating to the use of 64-bit operating systems was simplified to align with similar controls for operating systems [ISM-1408].

Hardening operating system configurations

The existing control relating to changing default credentials for operating systems was amended to changing default accounts or credentials for operating systems [ISM-0383].

Hardening application configurations

A new control was added covering changing default accounts or credentials for applications [ISM-1806].

Setting credentials for user accounts

The existing control relating to passphrases not being reused for single-factor authentication across different systems was expanded to cover all memorised secrets, including when used as part of multi-factor authentication [ISM-1596].

Protecting credentials

The existing control relating to local administrator and service accounts using unique, unpredictable and managed credentials was expanded to ensure they are also long [ISM-1685].

The existing control relating to storing physical credentials separately from systems that they are used to authenticate to was reworded to remove confusing 'physical credential' language and clarify that 'devices that store or generate credentials' can still be connected to systems when performing authentication activities [ISM-0418].

Session and screen locking

Language from an existing control relating to session and screen locking was amended to ensure consistency with similar authentication-related controls [ISM-0428].

Guidelines for System Management

Scanning for missing patches or updates

A new control was added covering the use of an automated method of asset discovery to support vulnerability scanning activities [ISM-1807].

A new control was added covering the use of up-to-date vulnerability databases by vulnerability scanners [ISM-1808].

Cessation of support

A new control was added covering the use of compensating controls when unsupported applications, operating systems, network devices or other ICT equipment cannot be immediately removed or replaced [ISM-1809].

Performing and retaining backups

Backup retention language associated with an existing control was amended to provide clarity of intent [ISM-1511]. This included the introduction of two new controls [ISM-1810, ISM-1811].

Backup access

Backup access language associated with existing controls was amended to provide clarity of intent [ISM-1705, ISM-1706]. This included the introduction of two new controls [ISM-1812, ISM-1813].

Backup modification and deletion

Backup modification and deletion language associated with existing controls was amended to provide clarity of intent [ISM-1707, ISM-1708]. This included the introduction of a new control [ISM-1814].

Testing restoration of backups

Backup testing language associated with an existing control was amended to provide clarity of intent [ISM-1515].

Guidelines for System Monitoring

Centralised event logging facility

Centralised event logging language associated with an existing control was amended to provide clarity of intent [ISM-1405]. This included the introduction of a new control [ISM-1815].

Guidelines for Software Development

Development, testing and production environments

A new control was added covering the prevention of unauthorised modifications to authoritative sources for software [ISM-1816].

Web application programming interfaces

A new control was added to ensure clients are authenticated when calling web application programming interfaces that facilitate access to data not authorised for release into the public domain [ISM-1817].

A new control was added to ensure clients are authenticated when calling web application programming interfaces that facilitate modification of data [ISM-1818].

Guidelines for Email

Email content filtering

Language from an existing control relating to content filtering was amended to ensure that controls for email content filtering and web content filtering are aligned [ISM-1234].

Guidelines for Networking

Use of Simple Network Management Protocol

Language from an existing control relating to the use of 'SNMP version 1 and 2' was amended to 'SNMP version 1 and SNMP version 2' [ISM-1311].

Protective Domain Name System Services

Language from an existing control relating to the use of protective Domain Name System (DNS) services was amended to include the intended purpose of using a protective DNS service [ISM-1782].

Default accounts and credentials for network devices

Language from an existing control relating to default accounts and credentials for network devices was amended to mirror similar language for controls relating to operating systems and applications [ISM-1304].

Default settings (for wireless access points)

The existing control on changing default accounts and credentials for wireless access points was rescinded as it was a subset of the control covering changing default accounts or credentials for network devices [ISM-1709].

Guidelines for Gateways

Web content filtering

Language from an existing control relating to content filtering was amended to ensure that controls for email content filtering and web content filtering are aligned [ISM-0963].

Guidelines for Data Transfers

Manual import of data

The existing control on the use of data formatting checks for manual import of data to systems was rescinded [ISM-0658].

Manual export of data

The existing control on security checks before manual export of data from systems was amended to remove the requirement for data format checks [ISM-0669].

Cyber Security Terminology

Definition of ICT equipment

The definition of ICT equipment was amended to explicitly state that ‘smart devices’ are considered ICT equipment and therefore all controls relating to ICT equipment equally apply to smart devices, such as smart televisions and smart fridges.

Various guidelines

Development, implementation and maintenance of documents, registers and diagrams

Existing controls relating to the development and implementation of cyber security documentation were amended to ensure documentation is maintained throughout its lifetime [ISM-0039, ISM-0042, ISM-0206, ISM-0258, ISM-0264, ISM-0313, ISM-0348, ISM-0363, ISM-0374, ISM-0507, ISM-0576, ISM-0580, ISM-0588, ISM-0663, ISM-0701, ISM-1019, ISM-1078, ISM-1082, ISM-1143, ISM-1359, ISM-1510, ISM-1533, ISM-1535, ISM-1547, ISM-1548, ISM-1549, ISM-1550, ISM-1551, ISM-1741, ISM-1755, ISM-1756, ISM-1785, ISM-1786].

Existing controls relating to the maintenance of registers were amended to ensure registers are developed and implemented in the first instance [ISM-0125, ISM-0211, ISM-0336, ISM-0518, ISM-1243, ISM-1493, ISM-1543, ISM-1637, ISM-1713, ISM-1736].

Existing control relating to the maintenance of diagrams was amended to ensure diagrams are developed and implemented in the first instance [ISM-1645].

Consolidation of event logging guidance

Existing controls relating to event logging were amended to increase clarity of intent and to reduce duplication of content. As a result, common guidance was consolidated into the event logging and monitoring section of the [Guidelines for System Monitoring](#) [ISM-1509, ISM-1650, ISM-1651, ISM-1652, ISM-1660, ISM-1661, ISM-1662, ISM-1663, ISM-1664, ISM-1665, ISM-1677, ISM-1678, ISM-1683, ISM-1684, ISM-1714, ISM-1715, ISM-1747, ISM-1757, ISM-1758, ISM-1775, ISM-1776, ISM-1777].

Contact details

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