Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

# Information Security Manual: June 2023 Changes

**Published:** 22 June 2023

## Summary of content changes

Changes to controls for the June 2023 update of the *Information Security Manual* (ISM) are covered below.

### Guidelines for Cyber Security Incidents

#### Reporting cyber security incidents

A minor grammatical change was made to the existing control relating to the reporting of cyber security incidents within an organisation. [ISM-0123]

#### Reporting cyber security incidents to the ACSC

The existing control relating to the reporting of cyber security incidents to the Australian Cyber Security Centre (ACSC) was amended to recommend that this should occur as soon as possible after they occur or are discovered. This allows the ACSC to work with an organisation to determine the extent of any assistance they may require in responding to the cyber security incident. [ISM-0140]

### Guidelines for Procurement and Outsourcing

#### Contractual security requirements with service providers

The existing control relating to the regions or availability zones where an organisation's data will be processed, stored and communicated being documented in contractual arrangements with service providers was amended to include minimum notification periods for any configuration changes to those regions or availability zones. [ISM-1572]

### Guidelines for Security Documentation

#### Continuous monitoring plan

The existing control relating to the development of a continuous monitoring plan for systems was amended to reflect that vulnerability scanning activities for systems should be undertaken at least fortnightly, as per the *Essential Eight Maturity Model*, and that both vulnerability assessments and penetration tests should be undertaken prior to the deployment of systems, including prior to the deployment of significant changes, as per control ISM-0911 which was previously partly merged into control ISM-1163. [ISM-1163]

# Guidelines for Personnel Security

### Unprivileged access to systems

A new control was added covering unprivileged access to systems, applications and data repositories being limited to only what is required for users and services to undertake their duties. [ISM-1852]

### Privileged access to systems

A new control was added covering privileged access to data repositories being limited to only what is required for users and services to undertake their duties. [ISM-1853]

# Guidelines for Communications Systems

### Authenticating to multifunction devices

A new control was added covering users authenticating to multifunction devices (MFDs) before they can print, scan or copy documents. [ISM-1854]

The existing control relating to ensuring that controls for MFDs connected to networks being of a similar strength to other devices was amended to clarify that it related to user authentication. For example, if multi-factor authentication is implemented for workstations on a network, it should also be implemented for MFDs. [ISM-0590]

### Scanning and copying documents on multifunction devices

The existing control relating to not copying documents above the sensitivity or classification of the network that MFDs are connected to was amended to cover both scanning and copying documents. This reflects that while copying a document may cause a localised data spill, scanning a document will cause a wider ranging data spill on the network. [ISM-0589]

### Auditing multifunction device use

A new control was added covering the logging of MFD use (e.g. by capturing metadata and shadow copies) for printing, scanning and copying. This can assist in monitoring for inappropriate MFD use as well as detecting malicious insiders. [ISM-1855]

A new control was added covering the centralised storage of event logs associated with MFD use. [ISM-1856]

# Guidelines for Evaluated Products

### Using evaluated products

The existing control relating to ‘evaluated products being installed, configured, administered and operated in accordance with vendor guidance and evaluation documentation’ was amended to ‘evaluated products being installed, configured, administered and operated in an evaluated configuration and in accordance with vendor guidance’. [ISM-0289]

The existing control relating to ‘high assurance ICT equipment being installed, configured, administered and operated in accordance with guidance produced by the ACSC’ was amended to ‘high assurance ICT equipment being installed, configured, administered and operated in an evaluated configuration and in accordance with ACSC guidance’. [ISM-0290]

The existing control relating to operating high assurance ICT equipment in an evaluated configuration was merged into control ISM-0290. [ISM-0292]

## Guidelines for ICT Equipment

### Selecting ICT equipment

A new control was added covering the selection of ICT equipment from vendors that have demonstrated a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products. [ISM-1857]

### Hardening ICT equipment configurations

A new control was added covering the implementation of ACSC and vendor hardening guidance for ICT equipment. [ISM-1858]

## Guidelines for System Hardening

### Hardening operating system configurations

A minor grammatical change was made to an existing control relating to applying ACSC and vendor hardening guidance for operating systems. [ISM-1409]

### Hardening user application configurations

The existing control relating to ACSC or vendor hardening guidance being implemented for web browsers, Microsoft Office and PDF software was split into three separate controls to facilitate independent implementation and assessment in accordance with the *Essential Eight Maturity Model*. [ISM-1412, ISM-1859, ISM-1860]

### Hardening server application configurations

The existing control relating to 'ACSC or vendor hardening guidance being implemented for server applications' was amended to 'ACSC and vendor hardening guidance being implemented for server applications' in order to match the approach recommended for operating systems within control ISM-1409. [ISM-1246]

### Multi-factor authentication

A minor grammatical change was made to an existing control relating to multi-factor authentication being enabled by default for an organisation's non-organisational users if they authenticate to the organisation's internet-facing services. [ISM-1681]

### Setting credentials for break glass accounts, local administrator accounts and service accounts

The existing control relating to ensuring that local administrator accounts and service accounts are long, unique, unpredictable and managed was amended to include break glass accounts. [ISM-1685]

The existing control related to ensuring that credentials for local administrator accounts and service accounts are a minimum of 30 characters was amended to include break glass accounts. [ISM-1795]

### Changing credentials

A minor change was made to the existing control covering scenarios for when to change credentials in order to remove duplication of content. [ISM-1590]

### Protecting credentials

A new control was added covering the enablement of Protective Process Light for the Local Security Authority Subsystem Service (LSASS), with a Unified Extensible Firmware Interface (UEFI) lock, on Microsoft Windows devices in order to protect against credential dumping attacks. [ISM-1861]

### Account lockouts

The existing control relating to locking out accounts after a maximum of five failed logon attempts was amended to exclude break glass accounts. [ISM-1403]

## Guidelines for System Management

### Administrative infrastructure

The existing control relating to 'segregating administrative infrastructure from the wider network' was amended to 'segregating administrative infrastructure from the wider network and the internet'. [ISM-1385]

### Scanning for missing patches or updates

The existing control relating to 'scanning for missing patches or updates in other applications' was amended to 'scanning for missing patches or updates in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products' to avoid confusion when the control is read in isolation. [ISM-1700]

The existing control relating to 'scanning for missing patches or updates in operating systems of other ICT equipment' was amended to 'scanning for missing patches or updates in operating systems of ICT equipment other than workstations, servers and network devices' to avoid confusion when the control is read in isolation. [ISM-1752]

### When to patch security vulnerabilities

The existing control relating to 'applying patches, updates or vendor mitigations for security vulnerabilities in other applications' was amended to 'applying patches, updates or vendor mitigations for security vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products' to avoid confusion when the control is read in isolation. [ISM-1693]

The existing control relating to 'applying patches, updates or vendor mitigations for security vulnerabilities in operating systems of other ICT equipment' was amended to 'applying patches, updates or vendor mitigations for security vulnerabilities in operating systems of ICT equipment other than workstations, servers and network devices' to avoid confusion when the control is read in isolation. [ISM-1751]

## Guidelines for Software Development

### Web application firewalls

A new control was added covering both avoiding the disclosure of Internet Protocol addresses of web servers under an organisation's control (referred to as origin servers) when they sit behind a web application firewall, and restricting access to origin servers to only the WAF and authorised management networks. [ISM-1862]

## Guidelines for Emails

### Sender Policy Framework

A minor grammatical change was made to the existing control relating to Sender Policy Framework (SPF) being used to specify authorised email servers (or lack thereof) for an organisation's domains (including subdomains). [ISM-0574]

A minor grammatical change was made to the existing control relating to a hard fail SPF record being used when specifying authorised email servers (or lack thereof) for an organisation's domains (including subdomains). [ISM-1183]

### DomainKeys Identified Mail

A minor grammatical change was made to the existing control relating to the verification of DomainKeys Identified Mail (DKIM) signatures on incoming emails. [ISM-1026]

### Domain-based Message Authentication, Reporting and Conformance

A minor grammatical change was made to the existing control relating to Domain-based Message Authentication, Reporting and Conformance (DMARC) records being configured for an organisation's domains (including subdomains) such that emails are rejected if they do not pass DMARC checks. [ISM-1540]

## Guidelines for Networking

### Networked management interfaces

A new control was added covering the avoidance of directly exposing networked management interfaces for ICT equipment residing on networks (such as servers), or constituting the makeup of network infrastructure (such as network devices), to the internet. [ISM-1863]

### Location policies for online services

The existing control relating to minimum notification periods for changes to regions or availability zones for online services was merged into control ISM-1572 within the *Guidelines for Procurement and Outsourcing*. [ISM-1578]

### Capacity and availability planning and monitoring for online services

The existing control relating to testing cloud service providers' ability to dynamically scale resources due to a genuine spike in demand or a denial-of-service attack was amended to recommend discussing and verifying cloud service providers' ability to dynamically scale resources in response to a genuine spike in demand – noting discussions on their capacity to withstand denial-of-service attacks, and any testing with the prior express consent of cloud service providers, is covered by control ISM-1431. [ISM-1579]

The existing control relating to using a denial of service mitigation service where a high availability requirement exists for online services was rescinded due to duplication of content with control ISM-1431 which recommends that denial-of-service attack mitigation strategies, and the capacity to withstand a denial-of-service attack, be discussed with cloud service providers. [ISM-1441]

The existing control relating to continuous real-time monitoring of the availability of online services was amended to cover both the capacity and availability of online services in order to match the associated rationale. [ISM-1581]

### Denial-of-service attack mitigation strategies

The existing control relating to determining what functionality and quality of online services can be lived without during a denial-of-service attack was rescinded due to its overlap with control ISM-1431 that calls for denial-of-service attack

mitigation strategies to be discussed with cloud service providers (including thresholds for turning off any online services or functionality, and other pre-approved actions that can be taken, during a denial-of-service attack). [ISM-1458]

The existing control relating to segregation of critical online services from 'other online services that are more likely to be targeted' was amended to 'other online services that are more likely to be targeted as part of a denial-of-service attack'. [ISM-1436]

### Monitoring with real-time alerting for online services

The existing control relating to performing availability monitoring to detect denial-of-service attacks was rescinded due to overlap with control ISM-1431 that recommends denial-of-service attack mitigation strategies be discussed with cloud service providers (including availability monitoring and thresholds for notification of denial-of-service attacks). [ISM-1435]

### Preparing for service continuity

The existing control relating to an organisation pre-preparing their own low-bandwidth static version of their website for when they suffer a denial-of-service attack was rescinded in preference to the organisation discussing denial-of-service attack mitigation strategies with their cloud services providers, as per control ISM-1431. [ISM-1518]

A minor grammatical change was made to the existing control relating to the use of registrar locking and confirming that domain registration details are correct. [ISM-1432]

## Guidelines for Cryptography

### Reporting cryptographic-related cyber security incidents

A minor grammatical change was made to the existing control relating to internal reporting of cryptographic-related cyber security incidents within an organisation. [ISM-0142]

## Guidelines for Data Transfers

### Authorising export of data

A minor grammatical change was made to an existing control relating to the identification of trusted sources for data transfers. [ISM-0665]

# Contact details

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