Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Information Security Manual

Last updated: September 2024

September 2024 Changes

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

Guidelines for Media

Media that cannot be successfully sanitised

The existing control relating to the destruction of faulty or damaged media that cannot be successfully sanitised was amended to clarify that media should also be destroyed when media sanitisation processes repeatedly fail. [ISM-1735]

Guidelines for System Hardening

Operating system event logging

The existing control recommending specific events for operating systems be centrally logged was amended to align with recommendations for the prioritised collection of high-quality event logs within the *Best Practices for Event Logging and Threat Detection* publication and audit event management recommendations within the *Hardening Microsoft Windows 10 and Windows 11* publication. [ISM-0582]

Microsoft Active Directory services

A new control was added recommending that Microsoft Active Directory Domain Services (AD DS) domain controllers, Microsoft Active Directory Certificate Services (AD CS) Certification Authority (CA) servers, Microsoft Active Directory Federation Services (AD FS) servers and Microsoft Entra Connect servers be only used for their designated role and no other applications or services are to be installed, unless they are security related. [ISM-1926]

A new control was added recommending that access to Microsoft AD DS domain controllers, Microsoft AD CS CA servers, Microsoft AD FS servers and Microsoft Entra Connect servers be limited to privileged users that require access. [ISM-1927]

A new control was added recommending that backups of Microsoft AD DS domain controllers, Microsoft AD CS CA servers, Microsoft AD FS servers and Microsoft Entra Connect servers be encrypted, stored securely and only be accessible to backup administrator accounts. [ISM-1928]

The existing control relating to security-relevant events for Microsoft AD DS domain controllers being centrally logged was extended to include security-relevant events for Microsoft AD CS CA servers, Microsoft AD FS servers and Microsoft Entra Connect servers. [ISM-1830]

Microsoft Active Directory Domain Services domain controllers

A new control was added recommending that Lightweight Directory Access Protocol signing be enabled on Microsoft AD DS domain controllers. [ISM-1929]

The existing control relating to 'passwords and cpasswords' not being stored in Group Policy Preferences was amended to simply refer to 'passwords', as this already captures 'cpasswords'. [ISM-1829]

A new control was added recommending that passwords be prevented from being stored in Group Policy Preferences. This requires the application of Microsoft patch 2962486 on some Microsoft AD DS domain controllers. [ISM-1930]

A new control was added recommending that SID Filtering be enabled for domain and forest trusts. [ISM-1931]

Microsoft Active Directory Domain Services account hardening

A new control was added recommending that the number of service accounts configured with a service principal name (SPN) be minimised. [ISM-1932]

A new control was added recommending that service accounts configured with an SPN not have DCSync permissions. [ISM-1933]

The existing control relating to service accounts being provisioned with the minimum privileges required and not being members of the Domain Admins security group, or similar highly-privileged security groups, was split into two separate controls. [ISM-1833, ISM-1940]

A new control was added recommending that user accounts with DCSync permissions be reviewed at least annually, and those without an ongoing requirement for the permissions have them removed. [ISM-1934]

A new control was added recommending that computer accounts not be configured for unconstrained delegation. [ISM-1935]

A new control was added recommending that the sIDHistory attribute for user accounts not be used. [ISM-1936]

A new control was added recommending that user accounts be checked at least weekly for the presence of the sIDHistory attribute. [ISM-1937]

The existing control relating to only dedicated service accounts being allowed to add machines to a domain was amended to clarify this recommendation relates to dedicated privileged service accounts. [ISM-1842]

The existing control relating to user accounts with unconstrained delegation being reviewed at least annually was slightly reworded to ensure consistent use of terminology with other controls. [ISM-1843]

A new control was added recommending that the Domain Computers security group not have write or modify permissions to any Microsoft Active Directory objects. [ISM-1938]

Microsoft Active Directory Domain Services security group memberships

A new control was added recommending that the number of user accounts that are members of the Domain Admins, Enterprise Admins or other highly-privileged security groups be minimised. [ISM-1939]

A new control was added recommending that service accounts not be members of the Domain Admins, Enterprise Admins or other highly-privileged security groups. [ISM-1940]

A new control was added recommending that computer accounts not be members of the Domain Admins, Enterprise Admins or other highly-privileged security groups. [ISM-1941]

A new control was added recommending that the Domain Computers security group not be a member of any privileged or highly-privileged security groups. [ISM-1942]

Microsoft Active Directory Certificate Services

A new control was added recommending that strong mapping between certificates and users be enforced. This requires the application of Microsoft patch 5014754 on some Microsoft AD CS CA servers and Microsoft AD DS domain controllers. [ISM-1943]

A new control was added recommending that the EDITF_ATTRIBUTESUBJECTALTNAME2 flag be removed from Microsoft AD CS CA configurations. [ISM-1944]

A new control was added recommending that the CT_FLAG_ENROLLEE_SUPPLIES_SUBJECT flag be removed from certificate templates. [ISM-1945]

A new control was added recommending that unprivileged user accounts not have write access to certificate templates. [ISM-1946]

A new control was added recommending that Extended Key Usages that enable user authentication be removed. [ISM-1947]

A new control was added recommending that CA Certificate Manager approval be required for certificate templates that allow a Subject Alternative Name to be supplied. [ISM-1948]

Microsoft Active Directory Federation Services

A new control was added recommending that Microsoft AD FS servers be administered using a dedicated service account that is not used to administer other systems. [ISM-1949]

Microsoft Entra Connect

A new control was added recommending that soft matching between Microsoft AD DS and Microsoft Entra ID be disabled following initial synchronisation activities. [ISM-1950]

A new control was added recommending that hard match takeover be disabled for Microsoft Entra Connect servers. [ISM-1951]

A new control was added recommending that privileged user accounts not be synchronised between Microsoft AD DS and Microsoft Entra ID. [ISM-1952]

Single-factor authentication

The existing control relating to passphrase length for single-factor authentication being a minimum length of 14 characters was amended to a minimum length of 15 characters. [ISM-0421]

Setting credentials for built-in Administrator accounts, break glass accounts, local administrator accounts and service accounts

A new control was added recommending that credentials for built-in Administrator accounts be long, unique, unpredictable and managed. [ISM-1953]

The existing control relating to credentials for break glass accounts, local administrator accounts and service accounts being a minimum of 30 characters was expanded to capture the built-in Administrator account in each domain. [ISM-1795]

A new control was added recommending that credentials for built-in Administrator accounts, break glass accounts, local administrator accounts and service accounts be randomly generated. [ISM-1954]

Changing credentials

The existing control relating to changing credentials was amended to clarify that it relates to changing credentials for user accounts. [ISM-1590].

A new control was added recommending that credentials for computer accounts be changed if they are compromised, if they are suspected of being compromised or if they have not been changed in the last 30 days. [ISM-1955]

A new control was added recommending that Microsoft AD FS token-signing and encryption certificates be changed twice in quick succession if they are suspected of being compromised or if they have not been changed in the last 12 months. [ISM-1956]

Protecting credentials

A new control was added recommending that private keys for Microsoft AD CS CA servers be protected by a hardware security module. [ISM-1957]

Guidelines for System Management

Separate privileged operating environments

A new control was added recommending that user accounts with DCSync permissions be prevented from logging onto unprivileged operating environments. [ISM-1958]

Guidelines for System Monitoring

Event log details

A new control was added recommending that, to the extent possible, event logs be captured and stored in a consistent and structured format. [ISM-1959]

A new control was added recommending that event logs from internet-facing network devices be analysed in a timely manner to detect cyber security events. [ISM-1960]

A new control was added recommending that event logs from non-internet-facing network devices be analysed in a timely manner to detect cyber security events. [ISM-1961]

Centralised event logging facility

The existing control relating to establishing and using an accurate and consistent time source for event logging was amended to remove the emphasis on establishing a time source, thereby allowing for any trusted time source to be used as long as it is accurate and consistently used. [ISM-0988]

Guidelines for Software Development

Vulnerability disclosure program

The existing control relating to the use of security.txt files in support of vulnerability disclosure programs was amended from 'all internet-facing organisational domains' to 'each of an organisation's internet-facing website domains'. [ISM-1717]

Guidelines for Database Systems

Database event logging

The existing control recommending specific events for databases be centrally logged was slightly reworded for consistency with similar controls. [ISM-1537]

Guidelines for Networking

Using the Server Message Block protocol

A new control was added recommending that SMB version 1 not be used on networks. [ISM-1962]

Network device event logging

A new control was added recommending that security-relevant events for internet-facing network devices be centrally logged. [ISM-1963]

A new control was added recommending that security-relevant events for non-internet-facing network devices be centrally logged. [ISM-1964]

Guidelines for Gateways

Gateway event logging

The existing control recommending specific events for gateways be centrally logged was slightly reworded for consistency with similar controls. [ISM-0634]

Cross Domain Solution event logging

The existing control recommending specific events for Cross Domain Solutions (CDSs) be centrally logged was slightly reworded for consistency with similar controls. [ISM-0670]

Content checking

A new control was added recommending that files imported or exported via gateways or CDSs undergo content checking, such as keyword checks, metadata checks or protective marking checks, to assist in preventing data spills and unauthorised export of data from systems. [ISM-1965]

Miscellaneous

References to ‘privileged accounts’ were changed to ‘privileged user accounts’ in order to more closely match Microsoft Active Directory account types (i.e. ‘users’ and ‘computers’). Note, the definition of privileged accounts (which referred to such accounts as being a combination of privileged user accounts and privileged service accounts) has been removed. Privileged service accounts are now treated as a subset of privileged user accounts. [ISM-0445, ISM-1175, ISM-1263, ISM-1650, ISM-1689, ISM-1705, ISM-1706, ISM-1707, ISM-1883]

References to ‘unprivileged accounts’ were changed to ‘unprivileged user accounts’ in order to more closely match Microsoft Active Directory account types (i.e. ‘users’ and ‘computers’). Note, the definition of unprivileged accounts (which referred to such accounts as being a combination of unprivileged user accounts and unprivileged service accounts) has been removed. Unprivileged service accounts are now treated as a subset of unprivileged user accounts. [ISM-1688, ISM-1812, ISM-1813, ISM-1814]

A reference to Microsoft Active Directory ‘groups’ was changed to ‘security groups’ in order to more closely match Microsoft Active Directory terminology. [ISM-1650]

A reference to ‘X11 display remoting’ was changed to ‘X11 forwarding’ in order to ensure use of consistent terminology. [ISM-0487]

Contact details

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

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2024.

With the exception of the Coat of Arms, the Australian Signals Directorate logo and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/government/commonwealth-coat-arms).

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate