Australian Government
Australian Signals Directorate

Information Security Manual

Published: 1 March 2024

March 2024 Changes

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

Guidelines for Communications Infrastructure

Applicability

The applicability statement for this section was amended to correct the position that changes in cabling infrastructure controls did not need to be considered when periodically reassessing the security of cabling infrastructure (as required).

Guidelines for Enterprise Mobility

Approved mobile platforms

The existing control relating to the use of mobile platforms that have completed a Common Criteria evaluation against the *Protection Profile for Mobile Device Fundamentals*, version 3.2 or later, was amended to version 3.3 or later. [ISM-1867]

Guidelines for ICT Equipment

Hardening ICT equipment configurations

A new control recommending that approved configurations for ICT equipment be developed, implemented and maintained was added in support of transitioning towards the adoption of zero trust principles. [ISM-1913]

Guidelines for System Hardening

Hardening operating system configurations

A new control recommending that approved configurations for operating systems be developed, implemented and maintained was added in support of transitioning towards the adoption of zero trust principles. [ISM-1914]

Hardening user application configurations

A new control recommending that approved configurations for user applications be developed, implemented and maintained was added in support of transitioning towards the adoption of zero trust principles. [ISM-1915]

Hardening server application configurations

A new control recommending that approved configurations for server applications be developed, implemented and maintained was added in support of transitioning towards the adoption of zero trust principles. [ISM-1916]

Guidelines for Cryptography

Asymmetric/public key algorithms

The existing control relating to the use of Elliptic Curve Diffie-Hellman (ECDH) and the Elliptic Curve Digital Signature Algorithm (ECDSA), in preference to the use of Diffie-Hellman (DH) and the Digital Signature Algorithm (DSA), was amended to remove references to ECDSA and DSA following DSA being withdrawn as an ASD-approved cryptographic algorithm (AACA). [ISM-0994]

Using the Digital Signature Algorithm

The existing controls relating to the use of DSA have been rescinded, as has its status as an AACA, following the recent withdrawal of Federal Information Processing Standard (FIPS) 186-4 by the United States' National Institute of Standards and Technology (NIST). [ISM-0473, ISM-1630, ISM-1760]

Using Elliptic Curve Cryptography

The existing control relating to the use of FIPS 186-4 for the selection of suitable curves for elliptic curve cryptography was amended to reference the replacement NIST Special Publication 800-186. [ISM-1446]

Planning for post-quantum cryptography standards

A new control recommending that future cryptographic requirements and dependencies be considered during the transition to post-quantum cryptographic standards was added. [ISM-1917]

Contact details

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