



Information Security Manual: December 2021 Changes

DECEMBER 2021

Summary of content changes

Changes for the December 2021 update of the [Information Security Manual](#) (ISM) are covered below.

Conducting intrusion remediation activities

To increase the likelihood of intrusion remediation activities successfully removing an adversary from their system, organisations can take preventative measures to ensure the adversary has limited forewarning and awareness of planned intrusion remediation activities. Specifically, using an alternative system to plan and coordinate intrusion remediation activities will prevent alerting the adversary if they have already compromised email, messaging or collaboration services. In addition, conducting intrusion remediation activities in a coordinated manner during the same planned outage will prevent forewarning the adversary, thereby depriving them of sufficient time to establish alternative access points or persistence methods on the system.

New Security Controls	Modified Security Controls	Rescinded Security Controls
1731, 1732		

Secure Internet Gateways

As per the [joint statement](#) between the Digital Transformation Agency and the Australian Signals Directorate (ASD) on the future of Secure Internet Gateways (SIGs), ASD will no longer be conducting re-certification activities for SIGs. This includes ASD staff members conducting joint security assessments with Infosec Registered Assessor Program assessors as part of re-certification activities. Note, currently certified SIGs will remain certified until 1 July 2022.

New Security Controls	Modified Security Controls	Rescinded Security Controls
		0100

Logging and monitoring of unprivileged and break glass access

The terminology used for logging and monitoring both unprivileged access and break glass access has been aligned with the terminology used for logging and monitoring privileged access within the [Essential Eight Maturity Model](#).

New Security Controls	Modified Security Controls	Rescinded Security Controls
1714, 1715	1566, 1613	

Disabling or removing inactive unprivileged accounts

The recommendation to disable or remove access to systems, applications and data repositories for unprivileged users after one month of inactivity has been amended to 45 days to align with the recommendation for privileged users within the [Essential Eight Maturity Model](#).

New Security Controls	Modified Security Controls	Rescinded Security Controls
1716	1404	

Shared facilities

The recommendations for ‘shared government facilities’ and ‘shared non-government facilities’ have been combined into simply ‘shared facilities’.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	0194, 0195, 1112, 1119, 1122, 1123, 1130, 1133, 1137, 1164	0184, 1118, 1126, 1134, 1135

Use of Bluetooth

The recommendation to use at least Bluetooth version 2.1 devices has been amended to using devices that support Secure Connections functionality. This requires either Bluetooth version 4.1 devices (for Bluetooth Classic) or Bluetooth version 4.2 devices (for Bluetooth Low Energy). In addition, the recommendation against using class 1 Bluetooth devices has been removed due to providing only limited protection against Bluetooth attacks.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	1200	1202

Off-site maintenance and repairs

The recommendation to handle ICT equipment as a higher classification, when it comes from an area that is of a higher classification than the ICT equipment, for the purposes of determining requirements for performing off-site repairs was no longer considered practical.

New Security Controls	Modified Security Controls	Rescinded Security Controls
		0944

Software bill of materials

A software bill of materials is a list of open source and commercial software components that are used in the development of software. This can assist in providing greater cyber supply chain transparency for consumers of software by allowing for easier identification and management of security risks associated with individual software components used by the software.

New Security Controls	Modified Security Controls	Rescinded Security Controls
1730		

Responsible disclosure of security vulnerabilities

A recommendation to host a 'security.txt' file for all internet-facing organisational domains has been added to assist in the responsible disclosure of security vulnerabilities to organisations in support of their vulnerability disclosure programs.

New Security Controls	Modified Security Controls	Rescinded Security Controls
1717		

Retirement of 3DES as an ASD Approved Cryptographic Algorithm

In light of ASD's guidance to transition to AES from 3DES (since the 2017 ISM release), [NIST guidance](#) deprecating existing 3DES use and prohibiting its use in new systems and applications, and attacks such as [Sweet32](#) that can reduce 3DES security from 112 bits to 80 bits of effective security strength, ASD has re-assessed the suitability of 3DES for the ongoing protection of up to PROTECTED data. As a result of this assessment, 3DES will be retired as an ASD Approved Cryptographic Algorithm effective immediately.

New Security Controls	Modified Security Controls	Rescinded Security Controls
		0480

Evaluation requirements for cryptographic products

The recommendation that cryptographic products have completed an ASD Cryptographic Evaluation before being used for the protection of data at rest or in transit has been replaced with a recommendation for the use of cryptographic products that have been evaluated and certified under the Common Criteria against a Protection Profile.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	0457, 0465	0157, 1161, 1162, 1464

Miscellaneous changes

Miscellaneous changes were made to rationale and security controls throughout the publication. This included:

- A review from the [Using the Information Security Manual](#) chapter through to the [Guidelines for Media](#) chapter.

- Security controls suitable for all audiences have been identified with the 'All' applicability marking while additional security controls suitable for just government audiences have been identified with the O, P, S and TS applicability markings.
- Security controls suitable for specific classifications have been amended to include their classification(s) in the wording of the security controls to reduce the reliance on applicability markings to confer suitability.
- Tables in security controls have been converted into prose to allow for inclusion in the SSP annex template and the XML list of security controls.
- The use of 'official' and 'highly classified' terminology has been replaced with specific classifications to remove ambiguity.
- Security controls relating to high assurance ICT equipment have had their applicability narrowed to 'S, TS' reflecting that they are intended for the protection of SECRET and TOP SECRET systems and data.

New Security Controls	Modified Security Controls	Rescinded Security Controls
1718, 1719, 1720, 1721, 1722, 1723, 1724, 1725, 1726, 1727, 1728, 1729, 1733, 1734, 1735	0041, 0042, 0043, 0109, 0137, 0142, 0164, 0187, 0198, 0206, 0218, 0231, 0235, 0236, 0241, 0247, 0248, 0249, 0250, 0286, 0290, 0292, 0296, 0305, 0310, 0312, 0313, 0315, 0316, 0321, 0323, 0330, 0337, 0341, 0343, 0345, 0348, 0350, 0351, 0352, 0354, 0356, 0357, 0358, 0359, 0360, 0361, 0363, 0368, 0370, 0371, 0372, 0373, 0374, 0375, 0378, 0405, 0420, 0421, 0422, 0432, 0459, 0460, 0467, 0471, 0477, 0479, 0481, 0484, 0501, 0529, 0530, 0535, 0547, 0548, 0558, 0559, 0591, 0610, 0626, 0635, 0643, 0645, 0657, 0658, 0659, 0660, 0663, 0664, 0665, 0669, 0675, 0677, 0678, 0682, 0687, 0694, 0701, 0702, 0705, 0810, 0813, 0835, 0836, 0839, 0854, 0863, 0864, 0869, 0874, 0926, 0931, 0994, 1013, 1014, 1019, 1053, 1059, 1065, 1067, 1074, 1075, 1078, 1079, 1084, 1088, 1091, 1095, 1098, 1101, 1102, 1103, 1104, 1107, 1143, 1145, 1157, 1158, 1163, 1187, 1199, 1211, 1213, 1216, 1217, 1218, 1219, 1220, 1223, 1232, 1294, 1296, 1297, 1299, 1300, 1364, 1366, 1390, 1395, 1400, 1418, 1431, 1432, 1433, 1435, 1436, 1437, 1438, 1439, 1441, 1446, 1450, 1457, 1458, 1461, 1480, 1482, 1518, 1521, 1522, 1528, 1529, 1530, 1532, 1535, 1544, 1547, 1548, 1550, 1555, 1556, 1557, 1559, 1560, 1561, 1578, 1579, 1580, 1581, 1609, 1629, 1630, 1635, 1641	0237, 0342, 0366, 0461, 0505, 0593, 0594, 0641, 0642, 0646, 0647, 0838, 0932, 1015, 1365, 1434, 1468, 1503

Contact details

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