System Security Plan Annex

Identifier	Revision	Updated					Security Control Description	Implementation Status	Implementation Comments	Document Reference	Essential Eight
Guidelines for Cyber Security Roles											
Chief Information Security Officer											
0714	4	Sep-18	O	P	S	TS	A CISO is appointed to provide cyber security leadership for their organisation.	Agency Responsibility	N/A	N/A	
1478	0	Sep-18	O	P	S	TS	The CISO provides strategic-level guidance for their organisation's cyber security program and ensures their organisation's compliance with cyber security policy, standards, regulations and legislation.	Agency Responsibility	N/A	N/A	
System owners											
1071	1	Sep-18	O	P	S	TS	Each system has a designated system owner.	Agency Responsibility	N/A	N/A	
1525	0	Sep-18	O	P	S	TS	System owners register each system with the system's authorising officer.	Agency Responsibility	N/A	N/A	
0027	3	Sep-18	O	P	S	TS	System owners obtain authorisation to operate each system from the system's authorising officer.	Agency Responsibility	N/A	N/A	
1526	0	Sep-18	O	P	S	TS	System owners monitor security risks and the effectiveness of security controls for each system.	Agency Responsibility	N/A	N/A	
Guidelines for Cyber Security Incidents											
Detecting cyber security incidents											
0576	7	Aug-19	O	P	S	TS	An intrusion detection and prevention policy is developed and implemented.	Agency Responsibility	N/A	N/A	
0120	4	Sep-18	O	P	S	TS	Cyber security personnel have access to sufficient data sources and tools to ensure that any security alerts generated by systems are investigated and that systems and data sources are able to be searched for key indicators of compromise including but not limited to IP addresses, domains and file hashes.	Agency Responsibility	N/A	N/A	
Managing cyber security incidents											
0125	4	Aug-19	O	P	S	TS	A cyber security incident register is maintained with the following information: ▪ the date the cyber security incident occurred ▪ the date the cyber security incident was discovered ▪ a description of the cyber security incident ▪ any actions taken in response to the cyber security incident ▪ to whom the cyber security incident was reported.	Agency Responsibility	N/A	N/A	
0133	1	Sep-18	O	P	S	TS	When a data spill occurs, information owners are advised and access to the information is restricted.	Agency Responsibility	N/A	N/A	
0917	7	Oct-19	O	P	S	TS	When malicious code is detected, the following steps are taken to handle the infection: ▪ the infected systems are isolated ▪ all previously connected media used in the period leading up to the infection are scanned for signs of infection and isolated if necessary ▪ antivirus software is used to remove the infection from infected systems and media ▪ if the infection cannot be reliably removed, systems are restored from a known good backup or rebuilt.	Agency Responsibility	N/A	N/A	
0137	2	Sep-18	O	P	S	TS	Legal advice is sought before allowing targeted cyber intrusion activity to continue on a system for the purpose of collecting further information or evidence.	Agency Responsibility	N/A	N/A	
1213	1	Sep-18	O	P	S	TS	Post-incident analysis is performed for successful targeted cyber intrusions; this includes storing full network traffic for at least seven days after a targeted cyber intrusion.	Agency Responsibility	N/A	N/A	
0138	3	Sep-18	O	P	S	TS	The integrity of evidence gathered during an investigation is maintained by investigators recording all of their actions and ensuring raw audit trails are copied onto media for archiving.	Agency Responsibility	N/A	N/A	
Reporting cyber security incidents											
0123	3	Sep-18	O	P	S	TS	Cyber security incidents are reported to an organisation's CISO, or one of their delegates, as soon as possible after they occur or are discovered.	Agency Responsibility	N/A	N/A	
0141	3	Sep-18	O	P	S	TS	When organisations use outsourced information technology or cloud services, their service providers report all cyber security incidents to the organisation's CISO, or one of their delegates, as soon as possible after they occur or are discovered.	Agency Responsibility	N/A	N/A	
0140	6	May-19	O	P	S	TS	Cyber security incidents are reported to the ACSC.	Agency Responsibility	N/A	N/A	
Guidelines for Outsourcing											
Information technology and cloud services											
0100	8	Sep-18	O	P	-	-	Commercial and government gateway and cloud services selected by the ACSC undergo a joint security assessment by ACSC and Information Security Registered Assessors Program assessors at least every two years.	Agency Responsibility	N/A	N/A	

1395	2	Sep-18	O	P	-	-	If using outsourced cloud services, only those listed on the ACSC's ***Certified Cloud Services List*** are used.	Partially Implemented	Microsoft cloud components, including Azure and Office 365, have been IRAP assessed and are currently on the CCSL. All services used by the Blueprint have been IRAP assessed with the exception of Microsoft Defender ATP.	2019 Microsoft Azure IRAP Assessment Report 2019 Microsoft Office 365 IRAP Assessment Report
1529	0	Sep-18	-	-	S	TS	If using outsourced cloud services for highly classified information, public clouds are not used.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1396	1	Sep-18	O	P	S	TS	If using an outsourced cloud service not listed on the ACSC's ***Certified Cloud Services List*** , or for highly classified information, the ACSC is notified in writing at the earliest opportunity, and certainly before entering into or renewing a contract.	Partially Implemented	Microsoft cloud components, including Azure and Office 365, have been IRAP assessed and are currently on the CCSL. All services used by the Blueprint have been IRAP assessed with the exception of Microsoft Defender ATP.	2019 Microsoft Azure IRAP Assessment Report 2019 Microsoft Office 365 IRAP Assessment Report
0873	5	Sep-18	O	P	S	TS	If using an outsourced information technology service, or cloud service not listed on the ACSC's ***Certified Cloud Services List*** , a service provider whose systems are located in Australia is used.	Not Applicable	N/A	N/A
0072	5	Sep-18	O	P	S	TS	Any security controls associated with the protection of information entrusted to a service provider are documented in contract provisions, a memorandum of understanding or an equivalent formal agreement between parties.	Agency Responsibility	N/A	N/A
1073	3	Sep-18	O	P	S	TS	An organisation's systems and information are not accessed or administered by a service provider from outside Australian borders unless a contractual arrangement exists between the organisation and the service provider to do so.	Agency Responsibility	N/A	N/A
1451	1	Sep-18	O	P	S	TS	When entering into a contractual arrangement for outsourced information technology or cloud services, contractual ownership over an organisation's data is explicitly retained.	Agency Responsibility	N/A	N/A
1452	1	Sep-18	O	P	S	TS	A review of suppliers, including their country of origin, is performed before obtaining software, hardware or services to assess the potential increase to an organisation's security risk profile.	Agency Responsibility	N/A	N/A

Guidelines for Security Documentation

Development and maintenance of security documentation

0039	4	May-19	O	P	S	TS	A cyber security strategy is developed and implemented for the organisation.	Agency Responsibility	N/A	N/A
0047	4	May-19	O	P	S	TS	Organisational-level security documentation is approved by the Chief Information Security Officer while system-specific security documentation is approved by the system's authorising officer.	Agency Responsibility	N/A	N/A
0888	5	May-19	O	P	S	TS	Security documentation is reviewed at least annually and includes a 'current as at [date]' or equivalent statement.	Implemented	All security documentation produced for the Blueprint includes a document control table that meets the intent of this control.	DTA - Blueprint System Security Plan DTA - Blueprint Standard Operating Procedures DTA - Blueprint Incident Response Plan

System-specific security documentation

0041	3	Aug-19	O	P	S	TS	Systems have a SSP that includes a description of the system and an annex that covers both security controls from this document (based on the system's classification, functionality and technologies) and any additional security controls that have been identified for the system.	Implemented	An SSP has been drafted for the Blueprint	DTA - Blueprint System Security Plan
0043	3	Sep-18	O	P	S	TS	Systems have an IRP that covers the following: ▪ guidelines on what constitutes a cyber security incident ▪ the types of incidents likely to be encountered and the expected response to each type ▪ how to report cyber security incidents, internally to the organisation and externally to the Australian Cyber Security Centre (ACSC) ▪ other parties which need to be informed in the event of a cyber security incident ▪ the authority, or authorities, responsible for investigating and responding to cyber security incidents ▪ the criteria by which an investigation of a cyber security incident would be requested from a law enforcement agency, the ACSC or other relevant authority ▪ the steps necessary to ensure the integrity of evidence relating to a cyber security incident ▪ system contingency measures or a reference to such details if they are located in a separate document.	Implemented	A system-specific IRP has been drafted for the Blueprint which integrates with the Agency-level IRP	DTA - Blueprint Incident Response Plan

Guidelines for Physical Security

Facilities and systems

0810	4	Sep-18	O	P	S	TS	Any facility containing a system, including a deployable system, is certified and accredited to at least the sensitivity or classification of the system.	Not Applicable	Physical security controls are implemented by Microsoft for Azure and Office 365 components.	2019 Microsoft Azure IRAP Assessment Report 2019 Microsoft Office 365 IRAP Assessment Report
1053	2	Sep-18	O	P	S	TS	Servers and network devices are secured in server rooms or communications rooms that meet the requirements for a Security Zone or secure room suitable for their sensitivity or classification.	Not Applicable	Physical security controls are implemented by Microsoft for Azure and Office 365 components.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
1530	0	Sep-18	O	P	S	TS	Servers and network devices are secured in lockable commercial cabinets or security containers suitable for their sensitivity or classification taking into account protection afforded by the Security Zone or secure room they reside in.	Not Applicable	Physical security controls are implemented by Microsoft for Azure and Office 365 components.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
0813	3	Sep-18	O	P	S	TS	Server rooms, communications rooms and security containers are not left in unsecured states.	Not Applicable	Physical security controls are implemented by Microsoft for Azure and Office 365 components.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
1074	2	Sep-18	O	P	S	TS	Keys or equivalent access mechanisms to server rooms, communications rooms and security containers are appropriately controlled.	Not Applicable	Physical security controls are implemented by Microsoft for Azure and Office 365 components.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
0157	5	Sep-18	O	P	S	TS	Information communicated over network infrastructure in areas not authorised for the processing of such information is encrypted as if it was communicated through unsecured spaces.	Not Applicable	Physical security controls are implemented by Microsoft for Azure and Office 365 components.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
1296	2	Sep-18	O	P	S	TS	Physical security controls are implemented to protect network devices, especially those in public areas, from physical damage or unauthorised access.	Not Applicable	Physical security controls are implemented by Microsoft for Azure and Office 365 components.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
0164	2	Sep-18	O	P	S	TS	Unauthorised people are prevented from observing systems, in particular, workstation displays and keyboards.	Not Applicable	Physical security controls are implemented by Microsoft for Azure and Office 365 components.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report

ICT equipment and media

0336	4	Aug-19	O	P	S	TS	An ICT equipment and media register is maintained and regularly audited.	Agency Responsibility	The Agency is responsible for the management of ICT equipment and media used in relation to the Blueprint.	N/A
0159	4	Sep-18	O	P	S	TS	All ICT equipment and media are accounted for on a regular basis.	Agency Responsibility	The Agency is responsible for the management of ICT equipment and media used in relation to the Blueprint.	N/A
0161	5	Mar-19	O	P	S	TS	ICT equipment and media are secured when not in use.	Agency Responsibility	The Agency is responsible for the management of ICT equipment and media used in relation to the Blueprint.	N/A

Wireless devices and Radio Frequency transmitters

1543	1	Aug-19	-	-	S	TS	An authorised RF devices for SECRET and TOP SECRET areas register is maintained and regularly audited.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0225	2	Sep-18	-	-	S	TS	Unauthorised RF devices are not brought into SECRET and TOP SECRET areas.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0829	4	Mar-19	-	-	S	TS	Security measures are used to detect and respond to unauthorised RF devices in SECRET and TOP SECRET areas.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1058	2	Oct-19	O	P	S	TS	Bluetooth and wireless keyboards are not used unless in an RF screened building.	Agency Responsibility	The Agency is responsible for managing the use of wireless devices and radio frequency transmitters.	N/A
0222	2	Sep-18	O	P	-	-	When using infrared keyboards, infrared ports are positioned to prevent line of sight and reflected communications travelling into an unsecured space.	Agency Responsibility	The Agency is responsible for managing the use of wireless devices and radio frequency transmitters.	N/A
0223	4	Sep-18	-	-	S	-	When using infrared keyboards, the following activities are prevented: ▪ line of sight and reflected communications travelling into unsecured spaces ▪ multiple infrared keyboards for different systems being used in the same area ▪ other infrared devices being used in the same area ▪ infrared keyboards operating in areas with unprotected windows.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A

0224	4	Sep-18	-	-	-	TS	When using infrared keyboards, the following activities are prevented: ▪ line of sight and reflected communications travelling into unsecured spaces ▪ multiple infrared keyboards for different systems being used in the same area ▪ other infrared devices being used in the same area ▪ infrared keyboards operating in areas with windows that have not had a permanent method of blocking infrared transmissions applied to them.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A	
0221	2	Sep-18	-	-	-	TS	Wireless RF pointing devices are not used in TOP SECRET areas unless used in an RF screened building.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A	

Guidelines for Personnel Security

Cyber security awareness raising and training

0252	4	Sep-19	O	P	S	TS	Ongoing cyber security awareness raising and training is provided to personnel and includes: ▪ the purpose of the cyber security awareness raising and training program ▪ security appointments and contacts within the organisation ▪ the authorised use of systems and their resources ▪ the protection of systems and their resources ▪ reporting of cyber security incidents and suspected compromises of systems and their resources.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
0817	3	Sep-18	O	P	S	TS	Personnel are advised what suspicious contact is and how to report it, especially when using online services.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
0820	4	Sep-18	O	P	S	TS	Personnel are advised to not post work information to non-approved online services and to report cases where such information is posted.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
1146	2	Sep-18	O	P	S	TS	Personnel are advised to maintain separate work and personal accounts for online services.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
0821	3	Oct-19	O	P	S	TS	Personnel are advised of security risks associated with posting personal information to online services and are encouraged to use any available privacy settings to restrict who can view such information.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
0824	2	Sep-18	O	P	S	TS	Personnel are advised not to send or receive files via unauthorised online services.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	

Access to systems and their resources

0432	5	Aug-19	O	P	S	TS	Each system's System Security Plan specifies any authorisations, security clearances and briefings necessary for access to the system and its resources.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
0434	6	Aug-19	O	P	S	TS	Personnel undergo appropriate employment screening, and where necessary hold an appropriate security clearance, before being granted access to a system and its resources.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
0435	3	Aug-19	O	P	S	TS	Personnel receive any necessary briefings before being granted access to a system and its resources.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
0414	4	Aug-19	O	P	S	TS	Personnel granted access to a system and its resources are uniquely identifiable.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
0975	7	Aug-19	O	P	S	TS	Personnel who are foreign nationals are identified as such, including by their specific nationality.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
0420	8	Aug-19	-	-	S	TS	Where systems process, store or communicate AUSTEO or AGAO information, personnel who are foreign nationals are identified as such, including by their specific nationality.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A	
1538	1	Aug-19	-	P	S	TS	Where systems process, store or communicate REL information, personnel who are foreign nationals are identified as such, including by their specific nationality.	Not Applicable	is not designed to process, store or communicate REL information.	N/A	
0415	3	Aug-19	O	P	S	TS	The use of shared user accounts is strictly controlled, and personnel using such accounts are uniquely identifiable.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
0405	5	Sep-19	O	P	S	TS	Standard access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
1503	1	Sep-19	O	P	S	TS	Standard access to systems, applications and data repositories is limited to that required for personnel to undertake their duties.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
0409	5	Aug-19	-	-	S	TS	Foreign nationals, including seconded foreign nationals, do not have access to systems that process, store or communicate AUSTEO information unless effective security controls are in place to ensure such information is not accessible to them.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A	
0411	5	Aug-19	-	-	S	TS	Foreign nationals, excluding seconded foreign nationals, do not have access to systems that process, store or communicate AGAO information unless effective security controls are in place to ensure such information is not accessible to them.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A	
0816	5	Aug-19	-	P	S	TS	Foreign nationals, including seconded foreign nationals, do not have access to systems that process, store or communicate REL information unless effective security controls are in place to ensure REL information that is not marked as releasable to their nation is not accessible to them.	Not Applicable	is not designed to process, store or communicate REL information.	N/A	
1507	1	Sep-19	O	P	S	TS	Privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	Restrict Administrative Privileges

1508	1	Sep-19	O	P	S	TS	Privileged access to systems, applications and data repositories is limited to that required for personnel to undertake their duties..	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	Restrict Administrative Privileges
0445	6	Sep-18	O	P	S	TS	Privileged users are assigned a dedicated privileged account to be used solely for tasks requiring privileged access.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
1509	0	Sep-18	O	P	S	TS	The use of privileged accounts, and any activities undertaken with them, are monitored and audited.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
1175	3	Sep-18	O	P	S	TS	Technical security controls are used to prevent privileged users from reading emails, browsing the Web and obtaining files via online services.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	Restrict Administrative Privileges
0448	6	Sep-19	O	P	S	TS	Foreign nationals, excluding seconded foreign nationals, do not have privileged access to systems, applications and data repositories.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
0446	3	Aug-19	-	-	S	TS	Foreign nationals, including seconded foreign nationals, do not have privileged access to systems that process, store or communicate AUSTEO information.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A	
0447	3	Aug-19	-	-	S	TS	Foreign nationals, excluding seconded foreign nationals, do not have privileged access to systems that process, store or communicate AGAO information.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A	
1545	0	Aug-19	-	P	S	TS	Foreign nationals, including seconded foreign nationals, do not have privileged access to systems that process, store or communicate REL information.	Not Applicable	is not designed to process, store or communicate REL information.	N/A	
0430	7	Sep-19	O	P	S	TS	Access to systems, applications and data repositories is removed or suspended on the same day personnel no longer have a legitimate requirement for access.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
1404	2	Sep-19	O	P	S	TS	Access to systems, applications and data repositories is removed or suspended after one month of inactivity.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
0407	4	Sep-18	O	P	S	TS	A secure record is maintained for the life of each system covering: ▪ all personnel authorised to access the system, and their user identification ▪ who provided authorisation for access ▪ when access was granted ▪ the level of access that was granted ▪ when access, and the level of access, was last reviewed ▪ when the level of access was changed, and to what extent (if applicable) ▪ when access was withdrawn (if applicable).	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
0441	6	Sep-19	O	P	S	TS	When personnel are granted temporary access to a system, effective security controls are put in place to restrict their access to only information required for them to undertake their duties.	Agency Responsibility	The Agency is responsible for the personnel security as it relates to users of the Blueprint.	N/A	
0443	3	Sep-18	-	-	S	TS	Temporary access is not granted to systems that process, store or communicate caveated or sensitive compartmented information.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A	
0078	4	Sep-18	-	-	S	TS	Systems processing, storing or communicating AUSTEO or AGAO information remain at all times under the control of an Australian national working for or on behalf of the Australian Government.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A	
0854	4	Sep-18	-	-	S	TS	Access to AUSTEO or AGAO information from systems not under the sole control of the Australian Government is prevented.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A	

Guidelines for Communications Infrastructure

Cable management

0181	2	Sep-18	O	P	S	TS	Cables are installed in accordance with the relevant Australian Standards, as directed by the Australian Communications and Media Authority (ACMA).	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A	
0926	7	Oct-19	O	P	S	TS	The cable colours in the following table are used. (See source document for referenced table)	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A	
0825	2	Oct-19	O	P	S	TS	Cable colours for foreign systems installed in Australian facilities are not the same colour as those used for Australian systems.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A	
0826	2	Oct-19	O	P	S	TS	Cable colours used for foreign systems are agreed between the host organisation and the foreign system's owner.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A	
1215	1	Sep-18	O	P	S	-	In non-TOP SECRET areas, cables with non-conformant cable colouring are banded with the appropriate colour at inspection points.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A	
1216	1	Sep-18	O	P	S	TS	In TOP SECRET areas, cables with non-conformant cable colouring are both banded with the appropriate colour and labelled at inspection points.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A	
1112	2	Sep-18	O	P	S	TS	In non-shared government facilities, cables are inspectable at a minimum of five-metre intervals.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A	
1118	1	Sep-18	O	P	S	-	In non-TOP SECRET areas of shared government facilities, cables are inspectable at a minimum of five-metre intervals.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A	
1119	1	Sep-18	O	P	S	TS	In TOP SECRET areas of shared government facilities, cables are fully inspectable for their entire length.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A	
1126	1	Sep-18	O	P	S	-	In non-TOP SECRET areas of shared non-government facilities, cables are inspectable at a minimum of five-metre intervals.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A	
0184	2	Sep-18	O	P	S	TS	In TOP SECRET areas of shared non-government facilities, cables are fully inspectable for their entire length.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A	

0187	5	Sep-18	O	P	S	TS	The approved group combinations for cables in the following table are used. (See source document for referenced table)	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1111	2	Oct-19	O	P	S	TS	Fibre-optic cables are used for network infrastructure instead of copper cables.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
0189	2	Sep-18	O	P	S	TS	With fibre-optic cables, the fibres in the sheath only carry a single group.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
0190	2	Sep-18	O	P	S	TS	If a fibre-optic cable contains subunits, each subunit only carries a single group; however, each subunit in the cable can carry a different group.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1114	2	Oct-19	O	P	S	TS	Approved cable groups sharing a common reticulation system have a dividing partition or a visible gap between the differing cable groups.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1130	3	Oct-19	O	P	S	TS	In shared non-government facilities, cables are run in an enclosed cable reticulation system.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1164	2	Oct-19	O	P	S	TS	In shared non-government facilities, conduits or the front covers of ducts, cable trays in floors and ceilings, and associated fittings are clear plastic.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
0195	3	Sep-18	-	-	-	TS	In shared non-government facilities, uniquely identifiable SCEC endorsed tamper-evident seals are used to seal all removable covers on reticulation systems, including box section front covers, conduit inspection boxes, outlet and junction boxes, and T-pieces.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0194	2	Sep-18	-	-	-	TS	In shared non-government facilities, a visible smear of conduit glue is used to seal all plastic conduit joints and conduit runs connected by threaded lock nuts.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1102	1	Sep-18	O	P	S	-	In non-TOP SECRET areas, reticulation systems leading into cabinets are terminated as close as possible to the cabinet.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1101	1	Sep-18	O	P	S	TS	In TOP SECRET areas, reticulation systems leading into cabinets in a secure communications or server room are terminated as close as possible to the cabinet.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1103	1	Sep-18	O	P	S	TS	In TOP SECRET areas, reticulation systems leading into cabinets not in a secure communications or server room are terminated at the boundary of the cabinet.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1098	2	Oct-19	O	P	S	-	Cables are terminated in individual cabinets, or for small systems, one cabinet with a division plate to delineate classifications.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1100	1	Sep-18	-	-	-	TS	TOP SECRET cables are terminated in an individual TOP SECRET cabinet.	Not Applicable		
1116	3	Oct-19	O	P	S	TS	There is a visible gap between TOP SECRET cabinets and cabinets of lower classifications.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1115	3	Oct-19	O	P	S	TS	Cables from cable trays to wall outlets are run in flexible or plastic conduit.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1133	1	Sep-18	-	-	-	TS	In shared non-government facilities, cables are not run in a party wall.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1122	1	Sep-18	-	-	-	TS	In shared government facilities, where wall penetrations exit into a lower classified space, cables are encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1134	1	Sep-18	-	-	-	TS	In shared non-government facilities, where wall penetrations exit into a lower classified space, cables are encased in conduit with all gaps between the conduit and the wall filled with an appropriate sealing compound.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1104	1	Sep-18	O	P	S	-	Cable groups sharing a wall outlet use fibre-optic cables and different connectors on opposite sides of the wall outlet for each group.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1105	1	Sep-18	O	P	S	TS	TOP SECRET cables do not share a wall outlet with cables of a lower classification.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1106	1	Sep-18	O	P	S	TS	The connectors for TOP SECRET systems are different from those of systems of lower classifications.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1107	2	Oct-19	O	P	S	TS	The wall outlet colours in the following table are used. (See source document for referenced table)	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1109	2	Oct-19	O	P	S	TS	Faceplates on wall outlets are clear plastic.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
0198	2	Sep-18	-	-	-	TS	When penetrating an audio secured space, ASIO is consulted and all directions provided are complied with.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1123	2	Sep-18	-	-	-	TS	In TOP SECRET areas of shared government facilities, a power distribution board with a feed from an Uninterruptible Power Supply is used to power all TOP SECRET ICT equipment.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1135	1	Sep-18	-	-	-	TS	In TOP SECRET areas of shared non-government facilities, a power distribution board with a feed from an Uninterruptible Power Supply is used to power all TOP SECRET ICT equipment.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A

Cable labelling and registration

0201	2	Sep-18	-	-	-	TS	Labels for TOP SECRET conduits are a minimum size of 2.5 cm x 1 cm, attached at 5 m intervals and marked as 'TS RUN'.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0202	2	Sep-18	-	-	-	TS	Conduit labels in areas where uncleared personnel could frequently visit have red text on a clear background.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0203	2	Sep-18	-	-	-	TS	Conduit labels in areas that are not clearly observable have red text on a white background.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A

0204	2	Sep-18	O	P	S	TS	Conduit labels installed in public or visitor areas do not draw undue attention from people who do not have a need-to-know of the existence of such cables.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1095	2	Oct-19	O	P	S	TS	Wall outlet boxes denote the classification, cable number and outlet number.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1096	2	Oct-19	O	P	S	TS	Cables are labelled at each end with sufficient source and destination details to enable the physical identification and inspection of the cable.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
0206	5	Aug-19	O	P	S	TS	A cable labelling process, and supporting cable labelling procedures, is developed and implemented.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
0208	2	Oct-19	O	P	S	TS	A cable register is maintained with the following information: ▪ cable identification number ▪ classification ▪ source ▪ destination ▪ site/floor plan diagram ▪ seal numbers (if applicable).	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
0211	3	Sep-18	O	P	S	TS	Cables are inspected for inconsistencies with the cable register in accordance with the frequency defined in a system's System Security Plan.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
Cable patching										
0213	2	Sep-18	O	P	S	TS	Only approved cable groups terminate on a patch panel.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1093	2	Sep-18	O	P	S	-	In areas containing cables for systems of different classifications, connectors for each system are different from those of other systems; unless the higher classified patch cables cannot bridge the distance between the higher classified patch panel and any patch panel of a lower classification.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
0214	3	Sep-18	O	P	S	TS	In areas containing cables for TOP SECRET systems and systems of lower classifications, the connectors for TOP SECRET systems are different from those of other systems.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1094	2	Oct-19	O	P	S	TS	In areas containing cables for systems of different classifications, the selection of connector types is documented.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
0216	2	Sep-18	O	P	S	TS	TOP SECRET and non-TOP SECRET patch panels are physically separated by installing them in separate cabinets.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
0217	4	Sep-18	O	P	S	TS	Where spatial constraints demand patch panels of lower classifications than TOP SECRET be located in the same cabinet as a TOP SECRET patch panel: ▪ a physical barrier in the cabinet is provided to separate patch panels ▪ only personnel holding a Positive Vetting security clearance have access to the cabinet ▪ approval from the TOP SECRET system's authorising officer is obtained prior to installation.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
0218	3	Sep-18	-	-	-	TS	If fibre-optic fly leads exceeding five meters in length are used to connect wall outlets to ICT equipment, they are run in a protective and easily inspected pathway and clearly labelled at the ICT equipment end with the wall outlet's designator.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
Emanation security										
0247	3	Sep-18	-	-	S	TS	System owners deploying systems with Radio Frequency (RF) transmitters inside or co-located with their facility contact the ACSC for an emanation security threat assessment and implement any additional installation criteria derived from the emanation security threat assessment.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0248	5	Sep-18	O	P	S	-	System owners deploying systems with RF transmitters that will be co-located with systems of a higher classification contact the ACSC for an emanation security threat assessment and implement any additional installation criteria derived from the emanation security threat assessment.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
1137	2	Sep-18	-	-	-	TS	System owners deploying systems in shared facilities with non-Australian government entities contact the ACSC for an emanation security threat assessment and implement any additional installation criteria derived from the emanation security threat assessment.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0932	5	Sep-18	O	P	-	-	System owners deploying systems overseas contact the ACSC for emanation security threat advice and implement any additional installation criteria derived from the emanation security threat advice.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
0249	3	Sep-18	-	-	S	TS	System owners deploying systems overseas contact the ACSC for an emanation security threat assessment and implement any additional installation criteria derived from the emanation security threat assessment.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0246	3	Sep-18	O	P	S	TS	An emanation security threat assessment is sought as early as possible in a project's life cycle as emanation security controls can have significant cost implications.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A
0250	3	Sep-18	O	P	S	TS	ICT equipment in TOP SECRET areas meets industry and government standards relating to electromagnetic interference/electromagnetic compatibility.	Agency Responsibility	The Agency is responsible for communications infrastructure leveraged by the Blueprint.	N/A

Guidelines for Communications Systems

Telephone systems

1078	2	Aug-19	O	P	S	TS	A telephone systems usage policy is developed and implemented.	Not Applicable	The Blueprint does not include telephone systems.	N/A

0229	3	Sep-18	O	P	S	TS	Personnel are advised of the permitted sensitivity or classification of information that can be discussed over both internal and external telephone systems.	Not Applicable	The Blueprint does not include telephone systems.	N/A
0230	3	Sep-18	O	P	S	TS	Personnel are advised of security risks posed by non-secure telephone systems in areas where sensitive or classified conversations can occur.	Not Applicable	The Blueprint does not include telephone systems.	N/A
0231	1	Sep-18	O	P	S	TS	When permitting different levels of conversation for different kinds of connections, telephone systems give a visual indication of what kind of connection has been made.	Not Applicable	The Blueprint does not include telephone systems.	N/A
0232	3	Sep-18	O	P	S	TS	Telephone systems used for sensitive or classified conversations encrypt all traffic that passes over external systems.	Not Applicable	The Blueprint does not include telephone systems.	N/A
0233	3	Sep-18	O	P	S	TS	Cordless telephone systems are not used for sensitive or classified conversations.	Not Applicable	The Blueprint does not include telephone systems.	N/A
0235	3	Sep-18	O	P	S	TS	Speakerphones are not used on telephone systems in TOP SECRET areas unless the telephone system is located in a room rated as audio secure, the room is audio secure during conversations and only personnel involved in discussions are present in the room.	Not Applicable	The Blueprint does not include telephone systems.	N/A
0236	4	Sep-18	O	P	-	-	In PROTECTED areas, off-hook audio protection features are used on all telephones that are not authorised for the transmission of PROTECTED information.	Not Applicable	The Blueprint does not include telephone systems.	N/A
0931	4	Sep-18	O	P	S	-	In SECRET areas, push-to-talk handsets are used on all telephones that are not authorised for the transmission of SECRET information.	Not Applicable	The Blueprint does not include telephone systems.	N/A
0237	3	Sep-18	O	P	S	TS	In TOP SECRET areas, push-to-talk handsets are used on all telephones that are not authorised for the transmission of TOP SECRET information.	Not Applicable	The Blueprint does not include telephone systems.	N/A
Video conferencing and Internet Protocol telephony										
0546	6	Sep-18	O	P	S	TS	Where a requirement exists to implement a firewall in a gateway, and video conferencing or IP telephony traffic passes through the gateway, a video or voice-aware firewall is used.	Agency Responsibility	The Agency is responsible for all gateway configurations.	N/A
0547	3	Sep-18	O	P	S	TS	Video conferencing and IP telephony signalling and data is encrypted.	Implemented	Microsoft Teams signalling data is encrypted.	2019 Microsoft Office 365 IRAP Assessment Report
0548	3	Sep-18	O	P	S	TS	Video conferencing and IP telephony functions are established using secure signalling and data protocols.	Implemented	Secure signalling and data protocols are used by Microsoft Teams including Session Initiation Protocol (SIP) and Secure Real Time Protocol (SRTP).	2019 Microsoft Office 365 IRAP Assessment Report
0554	1	Sep-18	O	P	S	TS	An encrypted and non-replayable two-way authentication scheme is used for call authentication and authorisation.	Implemented	Microsoft Teams leverages Azure AD for authentication.	2019 Microsoft Office 365 IRAP Assessment Report
0553	3	Sep-18	O	P	S	TS	Authentication and authorisation is used for all actions on a video conferencing network, including call setup and changing settings.	Implemented	Microsoft Teams leverages Azure AD for authentication.	2019 Microsoft Office 365 IRAP Assessment Report
0555	2	Sep-18	O	P	S	TS	Authentication and authorisation is used for all actions on a IP telephony network, including registering a new IP phone, changing phone users, changing settings and accessing voicemail.	Implemented	Microsoft Teams leverages Azure AD for authentication.	2019 Microsoft Office 365 IRAP Assessment Report
0551	6	Oct-19	O	P	S	TS	IP telephony is configured such that: ▪ IP phones authenticate themselves to the call controller upon registration ▪ auto-registration is disabled and only a whitelist of authorised devices is allowed to access the network ▪ unauthorised devices are blocked by default ▪ all unused and prohibited functionality is disabled.	Not Applicable	The Blueprint does not include physical IP telephones.	N/A
1014	5	Sep-18	-	-	S	TS	Individual logins are used for IP phones.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0549	4	Oct-19	O	P	S	TS	Video conferencing and IP telephony traffic is separated physically or logically from other data traffic.	Implemented	Microsoft Teams has a dedicated VLAN within the Microsoft cloud.	2019 Microsoft Office 365 IRAP Assessment Report
0556	5	Oct-19	O	P	S	TS	Workstations are not connected to video conferencing units or IP phones unless the workstation or the device uses VLANs or similar mechanisms to maintain separation between video conferencing, IP telephony and other data traffic.	Not Applicable	The Blueprint does not include physical IP telephones of video conferencing equipment.	N/A
1015	5	Sep-18	O	P	S	TS	Traditional analog phones are used in lobby and shared areas.	Not Applicable	The Blueprint does not include the use of analog phones.	N/A
0558	4	Sep-18	O	P	S	TS	If IP phones are used in lobby and shared areas, their ability to access data networks, voicemail and directory services are prevented.	Not Applicable	The Blueprint does not include physical IP telephones.	N/A
0559	4	Sep-18	O	P	S	-	Microphones (including headsets and USB handsets) and webcams are not used with non-SECRET workstations in SECRET areas.	Not Applicable	The Blueprint is not designed to be used in SECRET areas.	N/A
1450	1	Sep-18	O	P	S	TS	Microphones (including headsets and USB handsets) and webcams are not used with non-TOP SECRET workstations in TOP SECRET areas.	Not Applicable	The Blueprint is not designed to be used in TOP SECRET areas.	N/A
1019	7	Sep-18	O	P	S	TS	A denial of service response plan is developed and implemented that includes: ▪ how to identify signs of a denial of service ▪ how to identify the source of a denial of service ▪ how capabilities can be maintained during a denial of service ▪ what actions can be taken to clear a denial of service.	Implemented	Microsoft Teams leverages Azure's DDoS protection capabilities.	2019 Microsoft Office 365 IRAP Assessment Report
Fax machines and multifunction devices										
0588	3	Aug-19	O	P	S	TS	A fax machine and MFD usage policy is developed and implemented.	Agency Responsibility	The Agency is responsible for the use and management of all fax machines and MFDs.	N/A
1092	2	Sep-18	O	P	S	TS	Separate fax machines or MFDs are used for sending sensitive or classified fax messages and all other fax messages.	Agency Responsibility	The Agency is responsible for the use and management of all fax machines and MFDs.	N/A
0241	3	Sep-18	O	P	S	TS	When sending fax messages, the fax message is encrypted to an appropriate level to be communicated over unsecured telecommunications infrastructure or the PSTN.	Agency Responsibility	The Agency is responsible for the use and management of all fax machines and MFDs.	N/A

1075	1	Sep-18	O	P	S	TS	The sender of a fax message makes arrangements for the receiver to collect the fax message as soon as possible after it is received and notify the sender if the fax message does not arrive in an agreed amount of time.	Agency Responsibility	The Agency is responsible for the use and management of all fax machines and MFDs.	N/A
0245	4	Sep-18	O	P	S	TS	A direct connection from an MFD to a digital telephone system is not enabled unless the telephone system is authorised to operate at the same sensitivity or classification as the computer network to which the MFD is connected.	Agency Responsibility	The Agency is responsible for the use and management of all fax machines and MFDs.	N/A
0590	4	Sep-18	O	P	S	TS	Where MFDs connected to computer networks have the ability to communicate via a gateway to another network: ▪ each MFD applies user identification, authentication and audit functions for all information communicated by that device ▪ security controls are of similar strength to those specified for workstations on that network ▪ each gateway can identify and filter information in accordance with the security controls for the export of data via a gateway.	Agency Responsibility	The Agency is responsible for the use and management of all fax machines and MFDs.	N/A
0589	4	Sep-18	O	P	S	TS	MFDs connected to computer networks are not used to copy documents above the sensitivity or classification of the connected network.	Agency Responsibility	The Agency is responsible for the use and management of all fax machines and MFDs.	N/A
1036	3	Sep-18	O	P	S	TS	Fax machines and MFDs are located in areas where their use can be observed.	Agency Responsibility	The Agency is responsible for the use and management of all fax machines and MFDs.	N/A

Guidelines for Enterprise Mobility

Mobile device management

1533	2	Aug-19	O	P	S	TS	A mobile device management policy is developed and implemented.	Agency Responsibility	The Agency is responsible for developing a mobile device management policy in relation to the Blueprint.	N/A
1195	1	Sep-18	O	P	S	TS	A Mobile Device Management solution is used to ensure mobile device management policy is applied to all mobile devices.	Implemented	Microsoft Intune provides MDM capability.	DTA - Platform Design
0687	5	Sep-18	-	-	-	TS	Mobile devices do not process, store or communicate TOP SECRET information unless explicitly approved by the ACSC to do so.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1400	3	Oct-19	O	P	-	-	Personnel accessing official or classified information using a privately-owned mobile device use an ACSC approved platform, a security configuration in accordance with ACSC guidance, and have enforced separation of official and classified information from any personal information.	Not Applicable	The Blueprint does not include the use of privately-owned mobile devices.	N/A
0694	4	Sep-18	-	-	S	TS	Privately-owned mobile devices do not access highly classified systems.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1297	1	Sep-18	O	P	S	TS	Prior to allowing privately-owned mobile devices to connect to an organisation's systems, legal advice is sought.	Not Applicable	The Blueprint does not include the use of privately-owned mobile devices.	N/A
1482	2	Oct-19	O	P	S	TS	Personnel accessing official or classified information using an organisation-owned mobile device use an ACSC approved platform with a security configuration in accordance with ACSC guidance.	Partially Implemented	provides Windows 10 for laptops which is hardened in accordance with ACSC guidance. also provides MDM for iOS but does not fully implement ACSC's guidance for PROTECTED.	DTA - Workstation Design DTA - Platform Design
0869	3	Sep-18	O	P	S	TS	All information on mobile devices is encrypted using at least an Australian Signals Directorate Approved Cryptographic Algorithm.	Implemented	Microsoft BitLocker provides full disk encryption of mobile devices, implementing XTS-AES-256. Additionally, iOS devices implement AES-256 encryption by default.	DTA - Workstation Design DTA - Windows 10 ABAC
1085	2	Sep-18	O	P	S	TS	Mobile devices used to communicate sensitive or classified information over public network infrastructure use encryption approved for communicating such information over public network infrastructure.	Implemented	All information transmitted to and from mobile devices and Office 365 is encrypted.	DTA - Office 365 Design
1202	1	Sep-18	O	P	-	-	The range of Bluetooth communications between mobile devices and other Bluetooth devices is restricted to less than 10 metres by using class 2 or class 3 Bluetooth devices.	Partially Implemented	Bluetooth is disabled on Windows 10 devices. Bluetooth is not managed for iOS devices.	DTA - Workstation Design DTA - Platform Design
0682	4	Sep-18	-	-	S	TS	Bluetooth functionality is not enabled on highly classified mobile devices.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1196	1	Sep-18	O	P	-	-	Mobile devices are configured to remain undiscoverable to other Bluetooth devices except during Bluetooth pairing.	Partially Implemented	Bluetooth is disabled on Windows 10 devices. Bluetooth is not managed for iOS devices.	DTA - Workstation Design DTA - Platform Design
1200	3	Sep-18	O	P	-	-	Bluetooth pairing is performed using Bluetooth version 2.1 or later.	Partially Implemented	Bluetooth is disabled on Windows 10 devices. Bluetooth is not managed for iOS devices.	DTA - Workstation Design DTA - Platform Design
1198	1	Sep-18	O	P	-	-	Bluetooth pairing is performed in a manner such that connections are only made between intended Bluetooth devices.	Partially Implemented	Bluetooth is disabled on Windows 10 devices. Bluetooth is not managed for iOS devices.	DTA - Workstation Design DTA - Platform Design
1199	1	Sep-18	O	P	-	-	Bluetooth pairings are removed from mobile devices when there is no longer a requirement for their use.	Partially Implemented	Bluetooth is disabled on Windows 10 devices. Bluetooth is not managed for iOS devices.	DTA - Workstation Design DTA - Platform Design
0863	3	Sep-18	O	P	S	TS	Mobile devices prevent personnel from installing or uninstalling applications once provisioned.	Partially Implemented	standard users do not have sufficient permissions to install or uninstall applications on Windows 10 devices. Standard users can install and uninstall applications on iOS devices via the App Store.	DTA - Workstation Design DTA - Platform Design

0864	3	Apr-19	O	P	S	TS	Mobile devices prevent personnel from disabling or modifying security functions once provisioned.	Partially Implemented	standard users do not have sufficient permissions to modify security functions on Windows 10 devices. Standard users can modify security functions on iOS devices.	DTA - Workstation Design DTA - Platform Design
1365	1	Sep-18	O	P	S	TS	Mobile carriers that are able to provide timely security updates for mobile devices are used.	Implemented	Apple provide timely security updates for iOS devices.	DTA - Platform ABAC
1366	1	Sep-18	O	P	S	TS	Mobile devices are able to accept security updates from mobile carriers as soon as they become available.	Implemented	Apple provides timely security updates for iOS devices.	DTA - Platform ABAC
0874	4	Sep-18	O	P	-	-	Web browsing from mobile devices is conducted through an organisation's internet gateway rather than via a direct connection to the Internet.	Not Implemented	The Blueprint permits direct connection to the internet for all devices as per the DTA's requirements.	DTA - Platform Design
0705	3	Sep-18	O	P	S	TS	When accessing an organisation system via a VPN connection, split tunnelling is disabled.	Not Applicable	The Blueprint does not include the use of VPNs.	N/A
Mobile device usage										
1082	2	Aug-19	O	P	S	TS	A mobile device usage policy is developed and implemented.	Agency Responsibility	The Agency is responsible for developing and enforcing a mobile device usage policy in relation to the Blueprint.	N/A
1083	2	Sep-18	O	P	S	TS	Personnel are advised of the sensitivity or classification permitted for voice and data communications when using mobile devices.	Agency Responsibility	The Agency is responsible for developing and enforcing a mobile device usage policy in relation to the Blueprint.	N/A
0240	5	Sep-18	O	P	S	TS	Paging, Multimedia Message Service, Short Message Service or instant messaging apps are not used to communicate sensitive or classified information.	Agency Responsibility	The Agency is responsible for developing and enforcing a mobile device usage policy in relation to the Blueprint.	N/A
0866	4	Apr-19	O	P	S	TS	Sensitive or classified information is not viewed or communicated in public locations unless care is taken to reduce the chance of conversations being overheard or the screen of a mobile device being observed.	Agency Responsibility	The Agency is responsible for developing and enforcing a mobile device usage policy in relation to the Blueprint.	N/A
1145	3	Sep-18	-	-	S	TS	Privacy filters are applied to the screens of highly classified mobile devices.	Agency Responsibility	The Agency is responsible for developing and enforcing a mobile device usage policy in relation to the Blueprint.	N/A
0871	3	Apr-19	O	P	S	TS	Mobile devices are kept under continual direct supervision when being actively used.	Agency Responsibility	The Agency is responsible for developing and enforcing a mobile device usage policy in relation to the Blueprint.	N/A
0870	3	Apr-19	O	P	S	TS	Mobile devices are carried or stored in a secured state when not being actively used.	Agency Responsibility	The Agency is responsible for developing and enforcing a mobile device usage policy in relation to the Blueprint.	N/A
1084	2	Sep-18	O	P	S	TS	If unable to apply encryption to mobile devices that is suitable for them to be carried through areas not authorised to process the information stored on them, they are physically transferred in a security briefcase or an approved multi-use satchel, pouch or transit bag.	Agency Responsibility	The Agency is responsible for developing and enforcing a mobile device usage policy in relation to the Blueprint.	N/A
0701	4	Aug-19	O	P	S	TS	A mobile device emergency sanitisation process, and supporting mobile device emergency sanitisation procedures, is developed and implemented.	Agency Responsibility	The Agency is responsible for developing and enforcing a mobile device usage policy in relation to the Blueprint.	N/A
0702	4	Aug-19	-	-	S	TS	If a cryptographic zeroise or sanitise function is provided for cryptographic keys on highly classified mobile devices, the function is used as part of the mobile device emergency sanitisation process.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1298	2	Oct-19	O	P	S	TS	Personnel are advised of privacy and security risks when travelling overseas with mobile devices.	Agency Responsibility	The Agency is responsible for developing and enforcing a mobile device usage policy in relation to the Blueprint.	N/A
1554	0	Oct-19	O	P	S	TS	If travelling overseas with mobile devices to high/extreme risk countries, personnel are: ▪ issued with newly provisioned accounts and devices from a pool of dedicated travel devices which are used solely for work-related activities ▪ advised on how to apply and inspect tamper seals to key areas of devices ▪ advised to avoid taking any personal devices, especially if rooted or jailbroken.	Agency Responsibility	The Agency is responsible for developing and enforcing a mobile device usage policy in relation to the Blueprint.	N/A
1555	0	Oct-19	O	P	S	TS	Before travelling overseas with mobile devices, personnel take the following actions: ▪ record all details of the devices being taken, such as product types, serial numbers and International Mobile Equipment Identity numbers ▪ update all applications and operating systems ▪ remove all non-essential accounts, applications and data ▪ apply security configuration settings, such as lock screens ▪ configure remote locate and wipe functionality ▪ enable encryption, including for any media used ▪ backup all important data and configuration settings.	Agency Responsibility	The Agency is responsible for developing and enforcing a mobile device usage policy in relation to the Blueprint.	N/A

1299	2	Oct-19	O	P	S	TS	Personnel take the following precautions when travelling overseas with mobile devices: ▪ never leaving devices or media unattended for any period of time, including by placing them in checked-in luggage or leaving them in hotel safes ▪ never storing credentials with devices that they grant access to, such as in laptop bags ▪ never lending devices to untrusted people, even if briefly ▪ never allowing untrusted people to connect other devices or media to their devices, including for charging ▪ never using designated charging stations, wall outlet charging ports or chargers supplied by untrusted people ▪ avoiding connecting devices to open or untrusted Wi-Fi networks ▪ using an approved Virtual Private Network to encrypt all device communications ▪ using encrypted mobile applications for communications instead of using foreign telecommunication networks ▪ disabling any communications capabilities of devices when not in use, such as cellular data, wireless, Bluetooth and Near Field Communication ▪ avoiding reuse of media once used with other parties' devices or systems ▪ ensuring any media used for data transfers are thoroughly checked for malicious code beforehand ▪ never using any gifted devices, especially media, when travelling or upon returning from travelling.	Agency Responsibility	The Agency is responsible for developing and enforcing a mobile device usage policy in relation to the Blueprint.	N/A
1088	4	Oct-19	O	P	S	TS	Personnel report the potential compromise of mobile devices, media or credentials to their organisation as soon as possible, especially if they: ▪ provide credentials, decrypt devices or have devices taken out of sight by foreign government officials ▪ have devices or media stolen that are later returned ▪ loose devices or media that are later found ▪ observe unusual behaviour of devices.	Agency Responsibility	The Agency is responsible for developing and enforcing a mobile device usage policy in relation to the Blueprint.	N/A
1300	4	Oct-19	O	P	S	TS	Upon returning from travelling overseas with mobile devices, personnel take the following actions: ▪ sanitise and reset devices, including all media used with them ▪ decommission any physical credentials that left their possession during their travel ▪ report if significant doubt exists as to the integrity of any devices following their travel.	Agency Responsibility	The Agency is responsible for developing and enforcing a mobile device usage policy in relation to the Blueprint.	N/A
1556	0	Oct-19	O	P	S	TS	If returning from travelling overseas with mobile devices to high/extreme risk countries, personnel take the following additional actions: ▪ reset user credentials used with devices, including those used for remote access to their organisation's systems ▪ monitor accounts for any indicators of compromise, such as failed login attempts.	Agency Responsibility	The Agency is responsible for developing and enforcing a mobile device usage policy in relation to the Blueprint.	N/A

Guidelines for Evaluated Products

Evaluated product acquisition

0280	7	Sep-19	O	P	S	TS	If procuring an evaluated product, a product that has completed a PP-based evaluation is selected in preference to one that has completed an EAL-based evaluation.	Implemented	The Blueprint includes Windows 10 which has been evaluated against the relevant Protection Profile. Additionally, the Blueprint leverages Office 365 services which include evaluated products.	DTA - Blueprint System Security Plan Common Criteria Evaluation for Microsoft Windows 10 and Windows Server Version 1903 (May 2019 Update) 2019 Microsoft Office 365 IRAP Assessment Report
0285	1	Sep-18	O	P	S	TS	Evaluated products are delivered in a manner consistent with any delivery procedures defined in associated evaluation documentation.	Implemented	Windows 10 installation media is sourced directly from Microsoft in accordance with the evaluated delivery procedures. The use of evaluated products by Office 365 is detailed in the IRAP assessment report.	DTA - Blueprint System Security Plan Common Criteria Evaluation for Microsoft Windows 10 and Windows Server Version 1903 (May 2019 Update) 2019 Microsoft Office 365 IRAP Assessment Report
0286	5	Sep-18	O	P	S	TS	When procuring high assurance ICT equipment, the ACSC is contacted for any equipment-specific delivery procedures.	Not Applicable	The Blueprint, Office 365 and Azure do not include the use of high assurance products.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report

Evaluated product usage

0289	2	Sep-18	O	P	S	TS	Evaluated products are installed, configured, administered and operated in accordance with vendor guidance and evaluation documentation.	Implemented	Windows 10 is managed by Microsoft Intune in accordance with the published guidance from Microsoft as well the ACSC's hardening guide for Windows 10. The use of evaluated products by Office 365 is detailed in the IRAP assessment report.	DTA - Blueprint System Security Plan Common Criteria Evaluation for Microsoft Windows 10 and Windows Server Version 1903 (May 2019 Update) 2019 Microsoft Office 365 IRAP Assessment Report
0290	5	Sep-18	O	P	S	TS	High assurance ICT equipment is installed, configured, administered and operated in accordance with guidance produced by the ACSC.	Not Applicable	The Blueprint, Office 365 and Azure do not include the use of high assurance products.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
0292	5	Sep-18	O	P	S	TS	High assurance ICT equipment is only operated in an evaluated configuration.	Not Applicable	The Blueprint, Office 365 and Azure do not include the use of high assurance products.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report

Guidelines for ICT Equipment Management

ICT equipment usage

1551	0	Aug-19	O	P	S	TS	An ICT equipment management policy is developed and implemented.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
0293	4	Sep-18	O	P	S	TS	ICT equipment is classified based on the highest sensitivity or classification of information that it is approved for processing, storing or communicating.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
0294	4	Sep-18	O	P	S	TS	ICT equipment, with the exception of high assurance ICT equipment, is labelled with protective markings reflecting its sensitivity or classification.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
0296	4	Sep-18	O	P	S	TS	The Australian Cyber Security Centre (ACSC)'s approval is sought before applying labels to external surfaces of high assurance ICT equipment.	Not Applicable	The Blueprint, Office 365 and Azure do not include the use of high assurance products.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report

ICT equipment maintenance and repairs

1079	4	Sep-18	O	P	S	TS	The ACSC's approval is sought before undertaking any repairs to high assurance ICT equipment.	Not Applicable	The Blueprint, Office 365 and Azure do not include the use of high assurance products.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
0305	5	Oct-19	O	P	S	TS	Maintenance and repairs of ICT equipment is carried out on-site by an appropriately cleared technician.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
0307	2	Sep-18	O	P	S	TS	If an uncleared technician is used to undertake maintenance or repairs of ICT equipment, the ICT equipment and associated media is sanitised before maintenance or repair work is undertaken.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
0306	4	Sep-18	O	P	S	TS	If an uncleared technician is used to undertake maintenance or repairs of ICT equipment, the technician is escorted by someone who: ▪ is appropriately cleared and briefed ▪ takes due care to ensure that information is not disclosed ▪ takes all responsible measures to ensure the integrity of the ICT equipment ▪ has the authority to direct the technician ▪ is sufficiently familiar with the ICT equipment to understand the work being performed.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
0310	4	Sep-18	O	P	S	TS	ICT equipment maintained or repaired off-site is done so in accordance with the physical transfer and storage requirements for the sensitivity or classification of the ICT equipment.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
0944	4	Sep-18	O	P	S	TS	ICT equipment maintained or repaired off-site is treated as per the requirements for the sensitivity or classification of the area that the ICT equipment will be returned to.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A

ICT equipment sanitisation and disposal

0313	4	Aug-19	O	P	S	TS	An ICT equipment sanitisation process, and supporting ICT equipment sanitisation procedures, is developed and implemented.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
1550	0	Aug-19	O	P	S	TS	An ICT equipment disposal process, and supporting ICT equipment disposal procedures, is developed and implemented.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
0311	5	Sep-18	O	P	S	TS	When disposing of ICT equipment containing media, the ICT equipment is sanitised by sanitising the media within the ICT equipment, removing the media from the ICT equipment or destroying the ICT equipment in its entirety.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A

1217	1	Sep-18	O	P	S	TS	Labels and markings indicating the classification, codewords, caveats, owner, system, network, or any other marking that can associate the ICT equipment with its original use, are removed prior to disposal.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
0316	2	Sep-18	O	P	S	TS	Following sanitisation, destruction or declassification, a formal administrative decision is made to handle ICT equipment, or its waste, as 'publicly releasable' before it is released into the public domain.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
0315	5	Sep-18	O	P	S	TS	If disposing of high assurance ICT equipment or TEMPEST-rated ICT equipment, the ACSC is contacted for requirements relating to its secure disposal.	Not Applicable	The Blueprint, Office 365 and Azure do not include the use of high assurance products.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
1218	2	Oct-19	-	-	S	TS	ICT equipment, including associated media, that is located overseas and has processed or stored AUSTEO or AGAO information is sanitised in situ.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0312	4	Sep-18	-	-	S	TS	ICT equipment, including associated media, that is located overseas and has processed or stored AUSTEO or AGAO information that cannot be sanitised in situ is returned to Australia for destruction.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0317	3	Sep-18	O	P	S	TS	At least three pages of random text with no blank areas are printed on each colour printer cartridge or MFD print drum.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
1219	1	Sep-18	O	P	S	TS	MFD print drums and image transfer rollers are inspected and destroyed if there is remnant toner which cannot be removed or if a print is visible on the image transfer roller.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
1220	1	Sep-18	O	P	S	TS	Printer and MFD platens are inspected and destroyed if any images are retained on the platen.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
1221	1	Sep-18	O	P	S	TS	Printers and MFDs are checked to ensure no pages are trapped in the paper path due to a paper jam.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
0318	3	Sep-18	O	P	S	TS	When unable to sanitise printer cartridges or MFD print drums, they are destroyed as per electrostatic memory devices.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
1534	0	Sep-18	O	P	S	TS	Printer ribbons in printers and MFDs are removed and destroyed.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
1076	2	Sep-18	O	P	S	TS	Televisions and computer monitors with minor burn-in or image persistence are sanitised by displaying a solid white image on the screen for an extended period of time.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
1222	1	Sep-18	O	P	S	TS	Televisions and computer monitors that cannot be sanitised are destroyed.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
1223	3	Mar-19	O	P	S	TS	Memory in network devices is sanitised using the following processes, in order of preference: ▪ following device-specific guidance provided by the ACSC ▪ following vendor sanitisation guidance ▪ if guidance is unavailable, performing a full reset and loading of a dummy configuration file.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
1225	2	Sep-18	O	P	S	TS	The paper tray of the fax machine is removed, and a fax message with a minimum length of four pages is transmitted, before the paper tray is re-installed to allow a fax summary page to be printed.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A
1226	2	Sep-18	O	P	S	TS	Fax machines are checked to ensure no pages are trapped in the paper path due to a paper jam.	Agency Responsibility	The Agency is responsible for the management of ICT equipment used in relation to the Blueprint.	N/A

Guidelines for Media Management

Media usage

1549	0	Aug-19	O	P	S	TS	A media management policy is developed and implemented.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
1359	3	Aug-19	O	P	S	TS	A removable media usage policy is developed and implemented.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0323	5	Feb-19	O	P	S	TS	Media is classified to the highest sensitivity or classification of information stored on the media.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0325	5	Mar-19	O	P	S	TS	Any media connected to a system is classified as the same sensitivity or classification as the system, unless the media is read-only, the media is inserted into a read-only device or the system has a mechanism through which read-only access can be ensured.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0331	5	Sep-18	O	P	S	TS	Media is reclassified if information copied onto the media is of a higher sensitivity or classification than the information already on the media, or information stored on the media is subject to a classification upgrade.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0330	3	Sep-18	O	P	S	TS	If reclassifying media to a lower sensitivity or classification, the reclassification of all information on the media has been approved by the originator, or the media has been appropriately sanitised/destroyed and a formal administrative decision has been made to reclassify it.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0332	4	Sep-18	O	P	S	TS	Media, with the exception of internally mounted fixed media within ICT equipment, is labelled with protective markings reflecting its sensitivity or classification.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0337	4	Sep-18	O	P	S	TS	Media is not used with systems that are not authorised to process, store or communicate the sensitivity or classification of information on it.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A

0341	3	Sep-18	O	P	S	TS	Any automatic execution features for media are disabled in the operating system of systems.	Implemented	Autorun is disabled for removable media via Intune policies.	DTA - Platform ABAC
0342	5	Sep-18	O	P	S	TS	Unauthorised media is prevented from connecting to systems via the use of device access control software, disabling connection ports, or by physical means.	Implemented	Only authorised devices that are whitelisted in Intune policies can be connected to endpoints. Unauthorised devices will not be mounted to the operating system.	DTA - Platform ABAC
0343	4	Sep-18	O	P	S	TS	Media is prevented from being written to via the use of device access control software if there is no business requirement for its use.	Implemented	Only authorised devices that are whitelisted in Intune policies can be connected to endpoints. Unauthorised devices will not be mounted to the operating system.	DTA - Platform ABAC
0345	4	Sep-18	O	P	S	TS	External interface connections that allow DMA are disabled.	Implemented	External connections relying on DMA will be disabled via Intune policies	DTA - Platform ABAC
0831	5	Sep-18	O	P	S	TS	Media is handled in a manner suitable for its sensitivity or classification.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
1059	3	Sep-18	O	P	S	TS	Media is encrypted with at least an Australian Signals Directorate Approved Cryptographic Algorithm.	Implemented	Removable media is encrypted via BitLocker using AES-256.	DTA - Platform ABAC
0347	4	Sep-18	O	P	S	TS	When transferring data manually between two systems belonging to different security domains, write-once media is used.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
Media sanitisation										
0348	3	Aug-19	O	P	S	TS	A media sanitisation process, and supporting media sanitisation procedures, is developed and implemented.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0351	5	Sep-18	O	P	-	-	Volatile media is sanitised by removing power from the media for at least 10 minutes or by overwriting all locations on the media with a random pattern followed by a read back for verification.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0352	3	Sep-18	-	-	S	TS	Volatile media is sanitised by overwriting the media at least once in its entirety with a random pattern, followed by a read back for verification, and then followed by removing power from the media for at least 10 minutes.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0835	3	Sep-18	-	-	-	TS	Following sanitisation, highly classified volatile media retains its classification if it stored static data for an extended period of time, or had data repeatedly stored on or written to the same memory location for an extended period of time.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1065	2	Sep-18	O	P	S	TS	The host-protected area and device configuration overlay table of non-volatile magnetic media is reset prior to sanitisation.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0354	5	Sep-18	O	P	S	TS	Non-volatile magnetic media is sanitised by booting from separate media to the media being sanitised and then overwriting the media at least once (or three times if pre-2001 or under 15 Gigabytes) in its entirety with a random pattern followed by a read back for verification.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
1067	3	Sep-18	O	P	S	TS	The ATA secure erase command is used where available, in addition to using block overwriting software, to ensure the growth defects table (g-list) is overwritten.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0356	5	Sep-18	-	-	S	TS	Following sanitisation, highly classified non-volatile magnetic media retains its classification.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0357	4	Sep-18	O	P	S	TS	Non-volatile EPROM media is sanitised by erasing the media in accordance with the manufacturer's specification, increasing the specified ultraviolet erasure time by a factor of three, then overwriting the media at least once in its entirety with a random pattern followed by a read back for verification.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0836	2	Sep-18	O	P	S	TS	Non-volatile EEPROM media is sanitised by overwriting the media at least once in its entirety with a random pattern followed by a read back for verification.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0358	5	Sep-18	-	-	S	TS	Following sanitisation, highly classified non-volatile EPROM and EEPROM media retains its classification.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0359	3	Sep-18	O	P	S	TS	Non-volatile flash memory media is sanitised by overwriting the media at least twice in its entirety with a random pattern followed by a read back for verification.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0360	5	Sep-18	-	-	S	TS	Following sanitisation, highly classified non-volatile flash memory media retains its classification.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0947	4	Sep-18	O	P	S	TS	All media is sanitised prior to reuse.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
1464	1	Sep-18	O	P	S	TS	Where a Consumer Guide for evaluated encryption software exists, the sanitisation and post-sanitisation requirements stated in the Consumer Guide are followed.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
Media destruction										
0363	2	Aug-19	O	P	S	TS	A media destruction process, and supporting media destruction procedures, is developed and implemented.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0350	4	Sep-18	O	P	S	TS	The following media types are destroyed prior to disposal as they cannot be sanitised: ▪ microfiche and microfilm ▪ optical discs ▪ programmable read-only memory ▪ read-only memory ▪ other types of media that cannot be sanitised ▪ faulty media that cannot be successfully sanitised.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A

1361	1	Sep-18	O	P	S	TS	SCEC or ASIO approved equipment is used when destroying media.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
1160	1	Sep-18	O	P	S	TS	If using degaussers to destroy media, degaussers evaluated by the United States' National Security Agency or certified by the United Kingdom's National Cyber Security Centre are used.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
1517	0	Sep-18	O	P	S	TS	Equipment that is capable of reducing microform to a fine powder, with resultant particles not showing more than five consecutive characters per particle upon microscopic inspection, is used to destroy microfiche and microfilm.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0366	2	Sep-18	O	P	S	TS	One of the methods in the following table is used to destroy media. (See source document for referenced table)	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0368	6	Sep-18	O	P	S	TS	The resulting waste for all destruction methods, except for furnace/incinerator and degausser, is stored and handled as per the following table. (See source document for referenced table)	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0361	3	Sep-18	O	P	S	TS	A degausser of sufficient field strength for the coercivity of the magnetic media is used, with the field strength being checked at regular intervals.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0838	2	Sep-18	O	P	S	TS	A degausser capable of the magnetic orientation (longitudinal or perpendicular) of the magnetic media is used.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0362	3	Sep-18	O	P	S	TS	Any product-specific directions provided by degausser manufacturers are followed.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0370	4	Sep-18	O	P	S	TS	The destruction of media is performed under the supervision of at least one person cleared to the sensitivity or classification of the media being destroyed.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0371	3	Sep-18	O	P	S	TS	Personnel supervising the destruction of media supervise the handling of the media to the point of destruction and ensure that the destruction is completed successfully.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0372	4	Sep-18	O	P	S	TS	The destruction of accountable material is performed under the supervision of at least two personnel cleared to the sensitivity or classification of the media being destroyed.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0373	3	Sep-18	O	P	S	TS	Personnel supervising the destruction of accountable media supervise the handling of the material to the point of destruction, ensure that the destruction is completed successfully and sign a destruction certificate afterwards.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0840	3	Sep-18	O	P	S	-	When outsourcing the destruction of media to an external destruction service, a National Association for Information Destruction AAA certified destruction service with endorsements, as specified in ASIO's PSC-167, is used.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0839	2	Sep-18	O	P	S	TS	The destruction of TOP SECRET media or accountable material is not outsourced.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A

Media disposal

0374	2	Aug-19	O	P	S	TS	A media disposal process, and supporting media disposal procedures, is developed and implemented.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0375	3	Sep-18	O	P	S	TS	Following sanitisation, destruction or declassification, a formal administrative decision is made to handle media, or its waste, as 'publicly releasable' before it is released into the public domain.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A
0378	3	Sep-18	O	P	S	TS	Labels and markings indicating the classification, codewords, caveats, owner, system, network, or any other marking that can associate media with its original use, are removed prior to disposal.	Agency Responsibility	The Agency is responsible for the management of media used in relation to the Blueprint.	N/A

Guidelines for System Hardening

Operating system hardening

1407	3	Sep-18	O	P	S	TS	The latest version (N), or N-1 version, of an operating system is used for Standard Operating Environments (SOEs).	Implemented	Windows 10 Semi-Annual Channel (SAC) is used as the SOE for the Blueprint.	DTA - Workstation Design
1408	3	Sep-18	O	P	S	TS	When developing a Microsoft Windows SOE, the 64-bit version of the operating system is used.	Implemented	The 64-bit version of Windows 10 is used as the SOE for the Blueprint.	DTA - Workstation Design
1409	1	Sep-18	O	P	S	TS	ACSC and vendor guidance is implemented to assist in hardening the configuration of operating systems.	Partially Implemented	The Windows 10 SOE has been hardened in accordance with ACSC guidance where possible using Intune. The specific recommendations from the ACSC guidance that cannot be implemented are documented in the SSP.	DTA - Workstation Design DTA - Platform Design DTA - Blueprint System Security Plan
0383	6	Sep-18	O	P	S	TS	Default operating system accounts are disabled, renamed or have their passphrase changed.	Implemented	The default administrator and guest accounts have been disabled and renamed.	DTA - Workstation Design
0380	7	Sep-18	O	P	S	TS	Unneeded operating system accounts, software, components, services and functionality are removed or disabled.	Implemented	Only required software and components are included in the SOE. Default accounts are disabled.	DTA - Workstation Design
1491	0	Sep-18	O	P	S	TS	Standard users are prevented from running all script execution engines shipped with Microsoft Windows including Windows Script Host (cscript.exe and wscript.exe), powershell.exe, powershell_ise.exe, cmd.exe, wmic.exe and Microsoft HTML Application Host (mshta.exe).	Partially Implemented	Intune policies prevent standard users from running cmd.exe and only executing signed PowerShell scripts.	DTA - Workstation Design
1410	1	Sep-18	O	P	S	TS	Local administrator accounts are disabled; alternatively, passphrases that are random and unique for each device's local administrator account are used.	Implemented	The default administrator and guest accounts have been disabled and renamed.	DTA - Workstation Design

1469	1	Sep-18	O	P	S	TS	Unique domain accounts with local administrative privileges, but without domain administrative privileges, are used for workstation and server management.	Implemented	RBAC policy defines separate domain and local administrator roles.	DTA - Workstation Design	
0382	5	Sep-18	O	P	S	TS	Users do not have the ability to install, uninstall or disable software.	Implemented	Standard users do not have permissions to install or uninstall software.	DTA - Workstation Design	
0843	7	Sep-18	O	P	S	TS	An application whitelisting solution is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set.	Implemented	Windows Defender Application Control (WDAC) provides application whitelisting functionality.	DTA - Workstation Design	Application Whitelisting
1490	1	Jul-19	O	P	S	TS	An application whitelisting solution is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set.	Not Applicable	The Blueprint does not include servers.	N/A	Application Whitelisting
0955	5	Sep-18	O	P	S	TS	Application whitelisting is implemented using cryptographic hash rules, publisher certificate rules or path rules.	Implemented	A combination of hash, publisher certificate and path rules will be used.	DTA - Workstation Design	
1471	1	Sep-18	O	P	S	TS	When implementing application whitelisting using publisher certificate rules, both publisher names and product names are used.	Implemented	Both publisher and product names are used.	DTA - Workstation Design	
1392	1	Sep-18	O	P	S	TS	When implementing application whitelisting using path rules, file system permissions are configured to prevent unauthorised modification of folder and file permissions, folder contents (including adding new files) and individual files that are approved to execute.	Implemented	File permissions prevent standard users from writing to locations that are whitelisted using path rules.	DTA - Workstation Design	
1544	0	Jul-19	O	P	S	TS	Microsoft's latest recommended block rules are implemented to prevent application whitelisting bypasses.	Implemented	Microsoft's recommended block rules to prevent known WDAC bypasses are implemented.	DTA - Workstation Design	Application Whitelisting
0846	6	Sep-18	O	P	S	TS	All users (with the exception of privileged users when performing specific administrative activities) cannot disable, bypass or be exempted from application whitelisting mechanisms.	Implemented	Standard users cannot disable application whitelisting.	DTA - Workstation Design	
0957	5	Sep-18	O	P	S	TS	Application whitelisting solutions are configured to generate event logs for failed execution attempts, including information such as the name of the blocked file, the date/time stamp and the username of the user attempting to execute the file.	Implemented	WDAC writes to the local event log.	DTA - Workstation Design	
1414	1	Sep-18	O	P	S	TS	If supported, the latest version of Microsoft's EMET is implemented on workstations and servers and configured with both operating system mitigation measures and application-specific mitigation measures.	Not Applicable	EMET is not supported by the latest release of Windows 10.	N/A	
1492	0	Sep-18	O	P	S	TS	If supported, Microsoft's 'Exploit protection' functionality is implemented on workstations and servers.	Implemented	The 'Exploit protection' feature is enabled as part of the Blueprint Windows 10 SOE.	DTA - Workstation Design	
1341	2	Sep-18	O	P	S	TS	A HIPS is implemented on workstations.	Implemented	Windows Defender Exploit Guard and Defender ATP provide HIPS functionality as part of the Blueprint Windows 10 SOE.	DTA - Workstation Design	
1034	6	Sep-18	O	P	S	TS	A HIPS is implemented on high value servers such as authentication servers, Domain Name System (DNS) servers, web servers, file servers and email servers.	Not Applicable	The Blueprint does not include servers.	N/A	
1416	2	Sep-18	O	P	S	TS	A software firewall is implemented on workstations and servers to limit both inbound and outbound network connections.	Implemented	Windows Defender Firewall is enabled as part of the Blueprint Windows 10 SOE.	DTA - Workstation Design	
1417	2	Sep-18	O	P	S	TS	Antivirus software is implemented on workstations and servers and configured with: ▪ signature-based detection enabled and set to a high level ▪ heuristic-based detection enabled and set to a high level ▪ detection signatures checked for currency and updated on at least a daily basis ▪ automatic and regular scanning configured for all fixed disks and removable media.	Implemented	Defender Antivirus and Defender ATP provide antivirus including signature and heuristic-based detection.	DTA - Workstation Design	
1390	2	Sep-18	O	P	-	-	Antivirus software has reputation rating functionality enabled.	Implemented	Reputation rating features are enabled.	DTA - Workstation Design	
1418	1	Sep-18	O	P	S	TS	Endpoint device control software is implemented on workstations and servers to prevent unauthorised devices from being used.	Implemented	Intune provides device whitelisting.	DTA - Workstation Design	

Application hardening

0938	4	Sep-18	O	P	S	TS	Applications are chosen from vendors that have made a commitment to secure development and maintenance practices.	Implemented	All applications are supplied by Microsoft which has made a commitment to secure development. The Blueprint does not include any third party applications.	2019 Microsoft Azure IRAP Assessment Report 2019 Microsoft Office 365 IRAP Assessment Report	
1467	1	Sep-18	O	P	S	TS	The latest releases of key business applications such as office productivity suites, PDF viewers, web browsers, common web browser plugins, email clients and software platforms are used when present within SOEs.	Implemented	The latest version of Microsoft Office 365 is installed. No third-party applications are installed.	DTA - Workstation Design	
1483	0	Sep-18	O	P	S	TS	The latest releases of web server software, server applications that store important data, and other internet-accessible server applications are used when present within SOEs.	Not Applicable	The Blueprint does not include server software.	N/A	
1412	2	Feb-19	O	P	S	TS	ACSC and vendor guidance is implemented to assist in hardening the configuration of Microsoft Office, web browsers and PDF viewers.	Implemented	ACSC guidance has been implemented to harden Office and built-in web browsers.	DTA - Workstation Design	
1484	1	Jan-19	O	P	S	TS	Web browsers are configured to block or disable support for Flash content.	Implemented	Flash is blocked in both Edge and Internet Explorer.	DTA - Platform Design	User Application Hardening
1485	0	Sep-18	O	P	S	TS	Web browsers are configured to block web advertisements.	Partially Implemented	Flash and Java-based web advertisements are blocked in Edge and Internet Explorer.	DTA - Platform Design	User Application Hardening
1486	0	Sep-18	O	P	S	TS	Web browsers are configured to block Java from the Internet.	Implemented	Java is blocked in both Edge and Internet Explorer.	DTA - Platform Design	User Application Hardening
1541	0	Jan-19	O	P	S	TS	Microsoft Office is configured to disable support for Flash content.	Implemented	Support for Flash content is disabled by default.	DTA - Platform Design	User Application Hardening
1542	0	Jan-19	O	P	S	TS	Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.	Implemented	OLE is blocked for Microsoft Office.	DTA - Platform Design	User Application Hardening

1470	3	Mar-19	O	P	S	TS	Any unrequired functionality in Microsoft Office, web browsers and PDF viewers is disabled.	Implemented	Unrequired functionality, such as Microsoft Access, has been removed.	DTA - Platform Design	
1235	2	Apr-19	O	P	S	TS	The use of Microsoft Office, web browser and PDF viewer add-ons is restricted to organisation approved add-ons.	Implemented	The use of add-ons is restricted to Microsoft-provided add-ons only.	DTA - Office 365 Design	
1487	0	Sep-18	O	P	S	TS	Microsoft Office macros are only allowed to execute in documents from Trusted Locations where write access is limited to personnel whose role is to vet and approve macros.	Implemented	Only signed macros are enabled	DTA - Workstation Design	Configure Microsoft Office Macro Settings
1488	0	Sep-18	O	P	S	TS	Microsoft Office macros in documents originating from the Internet are blocked.	Implemented	All macros downloaded from the internet are disabled.	DTA - Workstation Design	Configure Microsoft Office Macro Settings
1489	0	Sep-18	O	P	S	TS	Microsoft Office macro security settings cannot be changed by users.	Implemented	Users cannot change macro settings.	DTA - Workstation Design	Configure Microsoft Office Macro Settings
Authentication hardening											
1546	0	Aug-19	O	P	S	TS	Users are authenticated before they are granted access to a system and its resources.	Implemented	Azure AD requires all users to be authenticated before granting access.	DTA - Workstation Design DTA - Platform Design DTA - Office 365 Design	
0974	5	Sep-18	O	P	S	TS	Multi-factor authentication is used to authenticate standard users.	Implemented	Azure MFA is enforced for standard users.	DTA - Platform Design	
1173	3	Mar-19	O	P	S	TS	Multi-factor authentication is used to authenticate all privileged users and any other positions of trust.	Implemented	Azure MFA is enforced for privileged users.	DTA - Platform Design	Multi-Factor Authentication
1504	0	Sep-18	O	P	S	TS	Multi-factor authentication is used to authenticate all users of remote access solutions.	Not Applicable	The Blueprint does not include remote access.	N/A	Multi-Factor Authentication
1505	0	Sep-18	O	P	S	TS	Multi-factor authentication is used to authenticate all users when accessing important data repositories.	Implemented	Azure MFA is enforced for all users accessing Office 365 content.	DTA - Platform Design	Multi-Factor Authentication
1401	4	Oct-19	O	P	S	TS	Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics or smartcards.	Partially Implemented	MFA requires complex password and OTP from Microsoft Authenticator App (soft token).	DTA - Platform Design	Multi-Factor Authentication
1559	0	Oct-19	O	P	-	-	Passwords used for multi-factor authentication are a minimum of 6 characters.	Implemented	Azure AD password complexity enforces a minimum character length of 14 characters.	DTA - Workstation Design	
1560	0	Oct-19	-	-	S	-	Passwords used for multi-factor authentication are a minimum of 8 characters.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A	
1561	0	Oct-19	-	-	-	TS	Passwords used for multi-factor authentication are a minimum of 10 characters.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A	
1357	1	Sep-18	O	P	S	TS	When multi-factor authentication is implemented, none of the authentication factors on their own can be used for single-factor authentication to another system.	Implemented	None of the authentication factors on their own can be used for single-factor authentication to another system.	DTA - Workstation Design	
0417	5	Oct-19	O	P	S	TS	When systems cannot support multi-factor authentication, single-factor authentication using passphrases is implemented instead.	Not Applicable	Azure MFA is enforced for all users accessing Office 365 content.	DTA - Platform Design	
0421	5	Oct-19	O	P	-	-	Passphrases used for single-factor authentication are a minimum of 14 characters with complexity, ideally as 4 random words.	Implemented	Azure AD password complexity enforces a minimum character length of 14 characters.	DTA - Workstation Design	
1557	0	Oct-19	-	-	S	-	Passphrases used for single-factor authentication are a minimum of 17 characters with complexity, ideally as 5 random words.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A	
0422	5	Oct-19	-	-	-	TS	Passphrases used for single-factor authentication are a minimum of 20 characters with complexity, ideally as 6 random words.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A	
1558	0	Oct-19	O	P	S	TS	Passphrases used for single-factor authentication: ▪ are not constructed from song lyrics, movies, literature or any other publically available material ▪ do not form a real sentence in a natural language ▪ are not a list of categorised words.	Not Applicable	Azure MFA is enforced for all users accessing Office 365 content.	DTA - Platform Design	
1403	2	Oct-19	O	P	S	TS	Accounts are locked out after a maximum of five failed logon attempts.	Implemented	Azure AD Smart Lockout is configured to lock account after five failed logon attempts.	DTA - Platform ABAC	
0431	2	Sep-18	O	P	S	TS	Repeated account lockouts are investigated before reauthorising access.	Agency Responsibility	The Agency is responsible for investigating repeated lockouts.	N/A	
0976	5	Oct-19	O	P	S	TS	Users provide sufficient evidence to verify their identity when requesting a password/passphrase reset.	Implemented	Azure AD self-service password reset requires users to verify their identity before resetting their password.	DTA - Platform Design	
1227	3	Oct-19	O	P	S	TS	Password/passphrase resets are random for each individual reset, not reused when resetting multiple accounts, and not based on another identifying factor such as the user's name or the date.	Implemented	Azure AD self-service password reset enforcing the Azure AD password complexity requirements.	DTA - Platform Design	
1055	3	Oct-19	O	P	S	TS	LAN Manager is disabled for password/passphrase authentication.	Implemented	LAN Manger is not used by the Blueprint.	DTA - Workstation Design	
0418	4	Oct-19	O	P	S	TS	Credentials are stored separately from systems to which they grant access.	Implemented	Credentials are stored within Azure AD.	DTA - Platform Design	
1402	2	Oct-19	O	P	S	TS	Credentials are protected by ensuring: ▪ passwords/passphrases expire every 12 months ▪ passwords/passphrases are stored as salted hashes ▪ password/passphrase stretching is implemented ▪ password/passwords appearing in breach databases are blacklisted ▪ passwords/passphrases are never sent in the clear across networks.	Implemented	Credentials are stored within Azure AD. Azure AD Identity Protection is enabled to detected leaked passwords.	DTA - Platform Design	

0428	6	Sep-18	O	P	S	TS	Systems are configured with a session or screen lock that: ▪ activates after a maximum of 15 minutes of user inactivity or if manually activated by the user ▪ completely conceals all information on the screen ▪ ensures that the screen does not enter a power saving state before the screen or session lock is activated ▪ requires the user to reauthenticate to unlock the system ▪ denies users the ability to disable the session or screen locking mechanism.	Implemented	The Blueprint Windows 10 SOE is configured with a screen saver after 15 minutes which requires users to re-authenticate.	DTA - Workstation Design	
0408	4	Sep-18	O	P	S	TS	Systems have a logon banner that requires users to acknowledge and accept their security responsibilities before access is granted.	Implemented	The Blueprint Windows 10 SOE is configured with a logon banner provided by the Agency.	DTA - Workstation Design	
0979	4	Sep-18	O	P	S	TS	Legal advice is sought on the exact wording of logon banners.	Implemented	The Blueprint Windows 10 SOE is configured with a logon banner provided by the Agency.	DTA - Workstation Design	

Guidelines for System Management

System administration

0042	4	Aug-19	O	P	S	TS	A system administration process, with supporting system administration procedures, is developed and implemented.	Implemented	The Blueprint includes a system administration SOP.	DTA - Blueprint Standard Operating Procedures	
1380	4	Oct-19	O	P	S	TS	Privileged users use a dedicated administrator workstation when performing privileged tasks.	Not Implemented	Privileged access workstations are not in scope of the Blueprint.	N/A	
1382	2	Sep-18	O	P	S	TS	Privileged users are assigned an unprivileged administration account for authenticating to their dedicated administrator workstations.	Not Implemented	Privileged access workstations are not in scope of the Blueprint.	N/A	
1381	2	Sep-18	O	P	S	TS	Dedicated administrator workstations used for privileged tasks are prevented from communicating to assets not related to administrative activities.	Not Implemented	Privileged access workstations are not in scope of the Blueprint.	N/A	
1383	2	Sep-18	O	P	S	TS	All administrative infrastructure including, but not limited to, administrator workstations and jump servers are hardened.	Not Implemented	Privileged access workstations are not in scope of the Blueprint.	N/A	
1384	2	Sep-18	O	P	S	TS	Multi-factor authentication is used to authenticate users each time they perform privileged actions.	Implemented	Azure MFA is enforced for all privileged users.	DTA - Platform Design	
1385	2	Sep-18	O	P	S	TS	Administrator workstations are placed into a separate network zone to user workstations.	Not Implemented	Privileged access workstations are not in scope of the Blueprint.	N/A	
1386	4	Oct-19	O	P	S	TS	Management traffic is only allowed to originate from network zones that are used to administer systems and applications.	Not Implemented	Privileged access workstations are not in scope of the Blueprint.	N/A	
1387	1	Sep-18	O	P	S	TS	All administrative actions are conducted through a jump server.	Not Implemented	Jump servers are not in scope of the Blueprint.	N/A	
1388	1	Sep-18	O	P	S	TS	Jump servers are prevented from communicating to assets and sending and receiving traffic not related to administrative activities.	Not Implemented	Jump servers are not in scope of the Blueprint.	N/A	

System patching

1143	7	Aug-19	O	P	S	TS	A patch management process, and supporting patch management procedures, is developed and implemented.	Implemented	The Blueprint includes a system administration SOP which specifically references patching.	DTA - Blueprint Standard Operating Procedures	
1493	1	Aug-19	O	P	S	TS	A software register, including versions and patch histories of applications, drivers, operating systems and firmware for workstations, servers, mobile devices, network devices and all other ICT equipment, is maintained and regularly audited.	Implemented	All configurations are included in the relevant ABAC.	DTA - Windows 10 - ABAC	
1144	9	Sep-18	O	P	S	TS	Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.	Implemented	Application and driver patches will be automatically deployed via Intune for the Blueprint Windows 10 SOE.	DTA - Platform Design	Patch Applications
0940	8	Sep-18	O	P	S	TS	Security vulnerabilities in applications and drivers assessed as high risk are patched, updated or mitigated within two weeks of the security vulnerability being identified by vendors, independent third parties, system managers or users.	Implemented	Application and driver patches will be automatically deployed via Intune for the Blueprint Windows 10 SOE.	DTA - Platform Design	
1472	1	Sep-18	O	P	S	TS	Security vulnerabilities in applications and drivers assessed as moderate or low risk are patched, updated or mitigated within one month of the security vulnerability being identified by vendors, independent third parties, system managers or users.	Implemented	Application and driver patches will be automatically deployed via Intune for the Blueprint Windows 10 SOE.	DTA - Platform Design	
1494	0	Sep-18	O	P	S	TS	Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.	Implemented	Operating system patches will be automatically deployed via Intune for the Blueprint Windows 10 SOE. The Agency is responsible for any firmware patching dependent on the specific hardware model chosen by them.	DTA - Platform Design	Patch Operating Systems
1495	0	Sep-18	O	P	S	TS	Security vulnerabilities in operating systems and firmware assessed as high risk are patched, updated or mitigated within two weeks of the security vulnerability being identified by vendors, independent third parties, system managers or users.	Implemented	Operating system patches will be automatically deployed via Intune for the Blueprint Windows 10 SOE. The Agency is responsible for any firmware patching dependent on the specific hardware model chosen by them.	DTA - Platform Design	
1496	0	Sep-18	O	P	S	TS	Security vulnerabilities in operating systems and firmware assessed as moderate or low risk are patched, updated or mitigated within one month of the security vulnerability being identified by vendors, independent third parties, system managers or users.	Implemented	Operating system patches will be automatically deployed via Intune for the Blueprint Windows 10 SOE. The Agency is responsible for any firmware patching dependent on the specific hardware model chosen by them.	DTA - Platform Design	
0300	6	Sep-18	-	-	S	TS	High assurance ICT equipment is only patched with patches approved by the ACSC using methods and timeframes prescribed by the ACSC.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A	

0298	7	Oct-19	O	P	S	TS	A centralised and managed approach is used to patch or update applications and drivers.	Implemented	Intune provides a centralised and managed approach to patching.	DTA - Platform Design	
0303	6	Sep-18	O	P	S	TS	An approach for patching or updating applications and drivers that ensures the integrity and authenticity of patches or updates, as well as the processes used to apply them, is used.	Implemented	Windows Update verifies the integrity of patches before installing them.	DTA - Platform Design	
1497	0	Sep-18	O	P	S	TS	An automated mechanism is used to confirm and record that deployed application and driver patches or updates have been installed, applied successfully and remain in place.	Implemented	Intune provides a centralised and managed approach to patching.	DTA - Platform Design	Patch Applications
1498	1	Oct-19	O	P	S	TS	A centralised and managed approach is used to patch or update operating systems and firmware.	Implemented	Intune provides a centralised and managed approach to patching.	DTA - Platform Design	
1499	0	Sep-18	O	P	S	TS	An approach for patching or updating operating systems and firmware that ensures the integrity and authenticity of patches or updates, as well as the processes used to apply them, is used.	Implemented	Windows Update verifies the integrity of patches before installing them.	DTA - Platform Design	
1500	0	Sep-18	O	P	S	TS	An automated mechanism is used to confirm and record that deployed operating system and firmware patches or updates have been installed, applied successfully and remain in place.	Implemented	Intune provides a centralised and managed approach to patching.	DTA - Platform Design	Patch Operating Systems
0304	5	Sep-18	O	P	S	TS	Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Not Applicable	All applications included in the Blueprint are vendor-supported versions.	DTA - Windows 10 ABAC	Patch Applications
1501	0	Sep-18	O	P	S	TS	Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.	Not Applicable	All operating systems included in the Blueprint are vendor-supported versions.	DTA - Windows 10 ABAC	Patch Operating Systems
Change management											
1211	2	Aug-19	O	P	S	TS	A change management process, and supporting change management procedures, is developed and implemented covering: ▪ identification and documentation of requests for change ▪ approval required for changes to be made ▪ implementation and testing of approved changes ▪ the maintenance of system and security documentation.	Agency Responsibility	The Agency is responsible for change management activities related to the Blueprint.	N/A	
Data backup and restoration											
1510	1	Aug-19	O	P	S	TS	A digital preservation policy is developed and implemented.	Agency Responsibility	The Agency is responsible for developing and implementing a digital preservation policy.	N/A	
1547	0	Aug-19	O	P	S	TS	A data backup process, and supporting data backup procedures, is developed and implemented.	Agency Responsibility	The Agency is responsible for backup and restoration of data and configurations stored in the Blueprint.	N/A	
1548	0	Aug-19	O	P	S	TS	A data restoration process, and supporting data restoration procedures, is developed and implemented.	Agency Responsibility	The Agency is responsible for backup and restoration of data and configurations stored in the Blueprint.	N/A	
1511	0	Sep-18	O	P	S	TS	Backups of important information, software and configuration settings are performed at least daily.	Agency Responsibility	The Agency is responsible for backup and restoration of data and configurations stored in the Blueprint.	N/A	Daily Backups
1512	0	Sep-18	O	P	S	TS	Backups are stored offline, or online but in a non-rewritable and non-erasable manner.	Agency Responsibility	The Agency is responsible for backup and restoration of data and configurations stored in the Blueprint.	N/A	Daily Backups
1513	0	Sep-18	O	P	S	TS	Backups are stored at a multiple geographically-dispersed locations.	Agency Responsibility	The Agency is responsible for backup and restoration of data and configurations stored in the Blueprint.	N/A	
1514	0	Sep-18	O	P	S	TS	Backups are stored for three months or greater.	Agency Responsibility	The Agency is responsible for backup and restoration of data and configurations stored in the Blueprint.	N/A	Daily Backups
1515	1	Jul-19	O	P	S	TS	Full restoration of backups is tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.	Agency Responsibility	The Agency is responsible for backup and restoration of data and configurations stored in the Blueprint.	N/A	Daily Backups
1516	1	Jul-19	O	P	S	TS	Partial restoration of backups is tested on a quarterly or more frequent basis.	Agency Responsibility	The Agency is responsible for backup and restoration of data and configurations stored in the Blueprint.	N/A	Daily Backups
Guidelines for System Monitoring											
Event logging and auditing											
0580	6	Aug-19	O	P	S	TS	An event logging policy is developed and implemented.	Agency Responsibility	The Agency is responsible for developing and implementing an event logging policy.	N/A	
1405	1	Sep-18	O	P	S	TS	A centralised logging facility is implemented and systems are configured to save event logs to the centralised logging facility as soon as possible after each event occurs.	Partially Implemented	Defender ATP and Office ATP centralise logs relating to the security of devices and Office services.	DTA - Platform Design	
0988	5	Sep-18	O	P	S	TS	An accurate time source is established and used consistently across systems and network devices to assist with the correlation of events.	Implemented	Windows Time is used as the time source for all Blueprint components.	DTA - Workstation Design	
0584	2	Sep-18	O	P	S	TS	For any system requiring authentication, logon, failed logon and logoff events are logged.	Implemented	Azure AD logs authentication events to Log Analytics.	DTA - Platform Design	

0582	5	Sep-18	O	P	S	TS	The following events are logged for operating systems: ▪ access to important data and processes ▪ application crashes and any error messages ▪ attempts to use special privileges ▪ changes to accounts ▪ changes to security policy ▪ changes to system configurations ▪ Domain Name System (DNS) and Hypertext Transfer Protocol requests ▪ failed attempts to access data and system resources ▪ service failures and restarts ▪ system startup and shutdown ▪ transfer of data to external media ▪ user or group management ▪ use of special privileges.	Implemented	These events are logged to the local event log on each Windows 10 endpoint.	DTA - Workstation Design
1536	0	Sep-18	O	P	S	TS	The following events are logged for web applications: ▪ attempted access that is denied ▪ crashes and any error messages ▪ search queries initiated by users.	Not Applicable	The Blueprint does not includes web applications.	N/A
1537	0	Sep-18	O	P	S	TS	The following events are logged for databases: ▪ access to particularly important information ▪ addition of new users, especially privileged users ▪ any query containing comments ▪ any query containing multiple embedded queries ▪ any query or database alerts or failures ▪ attempts to elevate privileges ▪ attempted access that is successful or unsuccessful ▪ changes to the database structure ▪ changes to user roles or database permissions ▪ database administrator actions ▪ database logons and logoffs ▪ modifications to data ▪ use of executable commands.	Not Applicable	The Blueprint does not include databases.	N/A
0585	4	Sep-18	O	P	S	TS	For each event logged, the date and time of the event, the relevant user or process, the event description, and the ICT equipment involved are recorded.	Implemented	Logs include the described meta-data.	DTA - Platform Design
0586	4	Sep-18	O	P	S	TS	Event logs are protected from unauthorised access, modification and deletion.	Implemented	Logs stored in Log Analytics are protected from unauthorised access, modification and deletion by the Azure AD RBAC model. Standard Windows 10 users to do have access to modify the local event logs.	DTA - Platform Design DTA - Workstation Design
0859	2	Sep-18	O	P	S	TS	Event logs are retained for a minimum of 7 years in accordance with the National Archives of Australia's **Administrative Functions Disposal Authority** publication.	Not Implemented	Logs are only stored in Log Analytics for 2 years. Local event logs on Windows 10 devices will be lost when endpoints are rebuilt.	DTA - Platform Design DTA - Workstation Design
0991	4	Sep-18	O	P	S	TS	DNS and proxy logs are retained for at least 18 months.	Not Applicable	The Blueprint does not provide DNS or proxy services.	N/A
0109	6	Aug-19	O	P	S	TS	An event log auditing process, and supporting event log auditing procedures, is developed and implemented covering the scope and schedule of audits, what constitutes a violation of security policy, and actions to be taken when violations are detected, including reporting requirements.	Agency Responsibility	The Agency is responsible for developing and implementing an event logging policy.	N/A
1228	2	Sep-18	O	P	S	TS	Events are correlated across event logs to prioritise audits and focus investigations.	Agency Responsibility	The Agency is responsible for developing and implementing an event logging policy.	N/A
Vulnerability management										
1163	3	Aug-19	O	P	S	TS	A vulnerability management policy is developed and implemented that includes: ▪ conducting vulnerability assessments and penetration tests for systems throughout their life cycle to identify security vulnerabilities ▪ analysing identified security vulnerabilities to determine their potential impact and appropriate mitigations based on effectiveness, cost and existing security controls ▪ using a risk-based approach to prioritise the implementation of identified mitigations.	Agency Responsibility	The Agency is responsible for developing and implementing a vulnerability management policy.	N/A
0911	6	Sep-18	O	P	S	TS	Vulnerability assessments and penetration tests are conducted by suitably skilled personnel before a system is deployed, after a significant change to a system, and at least annually or as specified by the system owner.	Agency Responsibility	The Agency is responsible for developing and implementing a vulnerability management policy.	N/A
Guidelines for Software Development										
Application development										
0400	4	Sep-18	O	P	S	TS	Software development, testing and production environments are segregated.	Not Applicable	The Blueprint is not designed to support software development activities.	N/A
1419	1	Sep-18	O	P	S	TS	Development and modification of software only takes place in development environments.	Not Applicable	The Blueprint is not designed to support software development activities.	N/A

1420	2	Sep-18	O	P	S	TS	Information in production environments is not used in testing or development environments unless the testing or development environments are secured to the same level as the production environments.	Not Applicable	The Blueprint is not designed to support software development activities.	N/A
1422	3	Sep-18	O	P	S	TS	Unauthorised access to the authoritative source for software is prevented.	Not Applicable	The Blueprint is not designed to support software development activities.	N/A
1238	3	Sep-18	O	P	S	TS	Threat modelling and other secure design techniques are used to ensure that threats to software and mitigations to those threats are identified and accounted for.	Not Applicable	The Blueprint is not designed to support software development activities.	N/A
0401	4	Oct-19	O	P	S	TS	Platform-specific secure programming practices are used when developing software, including using the lowest privilege needed to achieve a task, checking return values of all system calls, validating all inputs and encrypting all communications.	Not Applicable	The Blueprint is not designed to support software development activities.	N/A
0402	3	Sep-18	O	P	S	TS	Software is tested for security vulnerabilities by software developers, as well as an independent party, before it is used in a production environment.	Not Applicable	The Blueprint is not designed to support software development activities.	N/A

Web application development

1239	3	Sep-18	O	P	S	TS	Robust web application frameworks are used to aid in the development of secure web applications.	Not Applicable	The Blueprint is not designed to support software development activities.	N/A
1552	0	Oct-19	O	P	S	TS	All web application content is offered exclusively using HTTPS.	Not Applicable	The Blueprint is not designed to support software development activities.	N/A
1240	2	Sep-18	O	P	S	TS	Validation and/or sanitisation is performed on all input handled by a web application.	Not Applicable	The Blueprint is not designed to support software development activities.	N/A
1241	3	Sep-18	O	P	S	TS	Output encoding is performed on all output produced by a web application.	Not Applicable	The Blueprint is not designed to support software development activities.	N/A
1424	3	Oct-19	O	P	S	TS	Web applications implement Content-Security-Policy, HSTS and X-Frame-Options response headers.	Not Applicable	The Blueprint is not designed to support software development activities.	N/A
0971	7	Apr-19	O	P	S	TS	The OWASP ***Application Security Verification Standard*** is followed when developing web applications.	Not Applicable	The Blueprint is not designed to support software development activities.	N/A

Guidelines for Database Systems Management

Database servers

1425	1	Sep-18	O	P	S	TS	Hard disks of database servers are encrypted using full disk encryption.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1269	2	Sep-18	O	P	S	TS	Database servers and web servers are functionally separated, physically or virtually.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1277	2	Sep-18	O	P	S	TS	Information communicated between database servers and web applications is encrypted.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1270	2	Sep-18	O	P	S	TS	Database servers that require network connectivity are placed on a different network segment to an organisation's workstations.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1271	1	Sep-18	O	P	S	TS	Network access controls are implemented to restrict database servers' communications to strictly defined network resources such as web servers, application servers and storage area networks.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1272	1	Sep-18	O	P	S	TS	If only local access to a database is required, networking functionality of database management system (DBMS) software is disabled or directed to listen solely to the localhost interface.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1273	2	Sep-18	O	P	S	TS	Test and development environments do not use the same database servers as production environments.	Not Applicable	The Blueprint does not include the use of databases.	N/A

Database management system software

1245	2	Sep-18	O	P	S	TS	All temporary installation files and logs are removed after DBMS software has been installed.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1246	2	Sep-18	O	P	S	TS	DBMS software is configured according to vendor guidance.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1247	2	Sep-18	O	P	S	TS	DBMS software features, stored procedures, accounts and databases that are not required are disabled or removed.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1249	2	Sep-18	O	P	S	TS	DBMS software is configured to run as a separate account with the minimum privileges needed to perform its functions.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1250	1	Sep-18	O	P	S	TS	The account under which DBMS software runs has limited access to non-essential areas of the database server's file system.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1251	2	Sep-18	O	P	S	TS	The ability of DBMS software to read local files from a server is disabled.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1260	2	Sep-18	O	P	S	TS	Default database administrator accounts are disabled, renamed or have their passphrases changed.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1262	1	Sep-18	O	P	S	TS	Database administrators have unique and identifiable accounts.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1261	2	Sep-18	O	P	S	TS	Database administrator accounts are not shared across different databases.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1263	2	Sep-18	O	P	S	TS	Database administrator accounts are used exclusively for administrative tasks, with standard database accounts used for general purpose interactions with databases.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1264	1	Sep-18	O	P	S	TS	Database administrator access is restricted to defined roles rather than accounts with default administrative permissions, or all permissions.	Not Applicable	The Blueprint does not include the use of databases.	N/A

Databases

1243	4	Aug-19	O	P	S	TS	A database register is maintained and regularly audited.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1256	3	Sep-18	O	P	S	TS	File-based access controls are applied to database files.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1252	3	Jun-19	O	P	S	TS	Passphrases stored in databases are hashed with a uniquely salted Australian Signals Directorate Approved Cryptographic Algorithm.	Not Applicable	The Blueprint does not include the use of databases.	N/A

0393	7	Apr-19	O	P	S	TS	Databases and their contents are classified based on the sensitivity or classification of information that they contain.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1255	3	Sep-18	O	P	S	TS	Database users' ability to access, insert, modify and remove content in databases is restricted based on their work duties.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1268	1	Sep-18	O	P	S	TS	The need-to-know principle is enforced for database contents through the application of minimum privileges, database views and database roles.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1258	1	Sep-18	O	P	S	TS	Where concerns exist that the sum, or aggregation, of separate pieces of information from within databases could lead to a database user determining more sensitive or classified information, database views in combination with database user access roles are implemented.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1274	4	Sep-18	O	P	S	TS	Information in production databases is not used in testing or development databases unless the testing or development environments are secured to the same level as the production environment.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1275	1	Sep-18	O	P	S	TS	All queries to databases from web applications are filtered for legitimate content and correct syntax.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1276	2	Sep-18	O	P	S	TS	Parameterised queries or stored procedures are used for database interaction instead of dynamically generated queries.	Not Applicable	The Blueprint does not include the use of databases.	N/A
1278	2	Sep-18	O	P	S	TS	Web applications are designed to provide as little error information as possible to users about database schemas.	Not Applicable	The Blueprint does not include the use of databases.	N/A

Guidelines for Email Management

Email usage

0264	3	Aug-19	O	P	S	TS	An email usage policy is developed and implemented.	Agency Responsibility	The Agency is responsible for developing and implementing an email usage policy.	N/A
0267	7	Mar-19	O	P	S	TS	Access to non-approved webmail services is blocked.	Agency Responsibility	The Blueprint does not include a proxy services and therefore non-approved webmail services are not blocked. If an Agency's risk profile requires a proxy service, the DTA recommend the use of a certified Secure Internet Gateway (SIG) provider.	N/A
0270	5	Mar-19	O	P	S	TS	Protective markings are applied to emails and reflect the information in their subject, body and attachments.	Implemented	The Blueprint applies protective markings based on the classification of the content of emails, including attachments.	DTA - Office 365 Design DTA - Office 365 ABAC
0271	3	Mar-19	O	P	S	TS	Protective marking tools do not automatically insert protective markings into emails.	Implemented	Users are required to select the classification of emails to apply protective markings.	DTA - Office 365 Design DTA - Office 365 ABAC
0272	4	Mar-19	O	P	S	TS	Protective marking tools do not allow users to select protective markings that a system has not been authorised to process, store or communicate.	Implemented	Only appropriate classification options will be presented to Blueprint users.	DTA - Office 365 Design DTA - Office 365 ABAC
1089	4	Mar-19	O	P	S	TS	Protective marking tools do not allow users replying to or forwarding an email to select a protective marking that is lower than previously used for the email.	Implemented	Users are prevented from lowering the classification of emails.	DTA - Office 365 Design DTA - Office 365 ABAC
0565	4	Mar-19	O	P	S	TS	Email servers are configured to block, log and report emails with inappropriate protective markings.	Agency Responsibility	The Agency is responsible for ensuring their email gateway implements this control.	N/A
1023	5	Mar-19	O	P	S	TS	The intended recipients of any blocked inbound emails, and the sender of any blocked outbound emails, are notified.	Implemented	Office 365 ATP will notify users and administrators of blocked emails.	DTA - Office 365 ABAC
0269	2	Sep-18	-	-	S	TS	Emails containing AUSTEO or AGAO information are only sent to named recipients and not to groups or distribution lists unless the nationality of all members of the distribution lists can be confirmed.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1539	2	Aug-19	-	P	S	TS	Emails containing REL information are only sent to named recipients and not to groups or distribution lists unless the nationality of all members of the distribution lists can be confirmed.	Not Applicable	is not designed to process, store or communicate REL information.	N/A

Email gateways and servers

0569	3	Sep-18	O	P	S	TS	Email is routed through a centralised email gateway.	Implemented	Exchange Online is configured to route through the Agency's existing email gateway.	DTA - Office 365 Design
0571	5	Mar-19	O	P	S	TS	When users send email from outside their network, an authenticated and encrypted channel is configured to allow email to be routed via a centralised email gateway.	Implemented	Email traffic between external users and Exchange Online is encrypted with TLS 1.2. Exchange Online then forwards emails to the Agency's existing email gateway via an Exchange connector.	DTA - Office 365 Design
0570	4	Sep-18	O	P	S	TS	Where backup or alternative email gateways are in place, they are maintained at the same standard as the primary email gateway.	Agency Responsibility	The Agency is responsible for any backup or alternative email gateways.	N/A
0567	4	Mar-19	O	P	S	TS	Email servers only relay emails destined for or originating from their domains.	Implemented	Exchange Online is not configured to act as an open relay.	DTA - Office 365 Design
0572	3	Sep-18	O	P	S	TS	Opportunistic TLS encryption, as defined in IETF RFC 3207, is enabled on email servers that make incoming or outgoing email connections over public network infrastructure.	Implemented	Exchange Online implements TLS 1.2.	DTA - Office 365 Design
0574	4	Oct-19	O	P	S	TS	SPF is used to specify authorised email services (or lack thereof) for all domains.	Implemented	SPF is configured in Exchange Online.	DTA - Office 365 Design

1183	1	Sep-18	O	P	S	TS	A hard fail SPF record is used when specifying email servers.	Implemented	SPF is configured in Exchange Online using a hard fail record.	DTA - Office 365 ABAC
1151	3	Oct-19	O	P	S	TS	SPF is used to verify the authenticity of incoming emails.	Implemented	SPF is configured in Exchange Online.	DTA - Office 365 Design
1152	3	Mar-19	O	P	S	TS	Incoming emails that fail SPF checks are blocked or marked in a manner that is visible to the recipients.	Implemented	SPF blocks are visible to the recipients.	DTA - Office 365 ABAC
0861	2	Mar-19	O	P	S	TS	DKIM signing is enabled on emails originating from an organisation's domains.	Implemented	DKIM is configured in Exchange Online.	DTA - Office 365 Design
1026	4	Sep-18	O	P	S	TS	DKIM signatures on received emails are verified, taking into account that email distribution list software typically invalidates DKIM signatures.	Implemented	DKIM signatures on received emails are verified.	DTA - Office 365 Design
1027	4	Sep-18	O	P	S	TS	Email distribution list software used by external senders is configured such that it does not break the validity of the sender's DKIM signature.	Implemented	DKIM is configured in Exchange Online.	DTA - Office 365 ABAC
1540	1	Oct-19	O	P	S	TS	DMARC records are configured for all domains such that emails are rejected if they fail SPF or DKIM checks.	Implemented	DMARC records are configured in Exchange Online.	DTA - Office 365 Design
1234	3	Mar-19	O	P	S	TS	Email content filtering controls are implemented for email bodies and attachments.	Implemented	Office 365 ATP provides content filtering including sandboxing of attachments (Smart Attachments) and inspection of links (Smart Links).	DTA - Office 365 Design
1502	1	Mar-19	O	P	S	TS	Emails arriving via an external connection where the source address uses an internal domain name are blocked at the email gateway.	Agency Responsibility	This control should be configured at the Agency's email gateway.	N/A
1024	4	Sep-18	O	P	S	TS	Notification of undeliverable, bounced or blocked emails are only sent to senders that can be verified via SPF or other trusted means.	Agency Responsibility	This control should be configured at the Agency's email gateway.	N/A

Guidelines for Network Management

Network design and configuration

0516	4	Sep-18	O	P	S	TS	Network documentation includes a high-level network diagram showing all connections into the network; a logical network diagram showing all network devices, critical servers and services; and the configuration of all network devices.	Implemented	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The Office 365 design includes a high level network diagram showing the components that are considered in scope.	DTA - Office 365 Design
0518	4	Sep-18	O	P	S	TS	Network documentation is updated as network configuration changes are made and includes a 'current as at [date]' or equivalent statement.	Implemented	The Office 365 design which includes the high level network design has a document control table listing the last update date.	DTA - Office 365 Design
1178	3	Sep-18	O	P	S	TS	Network documentation provided to a third party, or published in public tender documentation, only contains details necessary for other parties to undertake contractual services.	Agency Responsibility	The agency is responsible for the distribution of information to third parties if required.	N/A
1181	3	Sep-18	O	P	S	TS	Networks are divided into multiple functional network zones according to the sensitivity or criticality of information or services.	Agency Responsibility	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The agency is responsible for the management of network devices used in relation to the Blueprint.	N/A
1532	1	Aug-19	O	P	S	TS	VLANs are not used to separate network traffic between official or classified networks and public network infrastructure.	Agency Responsibility	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The agency is responsible for the management of network devices used in relation to the Blueprint.	N/A
0529	5	Sep-18	O	P	S	TS	VLANs are not used to separate network traffic between official and classified networks, or networks of different classifications.	Agency Responsibility	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The agency is responsible for the management of network devices used in relation to the Blueprint.	N/A
1364	2	Sep-18	O	P	S	TS	VLANs belonging to different security domains are terminated on separate physical network interfaces.	Agency Responsibility	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The agency is responsible for the management of network devices used in relation to the Blueprint.	N/A
0535	5	Sep-18	O	P	S	TS	VLANs belonging to official and classified networks, or networks of different classifications, do not share VLAN trunks.	Agency Responsibility	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The agency is responsible for the management of network devices used in relation to the Blueprint.	N/A
0530	5	Sep-18	O	P	S	TS	Network devices implementing VLANs are managed from the most trusted network.	Agency Responsibility	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The agency is responsible for the management of network devices used in relation to the Blueprint.	N/A

0521	5	Sep-18	O	P	S	TS	IPv6 functionality is disabled in dual-stack network devices and ICT equipment unless it is being used.	Agency Responsibility	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The agency is responsible for the management of network devices used in relation to the Blueprint.	N/A
1186	3	Sep-18	O	P	S	TS	IPv6 capable network security devices are used on IPv6 and dual-stack networks.	Agency Responsibility	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The agency is responsible for the management of network devices used in relation to the Blueprint.	N/A
1428	1	Sep-18	O	P	S	TS	Unless explicitly required, IPv6 tunnelling is disabled on all network devices and ICT equipment.	Agency Responsibility	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The agency is responsible for the management of network devices used in relation to the Blueprint.	N/A
1429	1	Sep-18	O	P	S	TS	IPv6 tunnelling is blocked by network security devices at externally connected network boundaries.	Agency Responsibility	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The agency is responsible for the management of network devices used in relation to the Blueprint.	N/A
1430	1	Sep-18	O	P	S	TS	Dynamically assigned IPv6 addresses are configured with Dynamic Host Configuration Protocol version 6 in a stateful manner with lease information stored in a centralised logging facility.	Agency Responsibility	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The agency is responsible for the management of network devices used in relation to the Blueprint.	N/A
0520	6	Sep-18	O	P	S	TS	Network access controls are implemented on networks to prevent the connection of unauthorised network devices.	Agency Responsibility	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The agency is responsible for the management of network devices used in relation to the Blueprint.	N/A
1182	3	Sep-18	O	P	S	TS	Network access controls are implemented to limit traffic within and between network segments to only those that are required for business purposes.	Agency Responsibility	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The agency is responsible for the management of network devices used in relation to the Blueprint.	N/A
1301	2	Aug-19	O	P	S	TS	A network device register is maintained and regularly audited.	Agency Responsibility	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The agency is responsible for the management of network devices used in relation to the Blueprint.	N/A
1304	2	Sep-18	O	P	S	TS	Default accounts for network devices are disabled, renamed or have their passphrase changed.	Agency Responsibility	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The agency is responsible for the management of network devices used in relation to the Blueprint.	N/A
0534	2	Sep-18	O	P	S	TS	Unused physical ports on network devices are disabled.	Agency Responsibility	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The agency is responsible for the management of network devices used in relation to the Blueprint.	N/A
0385	6	Sep-18	O	P	S	TS	Servers maintain effective functional separation with other servers allowing them to operate independently.	Not Applicable	The Blueprint does not include servers.	N/A
1479	0	Sep-18	O	P	S	TS	Servers minimise communications with other servers at both the network and file system level.	Not Applicable	The Blueprint does not include servers.	N/A
1460	1	Sep-18	O	P	S	TS	When using a software-based isolation mechanism to share a physical server's hardware: ▪ the isolation mechanism is from a vendor that uses secure coding practices and, when security vulnerabilities have been identified, develops and distributes patches in a timely manner ▪ the configuration of the isolation mechanism is hardened by removing unneeded functionality and restricting access to the administrative interface used to manage the isolation mechanism ▪ the underlying operating system running on the server is hardened ▪ patches are applied to the isolation mechanism and underlying operating system in a timely manner ▪ integrity and log monitoring are performed for the isolation mechanism and underlying operating system in a timely manner.	Not Applicable	The Blueprint does not include servers.	N/A

1462	1	Jul-19	-	P	-	-	When using a software-based isolation mechanism to share a physical server's hardware, the physical server and all computing environments running on the physical server are of the same classification.	Not Applicable	The Blueprint does not include servers.	N/A
1461	2	Jul-19	-	-	S	TS	When using a software-based isolation mechanism to share a physical server's hardware, the physical server and all computing environments running on the physical server are controlled by the same organisation, are of the same classification and are within the same security domain.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1006	6	Sep-18	O	P	S	TS	Security measures are implemented to prevent unauthorised access to network management traffic.	Agency Responsibility	The Blueprint is designed to run using the public internet. All security controls are implemented on the endpoint devices and the Office 365 component. The agency is responsible for the management of network devices used in relation to the	N/A
1311	2	Sep-18	O	P	S	TS	SNMP version 1 and 2 are not used on networks.	Not Applicable	The Blueprint does not include the use of SNMP.	N/A
1312	2	Sep-18	O	P	S	TS	All default SNMP community strings on network devices are changed and have write access disabled.	Not Applicable	The Blueprint does not include the use of SNMP.	N/A
1028	6	Sep-18	O	P	S	TS	NIDS or NIPS are deployed in all gateways between an organisation's networks and other networks they do not manage, including public network infrastructure.	Agency Responsibility	The Agency is responsible for implementing security controls within their email gateway.	N/A
1030	6	Sep-18	O	P	S	TS	NIDS or NIPS in gateways are located immediately inside the outermost firewall and configured to generate a log entry, and an alert, for any information flows that contravene any rule in firewall rule sets.	Agency Responsibility	The Agency is responsible for implementing security controls within their email gateway.	N/A
1185	3	Sep-18	O	P	S	TS	When deploying NIDS or NIPS in non-internet gateways, they are configured to monitor unusual patterns of behaviour or traffic flows rather than internet-based communication protocol signatures.	Agency Responsibility	The Agency is responsible for implementing security controls within their email gateway.	N/A
Wireless networks										
1314	1	Sep-18	O	P	S	TS	All wireless access points are Wi-Fi Alliance certified.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
0536	6	Sep-18	O	P	S	TS	Wireless networks provided for the general public to access are segregated from all other networks.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1315	2	Sep-18	O	P	S	TS	The administrative interface on wireless access points is disabled for wireless network connections.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1316	2	Sep-18	O	P	S	TS	The default SSID of wireless access points is changed.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1317	2	Sep-18	O	P	S	TS	The SSID of a non-public wireless network is not readily associated with an organisation, the location of their premises or the functionality of the wireless network.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1318	2	Sep-18	O	P	S	TS	SSID broadcasting is enabled on wireless networks.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1319	2	Sep-18	O	P	S	TS	Static addressing is not used for assigning IP addresses on wireless networks.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1320	2	Sep-18	O	P	S	TS	MAC address filtering is not used to restrict which devices can connect to wireless networks.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1321	1	Sep-18	O	P	S	TS	WPA2-Enterprise with EAP-TLS is used to perform mutual authentication for wireless networks.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1322	3	Aug-19	O	P	S	TS	Evaluated supplicants, authenticators and authentication servers are used in wireless networks.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1324	3	Aug-19	O	P	S	TS	Certificates are generated using an evaluated certificate authority solution or hardware security module.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1323	2	Sep-18	O	P	S	TS	Both device and user certificates are required for accessing wireless networks.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1325	1	Sep-18	O	P	S	TS	Both device and user certificates for accessing wireless networks are not stored on the same device.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1326	2	Sep-18	O	P	S	TS	User certificates for accessing wireless networks are issued on smart cards with access PINs.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A

1327	1	Sep-18	O	P	S	TS	User or device certificates stored on devices accessing wireless networks are protected by encryption.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1330	1	Sep-18	O	P	S	TS	The PMK caching period is not set to greater than 1440 minutes (24 hours).	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1454	1	Sep-18	O	P	S	TS	Communications between wireless access points and a RADIUS server are encapsulated with an additional layer of encryption.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1332	2	Aug-19	O	P	S	TS	ASD approved cryptography is used to protect the confidentiality and integrity of all wireless network traffic.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1334	2	Sep-18	O	P	S	TS	Wireless networks implement sufficient frequency separation from other wireless networks.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1335	1	Sep-18	O	P	S	TS	Wireless access points enable the use of the 802.11w amendment to protect management frames.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1338	1	Sep-18	O	P	S	TS	Instead of deploying a small number of wireless access points that broadcast on high power, a greater number of wireless access points that use less broadcast power are deployed to achieve the desired footprint.	Agency Responsibility	The Blueprint does not provide a wireless network. The Agency is responsible for the management of wireless network devices used in relation to the Blueprint.	N/A
1013	5	Sep-18	-	-	S	TS	The effective range of wireless communications outside an organisation's area of control is limited by implementing RF shielding on buildings in which wireless networks are used.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
Service continuity for online services										
1458	1	Sep-18	O	P	-	-	The functionality and quality of online services, how to maintain such functionality, and what functionality can be lived without during a denial-of-service attack, are determined and documented.	Agency Responsibility	The Blueprint does not host online services. The Agency is responsible for the procurement and management of online services.	N/A
1431	1	Sep-18	O	P	-	-	Denial-of-service attack prevention and mitigation strategies are discussed with service providers, specifically: ▪ their capacity to withstand denial-of-service attacks ▪ any costs likely to be incurred by customers resulting from denial-of-service attacks ▪ thresholds for notifying customers or turning off their online services during denial-of-service attacks ▪ pre-approved actions that can be undertaken during denial-of-service attacks ▪ denial-of-service attack prevention arrangements with upstream providers to block malicious traffic as far upstream as possible.	Agency Responsibility	The Blueprint does not host online services. The Agency is responsible for the procurement and management of online services.	N/A
1432	1	Sep-18	O	P	-	-	Domain names for online services are protected via registrar locking and confirming domain registration details are correct.	Not Applicable	The Blueprint does not host online services.	N/A
1433	1	Sep-18	O	P	-	-	24x7 contact details are maintained for service providers and service providers maintain 24x7 contact details for their customers.	Not Applicable	The Blueprint does not host online services.	N/A
1434	1	Sep-18	O	P	-	-	Organisations and service providers provide each other with additional out-of-band contact details for use when normal communication channels fail.	Not Applicable	The Blueprint does not host online services.	N/A
1435	1	Sep-18	O	P	-	-	Availability monitoring with real-time alerting is implemented to detect denial-of-service attacks and measure their impact.	Not Applicable	The Blueprint does not host online services.	N/A
1436	1	Sep-18	O	P	-	-	Critical online services are segregated from other online services that are more likely to be targeted.	Not Applicable	The Blueprint does not host online services.	N/A
1518	0	Sep-18	O	P	-	-	A static version of a website is pre-prepared that requires minimal processing and bandwidth in order to facilitate at least a basic level of service when under a denial-of-service attack.	Not Applicable	The Blueprint does not host online services.	N/A
1437	2	Sep-18	O	P	-	-	A cloud service provider, preferably multiple different cloud service providers, is used for hosting online services.	Not Applicable	The Blueprint does not host online services.	N/A
1438	1	Sep-18	O	P	-	-	Where a high availability requirement exists for website hosting, CDNs that cache websites are used.	Not Applicable	The Blueprint does not host online services.	N/A
1439	1	Sep-18	O	P	-	-	If using a CDN, disclosing the IP address of the web server under the organisation's control (referred to as the origin server) is avoided and access to the origin server is restricted to the CDN and an authorised management network.	Not Applicable	The Blueprint does not host online services.	N/A
1441	1	Sep-18	O	P	-	-	Where a requirement for high availability exists for online services, a denial of service mitigation service is used.	Not Applicable	The Blueprint does not host online services.	N/A
Guidelines for Using Cryptography										
Cryptographic fundamentals										
1161	4	Sep-18	O	-	-	-	Encryption software that implements an ASD Approved Cryptographic Algorithm (AACA) is used if an organisation wishes to reduce the physical storage or handling requirements for ICT equipment or media that contains sensitive information.	Implemented	The Blueprint uses Microsoft BitLocker for encryption leveraging AES which is an AACA.	DTA - Workstation Design

0457	5	Sep-18	-	P	-	-	Encryption software that has completed an ACE is used if an organisation wishes to reduce the physical storage or handling requirements for ICT equipment or media that contains classified information.	Not Applicable	The Blueprint does not use encryption for the purposes of reducing the handling requirements for endpoints.	N/A
0460	8	Sep-18	-	-	S	TS	HACE is used if an organisation wishes to reduce the physical storage or handling requirements for ICT equipment or media that contains highly classified information.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0459	3	Sep-18	O	P	-	-	Encryption software used for data at rest implements full disk encryption, or partial encryption where access controls will only allow writing to the encrypted partition.	Implemented	Microsoft BitLocker provides full disk encryption of mobile devices, implementing XTS-AES-256.	DTA - Workstation Design
0461	5	Sep-18	-	-	S	TS	HACE used for data at rest implements full disk encryption, or partial encryption where access controls will only allow writing to the encrypted partition.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1080	2	Sep-18	-	-	S	TS	In addition to any encryption already in place, an AACA is used to encrypt AUSTEO and AGAO information when at rest on a system.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0455	2	Sep-18	O	P	S	TS	Where practical, cryptographic equipment and encryption software provides a means of data recovery to allow for circumstances where the encryption key is unavailable due to loss, damage or failure.	Implemented	BitLocker recovery keys are stored in Azure AD.	DTA - Workstation Design
0462	5	Sep-18	O	P	S	TS	When a user authenticates to encryption functionality for ICT equipment or media storing encrypted information, it is treated in accordance with its original sensitivity or classification until such a time that the user deauthenticates from the encryption functionality.	Agency Responsibility	The Agency is responsible for informing users of their responsibilities in relation to the management encrypted devices.	N/A
1162	3	Sep-18	O	-	-	-	Cryptographic equipment or encryption software that implements an ASD Approved Cryptographic Protocol (AACP) is used to communicate sensitive information over public network infrastructure and through unsecured spaces.	Implemented	TLS with AES is used to protect traffic to and from Azure and Office 365 servers over the internet.	DTA - Platform Design DTA - Office 365 Design
0465	6	Sep-18	-	P	-	-	Cryptographic equipment or encryption software that has completed an ACE is used to communicate classified information over official networks, public network infrastructure and through unsecured spaces.	Not Implemented	Microsoft's cryptographic software has not undergone an ACE.	2019 Microsoft Azure IRAP Assessment Report 2019 Microsoft Office 365 IRAP Assessment Report
0467	8	Sep-18	-	-	S	TS	HACE is used to communicate highly classified information over networks of a lower classification, official networks, public network infrastructure and through unsecured spaces.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0469	3	Sep-18	-	-	S	TS	In addition to any encryption already in place, an AACP is used to protect AUSTEO and AGAO information when communicated across network infrastructure.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A

ASD Approved Cryptographic Algorithms

0471	5	Sep-18	O	P	-	-	If using cryptographic equipment or software that implements an AACA, only AACAs can be used.	Implemented	Microsoft Azure and Office 365 services implement AACAs where possible.	2019 Microsoft Azure IRAP Assessment Report 2019 Microsoft Office 365 IRAP Assessment Report
0994	5	Sep-18	O	P	-	-	ECDH and ECDSA are used in preference to DH and DSA.	Implemented	Microsoft Azure and Office 365 services implement ECDHE as the preferred algorithm.	2019 Microsoft Azure IRAP Assessment Report 2019 Microsoft Office 365 IRAP Assessment Report
0472	4	Sep-18	O	P	-	-	When using DH for agreeing on encryption session keys, a modulus of at least 1024 bits, preferably 2048 bits, is used.	Not Applicable	Microsoft Azure and Office 365 services do not use DH.	2019 Microsoft Azure IRAP Assessment Report 2019 Microsoft Office 365 IRAP Assessment Report
0473	4	Sep-18	O	P	-	-	When using DSA for digital signatures, a modulus of at least 1024 bits, preferably 2048 bits, is used.	Not Applicable	Microsoft Azure and Office 365 services do not use DSA.	2019 Microsoft Azure IRAP Assessment Report 2019 Microsoft Office 365 IRAP Assessment Report
1446	1	Sep-18	O	P	-	-	When using elliptic curve cryptography, a curve from FIPS 186-4 is used.	Implemented	Microsoft Azure and Office 365 services implement NIST P-256 and P-384.	2019 Microsoft Azure IRAP Assessment Report 2019 Microsoft Office 365 IRAP Assessment Report
0474	4	Sep-18	O	P	-	-	When using ECDH for agreeing on encryption session keys, a field/key size of at least 160 bits, preferably 256 bits, is used.	Implemented	Microsoft Azure and Office 365 services use a 256 bit key where possible.	2019 Microsoft Azure IRAP Assessment Report 2019 Microsoft Office 365 IRAP Assessment Report

0475	4	Sep-18	O	P	-	-	When using ECDSA for digital signatures, a field/key size of at least 160 bits, preferably 256 bits, is used.	Implemented	Microsoft Azure and Office 365 services use a 256 bit key where possible.	2019 Microsoft Azure IRAP Assessment Report
0476	5	Sep-18	O	P	-	-	When using RSA for digital signatures, and passing encryption session keys or similar keys, a modulus of at least 1024 bits, preferably 2048 bits, is used.	Implemented	Microsoft Azure and Office 365 services use a 2048 bit key for RSA.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
0477	6	Sep-18	O	P	-	-	When using RSA for digital signatures, and for passing encryption session keys or similar keys, a key pair for passing encrypted session keys that is different from the key pair used for digital signatures is used.	Implemented	Microsoft Azure and Office 365 services use separate RSA key pairs for these purposes.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
1054	4	Sep-18	O	P	-	-	A hashing algorithm from the SHA-2 family is used instead of SHA-1.	Implemented	Microsoft Azure and Office 365 services use SHA-256 for hashing.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
0479	4	Sep-18	O	P	-	-	Symmetric cryptographic algorithms are not used in Electronic Codebook Mode.	Not Applicable	Microsoft Azure and Office 365 services do not use ECM.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
0480	6	Sep-18	O	P	-	-	3DES is used with three distinct keys.	Not Applicable	Microsoft Azure and Office 365 services do not use 3DES.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
1232	5	May-19	-	-	S	TS	AACAs are used in an evaluated implementation.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	2019 Microsoft Office 365 IRAP Assessment Report N/A
1468	5	Oct-19	-	-	S	TS	Preference is given to using the CNSA Suite algorithms and key sizes.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A

ASD Approved Cryptographic Protocols

0481	4	Sep-18	O	P	S	TS	If using cryptographic equipment or software that implements an AACP, only AACAs can be used.	Implemented	Microsoft Azure and Office 365 services implement AACAs where possible.	2019 Microsoft Azure IRAP Assessment Report 2019 Microsoft Office 365 IRAP Assessment Report

Transport Layer Security

1139	5	Oct-19	O	P	S	TS	Only the latest version of TLS is used.	Implemented	Microsoft Azure and Office 365 services implement TLS versions 1.2 and 1.3.	2019 Microsoft Azure IRAP Assessment Report 2019 Microsoft Office 365 IRAP Assessment Report
1369	2	Oct-19	O	P	S	TS	AES in Galois Counter Mode is used for symmetric encryption.	Implemented	Microsoft Azure and Office 365 services implement AES in GCM.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
1370	2	Oct-19	O	P	S	TS	Only sever-initiated secure renegotiation is used.	Implemented	Microsoft Azure and Office 365 services implement secure renegotiation.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
1372	2	Sep-18	O	P	S	TS	DH or ECDH is used for key establishment.	Implemented	Microsoft Azure and Office 365 services implement ECDHE as the preferred algorithm.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
1448	1	Sep-18	O	P	S	TS	When using DH or ECDH for key establishment, the ephemeral variant is used.	Implemented	Microsoft Azure and Office 365 services implement ECDH - Ephemeral (ECDHE) as the preferred algorithm.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report 2019 Microsoft Office 365 IRAP Assessment Report

1373	1	Sep-18	O	P	S	TS	Anonymous DH is not used.	Not Applicable	Microsoft Azure and Office 365 services do not use DH.	2019 Microsoft Azure IRAP Assessment Report
1374	2	Oct-19	O	P	S	TS	SHA-2-based certificates are used.	Implemented	Microsoft Azure and Office 365 services use SHA-2-based certificates.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
1375	3	Oct-19	O	P	S	TS	Cipher suites are configured to use SHA-2 as part of the Message Authentication Code and Pseudo-Random Function.	Implemented	Microsoft Azure and Office 365 services use SHA-2 as part of the Message Authentication Code and Pseudo-Random Function.	2019 Microsoft Office 365 IRAP Assessment Report 2019 Microsoft Azure IRAP Assessment Report
1553	0	Oct-19	O	P	S	TS	TLS compression is disabled.	Implemented	Microsoft Azure and Office 365 services disable TLS compression.	2019 Microsoft Office 365 IRAP Assessment Report N/A
1453	1	Sep-18	O	P	S	TS	PFS is used for TLS connections.	Implemented	Microsoft Azure and Office 365 services implement PFS.	2019 Microsoft Azure IRAP Assessment Report 2019 Microsoft Office 365 IRAP Assessment Report
Secure Shell										
1506	0	Sep-18	O	P	S	TS	The use of SSH version 1 is disabled.	Not Applicable	The Blueprint does not include the use of Secure Shell.	N/A
0484	4	Sep-18	O	P	S	TS	The configuration settings in the following table are implemented for the SSH daemon. (See source document for referenced table)	Not Applicable	The Blueprint does not include the use of Secure Shell.	N/A
0485	3	Sep-18	O	P	S	TS	Public key-based authentication is used for SSH connections.	Not Applicable	The Blueprint does not include the use of Secure Shell.	N/A
1449	1	Sep-18	O	P	S	TS	SSH private keys are protected with a passphrase or a key encryption key.	Not Applicable	The Blueprint does not include the use of Secure Shell.	N/A
0487	3	Sep-18	O	P	S	TS	When using logins without a passphrase for automated purposes, the following are disabled: ▪ access from IP addresses that do not require access ▪ port forwarding ▪ agent credential forwarding ▪ X11 display remoting ▪ console access.	Not Applicable	The Blueprint does not include the use of Secure Shell.	N/A
0488	3	Sep-18	O	P	S	TS	If using remote access without the use of a passphrase, the 'forced command' option is used to specify what command is executed and parameter checked is enabled.	Not Applicable	The Blueprint does not include the use of Secure Shell.	N/A
0489	4	Sep-18	O	P	S	TS	When SSH-agent or other similar key caching programs are used, it is only on workstations and servers with screen locks, key caches are set to expire within four hours of inactivity, and agent credential forwarding is enabled only when SSH traversal is required.	Not Applicable	The Blueprint does not include the use of Secure Shell.	N/A
Secure/Multipurpose Internet Mail Extension										
0490	3	Sep-18	O	P	S	TS	Versions of S/MIME earlier than 3.0 are not used.	Not Applicable	The Blueprint does not include the use of S/MIME.	N/A
Internet Protocol Security										
0494	3	Sep-18	O	P	S	TS	Tunnel mode is used for IPsec connections; however, if using transport mode, an IP tunnel is used.	Not Applicable	The Blueprint does not include the use of IPsec.	N/A
0496	4	Sep-18	O	P	S	TS	The ESP protocol is used for IPsec connections.	Not Applicable	The Blueprint does not include the use of IPsec.	N/A
1233	1	Sep-18	O	P	S	TS	IKE is used for key exchange when establishing an IPsec connection.	Not Applicable	The Blueprint does not include the use of IPsec.	N/A
0497	5	Sep-18	O	P	S	TS	If using ISAKMP in IKE version 1, aggressive mode is disabled.	Not Applicable	The Blueprint does not include the use of IPsec.	N/A
0498	3	Sep-18	O	P	S	TS	A security association lifetime of less than four hours, or 14400 seconds, is used.	Not Applicable	The Blueprint does not include the use of IPsec.	N/A
0998	4	Sep-18	O	P	S	TS	HMAC-SHA256, HMAC-SHA384 or HMAC-SHA512 is used as a HMAC algorithm.	Not Applicable	The Blueprint does not include the use of IPsec.	N/A
0999	5	Sep-18	O	P	S	TS	The largest modulus size possible for all relevant components in the network is used when conducting a key exchange.	Not Applicable	The Blueprint does not include the use of IPsec.	N/A
1000	4	Sep-18	O	P	S	TS	PFS is used for IPsec connections.	Not Applicable	The Blueprint does not include the use of IPsec.	N/A
1001	4	Sep-18	O	P	S	TS	The use of XAuth is disabled for IPsec connections using IKE version 1.	Not Applicable	The Blueprint does not include the use of IPsec.	N/A
Cryptographic system management										
0501	4	Sep-18	O	P	-	-	Keyed CGCE is transported based on the sensitivity or classification of the keying material in it.	Not Applicable	The Blueprint does not include the use of CGCE equipment.	N/A
0142	3	Jun-19	O	P	-	-	The compromise or suspected compromise of CGCE or associated keying material is reported to an organisation's Chief Information Security Officer, or one of their delegates, as soon as possible after it occurs.	Not Applicable	The Blueprint does not include the use of CGCE equipment.	N/A
1091	5	Jun-19	O	P	-	-	Keying material is changed when compromised or suspected of being compromised.	Not Applicable	The Blueprint does not include the use of CGCE equipment.	N/A
0499	8	Apr-19	-	-	S	TS	ACSI 53 E, ACSI 103 A, ACSI 105 B, ACSI 107 B, ACSI 173 A and the latest equipment-specific doctrine is complied with when using HACE.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A

0505	5	Sep-18	O	P	S	TS	Cryptographic equipment is stored in a room that meets the requirements for a server room based on the sensitivity or classification of the information the cryptographic equipment processes.	Not Applicable	The Blueprint does not include the use of CGCE equipment.	N/A
0506	3	Sep-18	-	-	S	TS	Areas in which HACE is used are separated from other areas and designated as a cryptographic controlled area.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A

Guidelines for Gateway Management

Gateways

0628	5	Mar-19	O	P	S	TS	All systems are protected from systems in other security domains by one or more gateways.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
1192	2	Sep-18	O	P	S	TS	All connections between security domains implement mechanisms to inspect and filter data flows for the transport and higher layers as defined in the OSI model.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
0631	5	Jun-19	O	P	S	TS	Gateways: ▪ are the only communications paths into and out of internal networks ▪ allow only explicitly authorised connections ▪ are managed via a secure path isolated from all connected networks (physically at the gateway or on a dedicated administration network) ▪ are protected by authentication, logging and auditing of all physical and logical access to gateway components ▪ have all security controls tested to verify their effectiveness after any changes to their configuration.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
1427	2	Jun-19	O	P	S	TS	Gateways implement ingress traffic filtering to detect and prevent Internet Protocol (IP) source address spoofing.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
0634	7	Jun-19	O	P	S	TS	All gateways connecting networks in different security domains are operated such that they: ▪ log network traffic permitted through the gateway ▪ log network traffic attempting to leave the gateway ▪ are configured to save event logs to a secure logging facility ▪ provide real-time alerts for any cyber security incidents, attempted intrusions and unusual usage patterns.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
0637	5	Sep-18	O	P	S	TS	Demilitarised zones are used to broker access to services accessed by external entities, and mechanisms are applied to mediate internal and external access to less-trusted services hosted in these demilitarised zones.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
0598	3	Sep-18	O	P	S	TS	A security risk assessment is performed on gateways and their configuration before their implementation.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
1519	0	Sep-18	O	P	S	TS	A security risk assessment is performed on all systems before they are connected to a gateway.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
0605	3	Sep-18	O	P	S	TS	All system owners of systems connected via a gateway understand and accept security risks associated with the gateway and any connected security domains, including those connected via a cascaded connection.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
1041	4	Sep-18	O	P	S	TS	The security architecture of a gateway, and security risks associated with all connected security domains, including those connected via a cascaded connection, is reviewed at least annually.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
0624	4	Sep-18	O	P	S	TS	Any associated security risk assessments are updated before changes are made to a gateway to ensure all relevant security risks have been documented and accepted.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
0625	5	Aug-19	O	P	S	TS	All changes to a gateway architecture are considered prior to implementation, documented and assessed in accordance with the organisation's change management process and supporting change management procedures.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
1037	4	Sep-18	O	P	S	TS	Gateways are subject to rigorous testing, performed at irregular intervals no more than six months apart, to determine the strength of security controls.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
0611	4	Mar-19	O	P	S	TS	Access to gateway administration functions is limited to the minimum roles and privileges to support the gateway securely.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
0612	4	Sep-18	O	P	S	TS	System administrators are formally trained to manage gateways.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
1520	0	Sep-18	O	P	S	TS	All system administrators of gateways are cleared to access the highest level of information communicated or processed by the gateway.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
0613	4	Sep-18	-	-	S	TS	All system administrators of gateways that process Australian Eyes Only (AUSTEO) or Australian Government Access Only (AGAO) information are Australian nationals.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0616	4	Oct-19	O	P	S	TS	Roles for the administration of gateways are separated.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
0629	3	Sep-18	O	P	S	TS	For gateways between networks in different security domains, a formal arrangement exists whereby any shared components are managed by the system managers of the highest security domain or by a mutually agreed third party.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
0607	3	Oct-19	O	P	S	TS	Once connectivity is established, system owners become information stakeholders for all connected security domains.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A

0619	5	Sep-18	O	P	S	TS	Users and services accessing networks through gateways are authenticated.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
0620	4	Sep-18	O	P	S	TS	Only users and services authenticated and authorised to a gateway can use the gateway.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
1039	4	Sep-18	O	P	S	TS	Multi-factor authentication is used for access to gateways.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
0622	5	Sep-18	O	P	S	TS	ICT equipment accessing networks through gateways is authenticated.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
Cross Domain Solutions										
0626	4	Sep-18	-	-	S	TS	When connecting a highly classified network to any other network from a different security domain, a CDS is implemented.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0597	6	Sep-18	-	-	S	TS	When designing and deploying a CDS, the ACSC is notified and consulted; and directions provided by the ACSC are complied with.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0627	5	Sep-18	-	-	S	TS	When introducing additional connectivity to a CDS, such as adding a new gateway to a common network, the ACSC is consulted on the impact to the security of the CDS; and directions provided by the ACSC are complied with.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0635	4	Sep-18	-	-	S	TS	All CDS between highly classified networks and any other network implement isolated upward and downward network paths.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1521	0	Sep-18	-	-	S	TS	All CDS between highly classified networks and any other network implement protocol breaks at each layer of the OSI model.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1522	0	Sep-18	-	-	S	TS	All CDS between highly classified networks and any other network implement content filtering and separate independent security-enforcing components for upward and downward data flows.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0670	4	Sep-18	-	-	S	TS	All security-relevant events generated by a CDS are logged and regularly analysed.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1523	0	Sep-18	-	-	S	TS	A representative sample of security events generated by a CDS, relating to the enforcement of data transfer policies, is taken at least every 3 months and assessed against the security policies that the CDS is responsible for enforcing between security domains.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0610	6	Apr-19	O	P	S	TS	Users are trained on the secure use of a CDS before access to the CDS is granted.	Not Applicable	The Blueprint does not include the use of CDS.	N/A
Firewalls										
1528	1	Apr-19	O	P	S	TS	An evaluated firewall is used between official or classified networks and public network infrastructure.	Not Applicable	The Blueprint does not include firewalls for the use of separating official/classified and public networks.	N/A
0639	8	Apr-19	O	P	S	TS	An evaluated firewall is used between networks belonging to different security domains.	Not Applicable	The Blueprint does not include firewalls for the use of separating official/classified and public networks.	N/A
1194	2	Sep-18	O	P	S	TS	The requirement to use a firewall as part of gateway infrastructure is met by both parties independently; shared ICT equipment does not satisfy the requirements of both parties.	Agency Responsibility	The Agency is responsible for the implementation of security controls relating to their email gateway.	N/A
0641	7	Sep-18	-	-	S	TS	In addition to the firewall between networks of different security domains, an evaluated firewall is used between an AUSTEO or AGAO network and a foreign network.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0642	7	Sep-18	-	-	S	TS	In addition to the firewall between networks of different security domains, an evaluated firewall is used between an AUSTEO or AGAO network and another Australian controlled network.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
Diodes										
0643	5	Sep-18	O	P	-	-	An evaluated diode is used for controlling the data flow of unidirectional gateways between official or classified networks and public network infrastructure.	Not Applicable	The Blueprint does not include the use of diodes.	N/A
0645	5	Sep-18	-	-	S	TS	A high assurance diode is used for controlling the data flow of unidirectional gateways between classified networks and public network infrastructure.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1157	3	Sep-18	O	P	-	-	An evaluated diode is used for controlling the data flow of unidirectional gateways between official and classified networks.	Not Applicable	The Blueprint does not include the use of diodes.	N/A
1158	4	Sep-18	O	P	S	TS	A high assurance diode is used for controlling the data flow of unidirectional gateways between official or classified networks where the highest system is SECRET or above.	Not Applicable	The Blueprint does not include the use of diodes.	N/A
0646	4	Sep-18	-	-	S	TS	An evaluated diode is used between an AUSTEO or AGAO network and a foreign network at the same classification.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0647	6	Sep-18	-	-	S	TS	An evaluated diode is used between an AUSTEO or AGAO network and another Australian controlled network at the same classification.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0648	3	Sep-18	O	P	S	TS	A diode (or server connected to the diode) deployed to control data flow in unidirectional gateways monitors the volume of the data being transferred.	Not Applicable	The Blueprint does not include the use of diodes.	N/A
Web content and connections										
0258	3	Aug-19	O	P	S	TS	A web usage policy is developed and implemented.	Agency Responsibility	The Agency is responsible for the development and implementation of a web usage policy.	N/A
0260	2	Sep-18	O	P	S	TS	All web access, including that by internal servers, is conducted through a web proxy.	Agency Responsibility	The Blueprint does not include a proxy service. If an Agency's risk profile requires a proxy service, the DTA recommend the use of a certified Secure Internet Gateway provider.	N/A

0261	4	Sep-18	O	P	S	TS	A web proxy authenticates users and provides logging that includes the following details about websites accessed: ▪ address (uniform resource locator) ▪ time/date ▪ user ▪ amount of data uploaded and downloaded ▪ internal and external IP addresses.	Agency Responsibility	The Blueprint does not include a proxy service. If an Agency's risk profile requires a proxy service, the DTA recommend the use of a certified Secure Internet Gateway provider.	N/A
0263	5	Sep-18	O	P	S	TS	If permitting TLS through internet gateways, either of the following approaches is implemented: ▪ a solution that decrypts and inspects TLS traffic as per content filtering security controls ▪ a whitelist specifying the addresses (uniform resource locators) to which encrypted connections are permitted, with all other addresses blocked or decrypted and inspected as per content filtering security controls.	Agency Responsibility	The Blueprint does not include a proxy service. If an Agency's risk profile requires a proxy service, the DTA recommend the use of a certified Secure Internet Gateway provider.	N/A
0996	5	Sep-18	O	P	S	TS	Legal advice is sought regarding the inspection of TLS traffic by internet gateways.	Agency Responsibility	The Blueprint does not include a proxy service. If an Agency's risk profile requires a proxy service, the DTA recommend the use of a certified Secure Internet Gateway provider.	N/A
0958	5	Sep-18	O	P	S	TS	Whitelisting is implemented for all Hypertext Transfer Protocol (HTTP) traffic communicated through internet gateways.	Agency Responsibility	The Blueprint does not include a proxy service. If an Agency's risk profile requires a proxy service, the DTA recommend the use of a certified Secure Internet Gateway provider.	N/A
0995	4	Sep-18	O	P	S	TS	If using a whitelist on internet gateways to specify the external addresses to which connections are permitted, it specifies whitelisted addresses by domain name or IP address.	Agency Responsibility	The Blueprint does not include a proxy service. If an Agency's risk profile requires a proxy service, the DTA recommend the use of a certified Secure Internet Gateway provider.	N/A
1170	1	Sep-18	O	P	S	TS	If websites are not whitelisted, categories are implemented for all websites and prohibited and uncategorised websites are blocked.	Agency Responsibility	The Blueprint does not include a proxy service. If an Agency's risk profile requires a proxy service, the DTA recommend the use of a certified Secure Internet Gateway provider.	N/A
0959	4	Sep-18	O	P	S	TS	If whitelisting of websites is not implemented, blacklisting of websites is implemented to prevent access to known malicious websites.	Agency Responsibility	The Blueprint does not include a proxy service. If an Agency's risk profile requires a proxy service, the DTA recommend the use of a certified Secure Internet Gateway provider.	N/A
0960	4	Sep-18	O	P	S	TS	If blacklisting websites, the blacklist is updated on a daily basis to ensure that it remains effective.	Agency Responsibility	The Blueprint does not include a proxy service. If an Agency's risk profile requires a proxy service, the DTA recommend the use of a certified Secure Internet Gateway provider.	N/A
1171	1	Sep-18	O	P	S	TS	Attempts to access a website through its IP address instead of through its domain name are blocked.	Agency Responsibility	The Blueprint does not include a proxy service. If an Agency's risk profile requires a proxy service, the DTA recommend the use of a certified Secure Internet Gateway provider.	N/A
1236	1	Sep-18	O	P	S	TS	Dynamic domains and other domains where domain names can be registered anonymously for free are blocked.	Agency Responsibility	The Blueprint does not include a proxy service. If an Agency's risk profile requires a proxy service, the DTA recommend the use of a certified Secure Internet Gateway provider.	N/A
0963	5	Sep-18	O	P	S	TS	A web content filter is used to filter potentially harmful web-based content.	Agency Responsibility	The Blueprint does not include a proxy service. If an Agency's risk profile requires a proxy service, the DTA recommend the use of a certified Secure Internet Gateway provider.	N/A
0961	5	Sep-18	O	P	S	TS	Client-side active content, such as Java, is restricted to a whitelist of approved websites which may be the same as the HTTP whitelist or a separate active content whitelist.	Agency Responsibility	The Blueprint does not include a proxy service. If an Agency's risk profile requires a proxy service, the DTA recommend the use of a certified Secure Internet Gateway provider.	N/A
1237	1	Sep-18	O	P	S	TS	Web content filtering controls are applied to outbound web traffic where appropriate.	Agency Responsibility	The Blueprint does not include a proxy service. If an Agency's risk profile requires a proxy service, the DTA recommend the use of a certified Secure Internet Gateway provider.	N/A
Peripheral switches										
0591	6	Sep-18	O	P	-	-	An evaluated peripheral switch is used when sharing peripherals between official and classified systems.	Not Applicable	The Blueprint does not include peripheral switches.	N/A
1480	0	Sep-18	O	P	S	TS	A high assurance peripheral switch is used when sharing peripherals between official or classified systems and highly classified systems.	Not Applicable	The Blueprint does not include peripheral switches.	N/A
1457	2	Sep-18	-	-	S	TS	An evaluated, preferably high assurance, peripheral switch is used when sharing peripherals between systems of different classifications.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0593	9	Apr-19	O	P	S	TS	An evaluated peripheral switch is used when sharing peripherals between official systems, or classified systems at the same classification, that belong to different security domains.	Not Applicable	The Blueprint does not include peripheral switches.	N/A

0594	4	Sep-18	-	-	S	TS	An evaluated peripheral switch is used when accessing a system containing AUSTEO or AGAO information and a system of the same classification that is not authorised to process the same caveat.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A

Guidelines for Data Transfers and Content Filtering

Data transfers

0663	5	Aug-19	O	P	S	TS	A data transfer process, and supporting data transfer procedures, is developed and implemented.	Agency Responsibility	The Agency is responsible for the development and implementation of a data transfer policy.	N/A
0661	7	Apr-19	O	P	S	TS	Users transferring data to and from a system are held accountable for the data they transfer.	Agency Responsibility	The Agency is responsible for the development and implementation of a data transfer policy.	N/A
0665	4	May-19	-	-	S	TS	Trusted sources are a strictly limited number of personnel that have been authorised as such by an organisation's CISO.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0675	3	Sep-18	-	-	S	TS	A trusted source makes an informed decision to sign all data authorised for export from a security domain.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0664	5	Sep-18	-	-	S	TS	All data transferred to a system of a lesser sensitivity or classification is reviewed and approved by a trusted source.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0657	4	Sep-18	O	P	-	-	Data imported to a system is scanned for malicious and active content.	Implemented	Defender ATP will scan all data copied onto Windows 10 devices.	Blueprint DTA - Workstation Design
0658	4	Sep-18	-	-	S	TS	Data imported to a system is scanned for malicious and active content, undergoes data format checks and logging, and is monitored to detect overuse/unusual usage patterns.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1187	1	Sep-18	O	P	-	-	When exporting data, protective marking checks are undertaken.	Not Implemented	Protective markings for documents are not implemented by the Blueprint.	N/A
0669	3	Sep-18	-	-	S	TS	When exporting data, the following activities are undertaken: ▪ protective marking checks ▪ data format checks and logging ▪ monitoring to detect overuse/unusual usage patterns ▪ limitations on data types and sizes ▪ keyword searches on all textual data.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1535	1	Aug-19	-	-	S	TS	A process, and supporting procedures, is developed and implemented to prevent AUSTEO and AGAO data in both textual and non-textual formats from being exported to foreign systems.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0678	2	Sep-18	-	-	S	TS	When exporting data from an AUSTEO or AGAO system, keyword searches are undertaken on all textual data and any identified data is quarantined until reviewed and approved for release by a trusted source other than the originator.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0667	4	Sep-18	O	P	S	TS	Data exported from each security domain, including through a gateway, is only permitted once the classification has been assessed including a protective marking check.	Not Implemented	Protective markings for documents are not implemented by the Blueprint.	N/A
0660	5	Sep-18	-	-	S	TS	When importing data to each security domain, by any means including through a gateway, the complete data transfer logs are audited at least monthly.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0673	5	Sep-18	-	-	S	TS	When exporting data out of each security domain, by any means including through a gateway, the complete data transfer logs are audited at least monthly.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1294	1	Sep-18	O	P	S	TS	When importing content to a security domain, including through a gateway, monthly audits of the imported content are performed.	Agency Responsibility	The Agency is responsible for the development and implementation of a data transfer policy.	N/A
1295	1	Sep-18	O	P	S	TS	When exporting content out of a security domain, including through a gateway, monthly audits of the exported content are performed.	Agency Responsibility	The Agency is responsible for the development and implementation of a data transfer policy.	N/A

Content filtering

0659	4	Sep-18	O	P	S	TS	When importing data into a security domain, by any means including a CDS, the data is filtered by a content filter designed for that purpose.	Partially Implemented	Exchange Online Protection and Office 365 ATP prevent specific file types from entering the system via email.	DTA - Office 365 Design
1524	0	Sep-18	-	-	S	TS	Content filters deployed in CDS are subject to rigorous security assessment to ensure they mitigate content-based threats and cannot be bypassed.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
0651	4	Sep-18	O	P	S	TS	All suspicious, malicious and active content is blocked from entering a security domain.	Partially Implemented	Exchange Online Protection and Office 365 ATP prevent malicious content from entering the system via email.	DTA - Office 365 Design
0652	2	Sep-18	O	P	S	TS	Any data identified by a content filtering process as suspicious is blocked until reviewed and approved for transfer by a trusted source other than the originator.	Partially Implemented	Exchange Online Protection and Office 365 ATP prevent malicious content from entering the system via email.	DTA - Office 365 Design
1389	1	Sep-18	O	P	S	TS	Email and web content entering a security domain is automatically run in a dynamic malware analysis sandbox to detect suspicious behaviour.	Partially Implemented	Office 365 ATP provides content filtering including sandboxing of attachments (Smart Attachments) and inspection of links (Smart Links).	DTA - Office 365 Design
1284	2	Oct-19	O	P	S	TS	Content validation is performed on all data passing through a content filter with content which fails content validation blocked.	Not Implemented	Content validation is not performed.	N/A
1286	1	Sep-18	O	P	S	TS	Content conversion is performed for all ingress or egress data transiting a security domain boundary.	Not Implemented	Content conversion is not performed.	N/A
1287	1	Sep-18	O	P	S	TS	Content sanitisation is performed on suitable file types if content conversion is not appropriate for data transiting a security domain boundary.	Not Implemented	Content sanitisation is not performed.	N/A
1288	1	Sep-18	O	P	S	TS	Antivirus scanning, using multiple different scanning engines, is performed on all content.	Implemented	Multiple scanning engines are provided by Exchange Online Protection, Office 365 ATP and Defender ATP.	DTA - Office 365 Design DTA - Workstation Design

1289	1	Sep-18	O	P	S	TS	The contents from archive/container files are extracted and subjected to content filter checks.	Implemented	Archives are scanned for malware.	DTA - Office 365 Design
1290	1	Sep-18	O	P	S	TS	Controlled inspection of archive/container files is performed to ensure that content filter performance or availability is not adversely affected.	Implemented	Archives are scanned for malware.	DTA - Workstation Design DTA - Office 365 Design
1291	1	Sep-18	O	P	S	TS	Files that cannot be inspected are blocked and generate an alert or notification.	Implemented	Office 365 ATP alerts are configured.	DTA - Workstation Design DTA - Office 365 Design
0649	4	Oct-19	O	P	S	TS	A whitelist of permitted content types is created and enforced based on business requirements and the results of a security risk assessment.	Implemented	Exchange Online Protection and Office 365 ATP prevent specific file types from entering the system via email.	DTA - Office 365 Design
1292	1	Sep-18	O	P	S	TS	The integrity of content is verified where applicable and blocked if verification fails.	Implemented	Integrity of patches is verified before installation.	DTA - Workstation Design
0677	4	Sep-18	-	-	S	TS	If data is signed, the signature is validated before the data is exported.	Not Applicable	Not applicable to OFFICIAL & PROTECTED.	N/A
1293	1	Sep-18	O	P	S	TS	All encrypted content, traffic and data is decrypted and inspected to allow content filtering.	Partially Implemented	Office 365 ATP provides content filtering including sandboxing of attachments (Smart Attachments) and inspection of links (Smart Links).	DTA - Office 365 Design