System Security Plan Documentation | Template

This template provides the content of ASD’s System Security Plan as advised on ASD’s Blueprint for Secure Cloud. Users can use their own branding. users should remove or add sections relevant to their documentation requirement. Delete this and all other pre-populated instructions from the final version of your report.

Table of Contents

# System Security Plan

| EOT |
| --- |
| **Instruction** |
| This System Security Plan (SSP) template provides a guide and resource to assist organisations in preparing a SSP describing organisational policies and processes relating to, and technical controls implemented within, system(s) built on ASD’s *Blueprint for Secure Cloud*. It provides guidance to facilitate decision-making, rather than prescriptive statements or measures, allowing organisations to tailor this document according to the controls implemented and the organisation’s context. |
| When using this template, organisations should insert and update the required information to ensure it accurately represents all relevant organisational policies, processes and technical controls. This may include organisational controls or policies that are outside of the scope of the Blueprint, but are still relevant to the system — placeholders are included where relevant throughout this template. |
| Text included in the guidance boxes throughout this template should be deleted from an organisation’s final SSP. |
| {{% download file= %}} Download the Blueprint System Security Plan Template (.docx) {{% /download %}} |

## About this System Security Plan

This System Security Plan (SSP) describes the organisational policies and processes relevant to, and technical controls implemented within the core <SYSTEM-NAME> or network that includes <ORGANISATION-NAME>’s Microsoft Workloads (Cloud and Software as a Service), endpoints and <OTHER SYSTEM COMPONENTS IN SCOPE>.

|  |
| --- |
| |  |  | | --- | --- | | ISM Version used: | June 2025 | |
|  |

## Purpose of this System Security Plan

The purpose of this SSP is to describe the organisational policies and processes relevant to, and technical controls implemented within <ORGANISATION-NAME>’s <SYSTEM-NAME>, including the underlying components leveraged in the system’s deployment. This document has been developed to comply with the Australian Signals Directorate’s (ASD’s) [*Information Security Manual’s*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism) (ISM’s) requirements in relation to documentation for system authorisation.

This document is written using descriptive and explanatory language to assist readers in understanding how <SYSTEM-NAME> operates securely, the controls implemented, and the residual controls that are addressed elsewhere by <ORGANISATION-NAME>.

For detailed information on how <SYSTEM-NAME> addresses specific controls in ASD’s ISM, please refer to the System Security Plan Annex.

# Overview

| EOT |
| --- |
| **Instruction** |
| The Overview of a System Security Plan (SSP) should provide a comprehensive overview of a system and clearly articulate its purpose, boundaries and any risks associated with operation of the system. This section should also include links to relevant documentation and outline any information or matters outside of the scope of the SSP. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their system. When complete, remove any grey instructional or blue guidance boxes throughout. |

## System information

|  |
| --- |
| | System Name | <SYSTEM-NAME> | | --- | --- | | System Classification | <SYSTEM-CLASSIFICATION> | | Operational Status | <UNDER DEVELOPMENT / IN OPERATION> | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## System purpose

| EOT |
| --- |
| **Blueprint guidance** |
| The system purpose section of an SSP should document the intended scope of implementation of the Blueprint, outlining the intended security and business value to be derived from <SYSTEM-NAME>. While the below template is a starting point to help describe a system, its scope and purpose, organisations should ensure they develop their own terminology to accurately portray the purpose and scope of their system in accordance with their requirements. |

<SYSTEM-NAME> aims to provide a scalable, multi-classified, multi-vendor platform that enables trusted external suppliers, partners, and staff to collaboratively develop and enhance our services more rapidly.

The objectives of the <SYSTEM-NAME> are to:

* Scale resources faster​
* Support the development of more innovative solutions​
* Provide faster on boarding for new staff
* Improve workplace and partner collaboration
* Assist with greater community engagement
* Enable scalable service continuity

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## System overview

<SYSTEM-NAME> is <ORGANISATION-NAME>’s implementation of a range of cloud services and applications focused on driving productivity and business outcomes and enabling <ORGANISATION-NAME>’s workforce to securely work and collaborate from the office, while travelling or from home.

<SYSTEM-NAME> includes the following components that will improve the security posture of <ORGANISATION-NAME>:

* **Identity**
  + Microsoft Entra ID (previously known as Azure Active Directory)
  + Multi-Factor Authentication (MFA)
  + Conditional Access
  + Privileged Identity Management
* **Microsoft 365** including:
  + Exchange Online & Exchange Online Protection
  + SharePoint Online
  + OneDrive for Business
  + Power Platform (Power Automate and Power Apps)
  + Microsoft Teams
  + Office 365 Applications
* **Device management (Intune)** including:
  + Windows 10
  + Windows 11
  + iOS
* **Connectivity**
  + Cloud to cloud
  + Endpoints
  + Point to site
  + Government to Government (GovLINK)
* **Security and Compliance Services** including:
  + Microsoft Defender XDR
  + Microsoft Defender for Cloud Apps
  + Microsoft Defender for Endpoints
  + Microsoft Defender for Identity
  + Microsoft Defender for Office 365
  + Microsoft Defender Vulnerability Management (MDVM)
  + Microsoft Information Protection
  + Microsoft Purview
  + Log Analytics
* **Automation** including:
  + Desired State Configuration (DSC)
  + Microsoft Graph
  + PowerShell
* **Support**

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### System boundary

The <SYSTEM-NAME> boundary consists of:

* Physical Boundaries — comprising the perimeter security measures of <ORGANISATION-NAME>’s office locations and service provider datacentre locations, network infrastructure and physical endpoints, and
* Virtual boundaries — comprising <SYSTEM-NAME>’s network segments, its information holdings, system access controls, internet gateway boundaries, inter-office connectivity and connectivity with partner services and Software as a Service (SaaS) applications.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

#### Diagram

<INSERT SYSTEM-BOUNDARY-DIAGRAM>

#### Out of scope

The following systems and components are out of the scope of this SSP as they are either addressed elsewhere or are not in-scope of <SYSTEM-NAME>:

* <SYSTEM/COMPONENT-1>
* <SYSTEM/COMPONENT-2>
* <SYSTEM/COMPONENT-3>

The above systems and components will have separate SSP(s) produced for them.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Risk assessment

The results of the threat and risk assessment undertaken for <SYSTEM-NAME> are documented in the Security Risk Management Plan (SRMP). This document describes the reduction in risk to the confidentiality, integrity and availability of system components and information processed and stored by <SYSTEM-NAME> by the implementation of security controls and mitigations.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## System delivery

The initial project to design, configure and deploy <SYSTEM-NAME> is being managed by <ORGANISATION-NAME>’s <SECTION/TEAM NAME> team as part of the <PROJECT-NAME> project. As this is a significant system build, this project has a variety of stakeholders, including:

* <STAKEHOLDER-1>
* <STAKEHOLDER-2>
* <STAKEHOLDER-3>

The design, configuration and deployment of <SYSTEM-NAME> will also leverage managed services from <MSP1-NAME> and <MSP2-NAME> respectively as described in the Procurement and Outsourcing section of this SSP. Similarly, as the build of <SYSTEM-NAME> primarily pertains to the use of Microsoft Cloud Services, the project team will liaise regularly with Microsoft in developing, improving and maintaining the system.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Cyber Security Roles

| EOT |
| --- |
| **Instruction** |
| The Cyber Security Roles section of a System Security Plan (SSP) should outline the relevant managerial and leadership roles involved in managing cyber security risks and controls relating to a system within an organisation. This information should be documented according to relevant controls outlined in ASD’s ISM. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents the cyber security roles in their organisation. When complete, remove any grey instructional or blue guidance boxes throughout. |

ASD’s ISM outlines the following key roles as required in relation to the operation of <SYSTEM-NAME>.

## Chief Information Security Officer (CISO)

### Applicability

ISM controls relating to the CISO role are applicable to <SYSTEM-NAME> as they require oversight of cyber security risks and controls within <ORGANISATION-NAME> and as such are applicable to this SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

The CISO is responsible for information security within <ORGANISATION-NAME>. They are responsible for the definition, authorisation, review, and monitoring of information security policies within the organisation in accordance with the duties outlined in the SSP Annex.

|  |
| --- |
| | Contact Name | Contact Phone | Contact Email | | --- | --- | --- | | <CISO-NAME> | <+61# ## ### ###> | <CISO-EMAIL@ORGANISATION.GOV.AU> | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to the CISO’s roles and responsibilities.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## System Owner

### Applicability

ISM controls relating to the System Owner role are applicable to <SYSTEM-NAME> as they require system-specific governance in <ORGANISATION-NAME> and as such are applicable to this SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

The System Owner monitors security risks and the effectiveness of security controls for <SYSTEM-NAME> and performs or delegates relevant duties outlined in the SSP Annex.

|  |
| --- |
| | Contact Name | Contact Phone | Contact Email | | --- | --- | --- | | <SYSTEM-OWNER-NAME> | <+61# ## ### ###> | <SYSTEM-OWNER-EMAIL@ORGANISATION.GOV.AU> | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to the System Owner’s roles and responsibilities.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Other roles

ASD’s ISM outlines other roles and responsibilities that may be relevant to the operation of <SYSTEM-NAME>.

### Applicability

ISM controls relating to the appropriate management of <SYSTEM-NAME> within <ORGANISATION-NAME> may be relevant to this SSP, but are not specifically required by the ISM.

### Organisational policies and processes implemented

#### Information Technology Security Advisor (ITSA)

The ITSA is responsible for managing IT Security across <ORGANISATION-NAME>.

|  |
| --- |
| | Contact Name | Contact Phone | Contact Email | | --- | --- | --- | | <ITSA-NAME> | <+61# ## ### ###> | <ITSA-EMAIL@ORGANISATION.GOV.AU> | |
|  |

#### System Manager

The System Manager is responsible for managing the day-to-day operations of <SYSTEM-NAME> as delegated by the System Owner.

|  |
| --- |
| | Contact Name | Contact Phone | Contact Email | | --- | --- | --- | | <SYSTEM-MANAGER-NAME> | <+61# ## ### ###> | <SYSTEM-MANAGER-EMAIL@ORGANISATION.GOV.AU> | |
|  |

#### Data Owner

Data Owners are responsible for ensuring relevant data complies with policies and regulatory requirements, and is assigned an appropriate classification as defined within the PSPF.

|  |
| --- |
| | Contact Name | Contact Phone | Contact Email | | --- | --- | --- | | <DATA-OWNER-1-NAME> | <+61# ## ### ###> | <DATA-OWNER-1-EMAIL@ORGANISATION.GOV.AU> | | <DATA-OWNER-2-NAME> | <+61# ## ### ###> | <DATA-OWNER-2-EMAIL@ORGANISATION.GOV.AU> | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to these roles and responsibilities.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Cyber Security Incidents

| EOT |
| --- |
| **Instruction** |
| The cyber security incidents section of a System Security Plan (SSP) should document an organisation’s approach to managing and responding to cyber security incidents. As with other sections of the SSP, information in the cyber security incidents section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents the approach to managing and responding to cyber security incidents within their organisation. When complete, remove any instructional boxes throughout. |

As <ORGANISATION-NAME>’s overall approach to implementing controls related to Cyber Security Incidents is consistent across all controls addressed within this section, it does not delve into subsections but rather addresses the controls as a group. This approach is also consistent with ASD’s [*Guidelines for Cyber Security Incidents*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents).

### Applicability

ISM controls relating to cyber security incidents are applicable to ensuring <SYSTEM-NAME> receives appropriate overarching governance of cyber security matters within <ORGANISATION-NAME> and are covered by this section of the SSP.

<ORGANISATION-NAME> is responsible for implementing administrative controls to govern the direct management of, and response to the cyber security incidents for <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

<ORGANISATION-NAME>’s management of cyber security incidents relating to <SYSTEM-NAME> is performed in line with <ORGANISATION-NAME>’s Cyber Security Incident Management Policy and Cyber Security Incident Response Plan , which include the reporting of incidents to <ORGANISATION-NAME>’s CISO and to ASD in a timely manner. These documents are exercised annually.

In accordance with the <SYSTEM-NAME> Incident Response Plan (IRP) , <ORGANISATION-NAME> will also liaise with Microsoft regarding the response to incidents that cover elements relating to their shared responsibility for <SYSTEM-NAME>.

All recorded incidents for <SYSTEM-NAME> are documented in its Cyber Security Incident Register .

The management of the threat that trusted insiders pose to <SYSTEM-NAME> is addressed as part of the <ORGANISATION-NAME>’s Trusted Insider Program .

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

| EOT |
| --- |
| **Blueprint guidance** |
| While the Blueprint provides limited guidance to support organisations in developing an approach for the response to cyber security incidents, the section below is provided for organisations to describe the measures implemented within their system. Effective implementation of these controls is generally built on a combination of system-specific and whole of organisation processes, and may include the coordination of a number of teams and staff across an organisation. |

<SYSTEM-NAME> utilises the Microsoft 365 Defender portal and <SIEM-PRODUCT> to assist in the identification of cyber security incidents. Specific capabilities include the Incident Queue and Action Centre views.

<ORGANISATION-NAME> has established a Security Operations Centre (SOC), a Cyber Security Incident Register , and an IRP to meet the requirements outlined in the SSP Annex .

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Procurement and Outsourcing

| EOT |
| --- |
| **Instruction** |
| The procurement and outsourcing section of a System Security Plan (SSP) should document an organisation’s approach to management of suppliers of applications, ICT equipment and services associated with systems built using the Blueprint. As with other sections of the SSP, information in the procurement and outsourcing section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to management of suppliers of applications, ICT equipment and services within their organisation. When complete, remove any instructional boxes throughout. |

As <ORGANISATION-NAME>’s overall approach to implementing controls related to procurement and outsourcing is consistent across all controls addressed within this section, it does not delve into subsections but rather addresses the controls as a group.

## Cyber supply chain risk management

### Applicability

* Laptops, endpoints and peripherals
* Server hardware
* Networking equipment
* On-premise server applications
* SaaS products

| EOT |
| --- |
| **Blueprint guidance** |
| This section of a SSP is directly applicable to the management of an organisation’s relationship with Microsoft as a service provider, including as a supplier of operating systems and applications. Similarly, this section is also applicable to the procurement of any other hardware, software or services used within a system built using the Blueprint, including: |

<ORGANISATION-NAME> uses Azure, Microsoft 365, and other cloud-based Software as a Service (SaaS) products as shared services, as well as Information and Communication Technology (ICT) equipment for client and on-premises components of <SYSTEM-NAME>. As such, controls related to cyber supply chain risk management are directly applicable to <SYSTEM-NAME>.

<ORGANISATION-NAME> is responsible for implementing administrative controls to govern the direct management of supply chain risks and security for <SYSTEM-NAME>.

### Organisational policies and processes implemented

Endpoints, networking, ICT equipment and relevant operating systems and applications should be procured through existing <ORGANISATION-NAME> supply arrangements. ICT equipment has been procured for <SYSTEM-NAME> using these existing procurement arrangements.

The following suppliers are used to procure ICT equipment and software for <SYSTEM-NAME>:

|  |
| --- |
| | Provider Name | Equipment or Software Provided | Notes | | --- | --- | --- | | Microsoft | Windows Operating System and related applications | <NOTES> | | Apple | iOS Operating System and related applications | <NOTES> | | Apple | iPhones | <NOTES> | | <HARDWARE-MANUFACTURER-1> | <LAPTOPS> | <NOTES> | | <HARDWARE-MANUFACTURER-2> | <SERVER EQUIPMENT> | <NOTES> | | <HARDWARE-MANUFACTURER-3> | <FIREWALL DEVICE> | <NOTES> | | <HARDWARE-MANUFACTURER-4> | <PRINTERS> | <NOTES> | | <HARDWARE-MANUFACTURER-5> | <FIDO2 HARDWARE KEYS> | <NOTES> | |  |  |  | |
|  |

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to cyber supply chain risk management.

## Managed services

### Applicability

| EOT |
| --- |
| **Blueprint guidance** |
| The Blueprint does not inherently leverage the use of Managed Service Providers (MSPs). However, the section below is provided for organisations to describe their use of MSPs in the implementation of systems built on using the Blueprint. |

<ORGANISATION-NAME> uses managed services in the delivery and operation of <SYSTEM-NAME>. As such, controls related to managed services are directly applicable to <SYSTEM-NAME>. <ORGANISATION-NAME> is responsible for implementing administrative controls to govern the administration and oversight of managed services for <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

<SYSTEM-NAME> only uses managed services that have been procured through existing <ORGANISATION-NAME> supply arrangements.

The following Managed Service Providers (MSPs) are used in relation to <SYSTEM-NAME>:

**<MANAGED SERVICE PROVIDER 1>**

|  |
| --- |
| | MSP Name | <MSP-NAME> | | --- | --- | | Managed service name | <MSP-SERVICE> | | Purpose of managed service | <PURPOSE> | | Sensitivity/classification of data involved | <PROTECTED> | | Due date for next security assessment | <MMM-YYYY> | | Contractual arrangements | <LINK> | | Point of contact | <MSP-POC-NAME> | | Contact email | <CONTACT-EMAIL> | | 24/7 contact phone | <+61X XX XXX XXX> | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to procurement or outsourcing of managed services.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Cloud services

### Applicability

<ORGANISATION-NAME> utilises cloud services in the delivery and operation of <SYSTEM-NAME>. As such, controls relating to cloud services are directly applicable to <SYSTEM-NAME>. <ORGANISATION-NAME> is responsible for implementing administrative controls to govern the direct management of outsourced cloud services for <SYSTEM-NAME>.

### Organisational policies and processes implemented

<SYSTEM-NAME> only uses cloud services that have been procured through existing <ORGANISATION-NAME> supply arrangements. All cloud services have been configured to store and process data solely in Australia.

The following cloud services providers are used in relation to <SYSTEM-NAME>:

#### Microsoft

**Contractual details and contacts**

|  |
| --- |
| | Field | Value | | --- | --- | | Completed IRAP Assessment | Yes ([<LINK> >}})) | | Completed Vendor Assessment by <ORGANISATION-NAME> | Yes ([<LINK> >}})) | | Due date for next security assessment | <MMM-YYYY> | | Contractual arrangements | <LINK> | | Point of contact | <CSP-POC-NAME> | | Contact email | <CONTACT-EMAIL> | | 24/7 contact phone | <+61X XX XXX XXX> | |
|  |

**Entra ID**

|  |
| --- |
| | Field | Value | | --- | --- | | Included in latest Microsoft IRAP assessment | Yes | | Included in latest Vendor Assessment by <ORGANISATION-NAME> | Yes | | Purpose of using service | <PURPOSE> | | Description of data involved | <DESCRIPTION> | | Sensitivity/classification of data involved | <PROTECTED> | | Availability regions used | <REGION> | |
|  |

**Purview**

|  |
| --- |
| | Field | Value | | --- | --- | | Included in latest Microsoft IRAP assessment | Yes | | Included in latest Vendor Assessment by <ORGANISATION-NAME> | Yes | | Purpose of using service | <PURPOSE> | | Description of data involved | <DESCRIPTION> | | Sensitivity/classification of data involved | <PROTECTED> | | Availability regions used | <REGION> | |
|  |

**Defender**

|  |
| --- |
| | Field | Value | | --- | --- | | Included in latest Microsoft IRAP assessment | Yes | | Included in latest Vendor Assessment by <ORGANISATION-NAME> | Yes | | Purpose of using service | <PURPOSE> | | Description of data involved | <DESCRIPTION> | | Sensitivity/classification of data involved | <PROTECTED> | | Availability regions used | <REGION> | |
|  |

**Exchange Online**

|  |
| --- |
| | Field | Value | | --- | --- | | Included in latest Microsoft IRAP assessment | Yes | | Included in latest Vendor Assessment by <ORGANISATION-NAME> | Yes | | Purpose of using service | <PURPOSE> | | Description of data involved | <DESCRIPTION> | | Sensitivity/classification of data involved | <PROTECTED> | | Availability regions used | <REGION> | |
|  |

**Exchange Online Protection**

|  |
| --- |
| | Field | Value | | --- | --- | | Included in latest Microsoft IRAP assessment | Yes | | Included in latest Vendor Assessment by <ORGANISATION-NAME> | Yes | | Purpose of using service | <PURPOSE> | | Description of data involved | <DESCRIPTION> | | Sensitivity/classification of data involved | <PROTECTED> | | Availability regions used | <REGION> | |
|  |

**SharePoint Online**

|  |
| --- |
| | Field | Value | | --- | --- | | Included in latest Microsoft IRAP assessment | Yes | | Included in latest Vendor Assessment by <ORGANISATION-NAME> | Yes | | Purpose of using service | <PURPOSE> | | Description of data involved | <DESCRIPTION> | | Sensitivity/classification of data involved | <PROTECTED> | | Availability regions used | <REGION> | |
|  |

**OneDrive for Business**

|  |
| --- |
| | Field | Value | | --- | --- | | Included in latest Microsoft IRAP assessment | Yes | | Included in latest Vendor Assessment by <ORGANISATION-NAME> | Yes | | Purpose of using service | <PURPOSE> | | Description of data involved | <DESCRIPTION> | | Sensitivity/classification of data involved | <PROTECTED> | | Availability regions used | <REGION> | |
|  |

**Teams**

|  |
| --- |
| | Field | Value | | --- | --- | | Included in latest Microsoft IRAP assessment | Yes | | Included in latest Vendor Assessment by <ORGANISATION-NAME> | Yes | | Purpose of using service | <PURPOSE> | | Description of data involved | <DESCRIPTION> | | Sensitivity/classification of data involved | <PROTECTED> | | Availability regions used | <REGION> | |
|  |

**Forms**

|  |
| --- |
| | Field | Value | | --- | --- | | Included in latest Microsoft IRAP assessment | Yes | | Included in latest Vendor Assessment by <ORGANISATION-NAME> | Yes | | Purpose of using service | <PURPOSE> | | Description of data involved | <DESCRIPTION> | | Sensitivity/classification of data involved | <PROTECTED> | | Availability regions used | <REGION> | |
|  |

**Power Automate**

|  |
| --- |
| | Field | Value | | --- | --- | | Included in latest Microsoft IRAP assessment | Yes | | Included in latest Vendor Assessment by <ORGANISATION-NAME> | Yes | | Purpose of using service | <PURPOSE> | | Description of data involved | <DESCRIPTION> | | Sensitivity/classification of data involved | <PROTECTED> | | Availability regions used | <REGION> | |
|  |

**Power BI**

|  |
| --- |
| | Field | Value | | --- | --- | | Included in latest Microsoft IRAP assessment | Yes | | Included in latest Vendor Assessment by <ORGANISATION-NAME> | Yes | | Purpose of using service | <PURPOSE> | | Description of data involved | <DESCRIPTION> | | Sensitivity/classification of data involved | <PROTECTED> | | Availability regions used | <REGION> | |
|  |

**Power Apps**

|  |
| --- |
| | Field | Value | | --- | --- | | Included in latest Microsoft IRAP assessment | Yes | | Included in latest Vendor Assessment by <ORGANISATION-NAME> | Yes | | Purpose of using service | <PURPOSE> | | Description of data involved | <DESCRIPTION> | | Sensitivity/classification of data involved | <PROTECTED> | | Availability regions used | <REGION> | |
|  |

**Log Analytics**

|  |
| --- |
| | Field | Value | | --- | --- | | Included in latest Microsoft IRAP assessment | Yes | | Included in latest Vendor Assessment by <ORGANISATION-NAME> | Yes | | Purpose of using service | <PURPOSE> | | Description of data involved | <DESCRIPTION> | | Sensitivity/classification of data involved | <PROTECTED> | | Availability regions used | <REGION> | |
|  |

**Whiteboard**

|  |
| --- |
| | Field | Value | | --- | --- | | Included in latest Microsoft IRAP assessment | Yes | | Included in latest Vendor Assessment by <ORGANISATION-NAME> | Yes | | Purpose of using service | <PURPOSE> | | Description of data involved | <DESCRIPTION> | | Sensitivity/classification of data involved | <PROTECTED> | | Availability regions used | <REGION> | |
|  |

**Planner**

|  |
| --- |
| | Field | Value | | --- | --- | | Included in latest Microsoft IRAP assessment | Yes | | Included in latest Vendor Assessment by <ORGANISATION-NAME> | Yes | | Purpose of using service | <PURPOSE> | | Description of data involved | <DESCRIPTION> | | Sensitivity/classification of data involved | <PROTECTED> | | Availability regions used | <REGION> | |
|  |

**Viva Learning**

|  |
| --- |
| | Field | Value | | --- | --- | | Included in latest Microsoft IRAP assessment | Yes | | Included in latest Vendor Assessment by <ORGANISATION-NAME> | Yes | | Purpose of using service | <PURPOSE> | | Description of data involved | <DESCRIPTION> | | Sensitivity/classification of data involved | <PROTECTED> | | Availability regions used | <REGION> | |
|  |

#### <PROVIDER-2>

**Contractual details and contacts**

|  |
| --- |
| | Field | Value | | --- | --- | | Due date for next security assessment | <MMM-YYYY> | | Contractual arrangements | <LINK> | | Point of contact | <CSP-POC-NAME> | | Contact email | <CONTACT-EMAIL> | | 24/7 contact phone | <+61X XX XXX XXX> | |
|  |

**<SERVICE 1>**

|  |
| --- |
| | Field | Value | | --- | --- | | Included in latest <PROVIDER-2> IRAP assessment | Yes | | Included in latest Vendor Assessment by <ORGANISATION-NAME> | Yes | | Purpose of using service | <PURPOSE> | | Description of data involved | <DESCRIPTION> | | Sensitivity/classification of data involved | <PROTECTED> | | Availability regions used | <REGION> | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to the procurement or outsourcing of cloud services.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Security Documentation

| EOT |
| --- |
| **Instruction** |
| The cyber security documentation section of a System Security Plan (SSP) should document an organisation’s approach to development of organisational and system-specific cyber security documentation associated with systems built using the Blueprint. As with other sections of the SSP, information in the cyber security documentation section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents the approach to cyber security documentation within their organisation. When complete, remove any instructional boxes throughout. |

As <ORGANISATION-NAME>’s approach to implementing controls related to cyber security documentation is consistent across all controls addressed within this section, it does not delve into subsections but rather addresses the controls as a group.

### Applicability

ISM controls relating to cyber security documentation are applicable to ensuring <SYSTEM-NAME>receives appropriate overarching governance of cyber security matters within <ORGANISATION-NAME> and are covered by this section of the SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

<ORGANISATION-NAME>’s CISO is responsible for approving all organisational level cyber security documentation, ensuring this documentation is reviewed at least annually and ensuring all relevant stakeholders are aware of this documentation and subsequent updates.

As <SYSTEM-NAME>’s authorising officer, <ORGANISATION-NAME>’s ITSA is responsible for approving all system-specific cyber security documentation, ensuring that the documentation is reviewed at least annually and ensuring all relevant stakeholders are aware of this documentation and subsequent updates.

Links to relevant <ORGANISATION-NAME> and <SYSTEM-NAME> cyber security documentation are provided below.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to cyber security documentation.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

* <ORGANISATION-NAME>
* <SYSTEM-NAME>
* <SYSTEM-NAME>
* <SYSTEM-NAME>
* <SYSTEM-NAME>
* <SYSTEM-NAME>

# Physical Security

| EOT |
| --- |
| **Instruction** |
| The physical security section of a System Security Plan (SSP) should document an organisation’s approach to managing physical security associated with facilities and systems. As with other sections of the SSP, information in the physical security section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to physical security within their organisation. When complete, remove any instructional boxes throughout. |

As <ORGANISATION-NAME>’s approach to implementing controls related to physical security is consistent across all controls addressed within this section, it does not delve into subsections but rather addresses the controls as a group. This approach is consistent with ASD’s [*Guidelines for Physical Security*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-physical-security).

### Applicability

| EOT |
| --- |
| **Blueprint guidance** |
| While system(s) built using the Blueprint rely on Microsoft (and any other cloud or managed service providers used) for managing the physical security of facilities and systems that host their services, organisations that own system(s) built using the Blueprint are responsible for the physical security of all other components. |
| In particular, this is relevant to any server infrastructure hosting a hybrid deployment of system(s) built using the Blueprint and for any additional services, such as gateways or networking equipment where they are within the relevant system boundary. |

<ORGANISATION-NAME> uses on-premises facilities and systems to host hybrid components of <SYSTEM-NAME>, as well as networking components for the use of ICT devices in <ORGANISATION-NAME>’s offices.

<SYSTEM-NAME> does not consider the direct management of these physical facilities or systems within its system boundary, and relies on the implementation from the following system assessments:

* <ORG-NETWORKING-SYSTEM>
* <ORG-IDENTITY-SYSTEM>

Use of laptops and/or iPhones by staff outside of <ORGANISATION-NAME>’s offices is in accordance with the [Enterprise Mobility](#enterprise-mobility) section of this SSP. However, <SYSTEM-NAME> endpoints and peripherals are also deployed in <ORGANISATION-NAME>’s offices as their primary place of operation.

<ORGANISATION-NAME> is responsible for the physical security of devices located at <ORGANISATION-NAME>’s` offices.

### Organisational policies and processes implemented

Management of facilities and physical security is performed in accordance with <ORGANISATION-NAME>’s Physical Security Policy, which requires all organisational assets, including ICT equipment and media to be appropriately secured according to their use.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Physical server hardware, networking devices, and cryptographic equipment are deployed in secure rooms within <ORGANISATION-NAME>’s offices, assessed to meet <ZONE 2> requirements as per the Department of Home Affair’s Protective Security Policy Framework (PSPF).

Workstations are also deployed within <ORGANISATION-NAME>’s offices, assessed to meet <ZONE 2> requirements as per the PSPF.

<SYSTEM-NAME> also inherits implementation of physical security controls by <ORGANISATION-NAME>’s cloud and managed service providers.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Personnel Security

| EOT |
| --- |
| **Instruction** |
| The personnel security section of a System Security Plan (SSP) should document an organisation’s approach to managing personnel security associated with facilities and systems. As with other sections of the SSP, information in the personnel security section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to cyber security documentation within their organisation. When complete, remove any instructional boxes throughout. |

## Cyber security awareness training

### Applicability

ISM controls relating to cyber security awareness training are applicable to ensuring <SYSTEM-NAME>receives appropriate overarching governance of decisions and activities that might affect the cyber security within <ORGANISATION-NAME> and are covered by this section of the SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

<ORGANISATION-NAME> is responsible for conducting regular cyber security awareness training for all staff and contractors. As such, cyber security awareness training is undertaken annually by all <ORGANISATION-NAME> staff and contractors covering:

* the purpose of cyber security awareness training
* cyber security roles and key contacts
* authorised use of systems and resources
* protection of systems and resources
* reporting of cyber security incidents and suspected compromises.

Tailored privileged user training is also undertaken annually by all privileged users of <SYSTEM-NAME>.

<ORGANISATION-NAME>’s cyber security awareness training material can be found here.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to cyber security awareness training.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Access to systems and resources

### Applicability

ISM controls relating to access control are directly applicable to <SYSTEM-NAME> and are covered by this section of the SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

Use of <SYSTEM-NAME> by <ORGANISATION-NAME> staff and contractors is in accordance with the <SYSTEM-NAME> System Usage Policy.

Staff are only granted access to <SYSTEM-NAME> after:

* undergoing employment screening and obtaining a <REQUIRED-CLEARANCE> security clearance from the Australian Government Security Vetting Agency (AGSVA)
* agreeing to the <SYSTEM-NAME> Acceptable Usage Policy
* receiving a <REQUIRED-BRIEFING> briefing
* the request for system access and completion of the above requirements by the user has been validated via <VALIDATION-PROCESS>.

| EOT |
| --- |
| **Blueprint guidance** |
| The requirement for staff to obtain a security clearance from AGSVA is particularly applicable to government organisations working with information up to the PROTECTED level. Organisations should consider their own requirements, with reference to the Department of Home Affairs’ [*Protective Security Policy Framework* (PSPF)](https://www.protectivesecurity.gov.au/) as appropriate. |

All <SYSTEM-NAME> users are granted uniquely identifiable accounts for their general system use, with privileged users granted additional uniquely identifiable privileged accounts to be used for these duties. In accordance with the <PRIVILEGED-ACCESS-PROCESS>, the validity of the business case for each privileged account will be assessed on request and revalidated on an annual basis.

**Temporary access**

Temporary access to <SYSTEM-NAME> is only granted in the following circumstances:

* <TEMP-ACCESS-REASON-1>
* <TEMP-ACCESS-REASON-2>
* <TEMP-ACCESS-REASON-3>

Accounts used for temporary access are specifically restricted using Role Based Access Control (RBAC) to the minimum required access for these users to undertake their duties.

**Shared and emergency access**

Shared accounts for <SYSTEM-NAME> will only be used in the following extenuating circumstances:

* Break Glass Accounts

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

Use of Break Glass Accounts is documented in <SYSTEM-NAME>’s Incident Response Plan, which has been tested on <TEST-DATE> as part of its initial implementation and deployment. This testing is also to be completed after any fundamental system change, with the last test completed on <TEST-DATE>.

### Technical controls implemented

Technical controls for implementation of user access to <SYSTEM-NAME> and its resources are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au). In particular, the following technical configurations have been implemented:

* all unprivileged access attempts are logged within Microsoft Entra Sign-ins
* Microsoft Entra logs are forwarded to a log analytics workspace for long-term secure retention
* an AppLocker blocklist is configured on workstations via Intune to prevent administrators from launching web browsers and email clients
* Microsoft Privileged Identity Management (MPIM) has been configured to provide Just-in-Time (JIT) administration
* changes to privileged accounts and groups are logged in the Microsoft Entra Audit Log
* Microsoft Entra accounts are automatically disabled after 45-days of inactivity
* privileged users access to systems, applications and data repositories is automatically disabled after 12-months unless revalidated
* Microsoft Defender for Cloud Apps policy monitoring is implemented to monitor the activity of Break Glass Accounts
* the use of Break Glass Accounts is logged in Microsoft Entra Sign-ins.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

* <SYSTEM-NAME>

# Communication Infrastructure

| EOT |
| --- |
| **Instruction** |
| The communications infrastructure section of a System Security Plan (SSP) should document an organisation’s approach to managing communications infrastructure, such as cabling. As with other sections of the SSP, information in the communications infrastructure section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents the approach to communications infrastructure within their organisation. When complete, remove any instructional boxes throughout. |

| EOT |
| --- |
| **Blueprint guidance** |
| The Blueprint does not cover management of communications infrastructure and the below template therefore excludes communications infrastructure from the documented scope. |
| Where organisations decide to implement communications infrastructure within the boundary of their system, they are responsible for assessing and documenting risk and applicability of each associated security control, and describing the implementation of these controls below. |

As <ORGANISATION-NAME>’s approach to implementing controls related to communications infrastructure is consistent across all controls addressed within this section, it does not delve into subsections but rather addresses the controls as a group. This approach is consistent with ASD’s [*Guidelines for Communications Infrastructure*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-communications-infrastructure).

### Applicability

ISM controls relating to communications infrastructure are not applicable to <SYSTEM-NAME> as direct management of these physical facilities or systems are not within its system boundary. <SYSTEM-NAME> relies on the implementation of relevant controls from the following system assessments:

* ORG-NETWORKING-SYSTEM
* ORG-IDENTITY-SYSTEM

As such the requirements of this section are **not** directly applicable for this SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

If and when the management of communications infrastructure is considered as part of <ORGANISATION-NAME>’s management of <SYSTEM-NAME>, <ORGANISATION-NAME> will assess and implement appropriate controls in relation to <SYSTEM-NAME> at that time.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to the management of communications infrastructure.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Communications Systems

| EOT |
| --- |
| **Instruction** |
| The communications systems section of a System Security Plan (SSP) should document an organisation’s approach to managing communications systems, such as telephone, videoconferencing and faxes. As with other sections of the SSP, information in the communications systems section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents the approach to communications systems organisation. When complete, remove any instructional boxes throughout. |

## Telephone systems

### Applicability

| EOT |
| --- |
| **Blueprint guidance** |
| The Blueprint does not cover management of landline and mobile telephone systems. However, the use of Microsoft Teams does constitute a telephone system for the purpose of organisational policies relating to these systems. |
| Please note that the Blueprint does not currently provide guidance on implementing [Telstra Calling for Office 365](https://www.telstra.com.au/small-business/business-software/telstra-calling-for-office-365). This service enables calling between Microsoft Teams and landline and mobile telephones. Organisations wishing to use this service or another similar service should ensure it is implemented, assessed, and managed appropriately. |

ISM controls relating to communications systems are applicable to the use of Microsoft Teams within <SYSTEM-NAME>, considering it as a telephone system in alignment with <ORGANISATION-NAME>’s policies and processes governing its use, and are covered by this section of the SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes

Use of Microsoft Teams within <SYSTEM-NAME> is subject to <ORGANISATION-NAME>’s Telephone Usage Policy , which describes the sensitivity or classification of information that can be discussed over applicable systems and connection types.

<ORGANISATION-NAME> cyber security awareness training also informs staff of the security risks associated with using each of these connection types, particularly in areas where sensitive classified conversations may occur.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to the management of telephone systems.

| EOT |
| --- |
| **Blueprint guidance** |
| Organisations that use Telstra Calling for Office 365 or a similar service, should consider inclusion of the following words or similar in this section of the SSP: |
| <SYSTEM-NAME> utilises <SERVICE-NAME> to allow calling between Teams and landline and mobile telephones. |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Video conferencing and internet protocol telephony

### Applicability

ISM controls relating to communications systems are applicable to the use of Microsoft Teams for video conferencing and IP telephony services within <SYSTEM-NAME> and are covered by this section of the SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

<ORGANISATION-NAME> implements and maintains a Denial of Service Response Plan for IP Telephony that includes appropriate business continuity practices in the event of a loss of Microsoft Teams functionality within <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for <SYSTEM-NAME>’s implementation of Microsoft Teams for video conferencing and IP telephony were configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au).

<SYSTEM-NAME> use of Microsoft Teams inherits the implementation of the following controls from Microsoft:

* use of Entra ID as the source of authentication and authorisation
* use of Microsoft Azure’s Distributed Denial of Service (DDoS) protection capabilities
* implementation of secure signalling data encryption, including:
* Session Initiation Protocol (SIP)
* Secure Real Time Protocol (SRTP)
* use of a dedicated Virtual Local Area Network (VLAN) within the Microsoft cloud.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Fax machines and multifunction devices

| EOT |
| --- |
| **Blueprint guidance** |
| The Blueprint does not cover management of fax machines or multifunction devices. However, organisations may find the below template a useful guide for documenting the use of fax machines or multifunction devices associated with system(s) built using the Blueprint. |

### Applicability

ISM controls relating to multifunction devices (MFDs) are applicable to <ORGANISATION-NAME>’s use of MFDs for office productivity purposes. These devices are connected to <SYSTEM-NAME> for printing and scanning services. However, the technical implementation of these devices is not within the authorisation boundary of <SYSTEM-NAME>.

Please see the <PRINT-SYSTEM> System Security at Plan <insert document reference here> for further information on implementation of these services.

<ORGANISATION-NAME> does not use faxing services, and therefore these controls are not in scope of this SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

Appropriate organisational use of MFDs and fax machines is detailed in the <ORGANISATION-NAME>’s Fax Machine and MFD Usage Policy .

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to the use of fax machines or MFDs.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Enterprise Mobility

| EOT |
| --- |
| **Instruction** |
| The enterprise mobility section of a System Security Plan (SSP) should document an organisation’s approach to enterprise mobility, including allowing privately owned devices to access systems and data and mobile device management. As with other sections of the SSP, information in the enterprise mobility section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to enterprise mobility. When complete, remove any instructional boxes throughout. |

## Enterprise mobility

### Applicability

ISM controls relating to enterprise mobility are applicable to <SYSTEM-NAME> and are covered by this section of the SSP as the system includes the use of corporate mobile devices, but does not permit personal devices to connect to <SYSTEM-NAME> or its resources.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

Use of <SYSTEM-NAME> by <ORGANISATION-NAME>’s staff and contractors is in accordance with the <SYSTEM-NAME> Mobile Device Usage Policy , which requires that all system access is performed via corporately issued devices, and that these devices are used solely for corporate use.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for <SYSTEM-NAME>’s implementation of enterprise mobility are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au), and includes the following technical configurations:

* conditional access policies are set to prevent non corporately-issued devices from connecting to <SYSTEM-NAME> or its resources
* application control is configured on corporately issued mobile devices to provide some restriction of personal use on these devices
* corporately issued devices connect to the internet through <ORGANISATION-NAME>’s <VPN-SYSTEM> when connecting remotely, and do so with split tunnelling disabled
* corporately issued devices connect to the internet through <ORGANISATION-NAME>’s <GATEWAY-SYSTEM>, which also restricts web categories associated with personal use on these devices.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Mobile device management

### Applicability

ISM controls relating to the management of mobile devices are applicable to <SYSTEM-NAME> and are covered by this section of the SSP as the system includes the configuration and hardening of corporately owned and issued Apple iPhones.

While considered to be mobile devices in other contexts, this section of the SSP does not apply to the management of Windows laptops.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

The management of corporately owned and issued mobile devices for <SYSTEM-NAME> is implemented through the use of Microsoft Intune, and is governed by <ORGANISATION-NAME>’s Mobile Device Management Policy . This policy requires appropriate selection of mobile operating systems and use of mobile device management solutions to be from those that have completed appropriate [Common Criteria Protection Profiles](https://commoncriteriaportal.org/pps/index.cfm).

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for <SYSTEM-NAME>’s implementation of mobile device management are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au).

<SYSTEM-NAME> uses Microsoft Intune as its Mobile Device Management (MDM) solution, which has [completed the relevant protection profile assessment](https://www.niap-ccevs.org/products/11298).

<SYSTEM-NAME> requires use of the latest version of iOS, which is currently iOS 18. The most recent version of iOS to have completed the relevant protection profile assessment is iOS 16. However, <ORGANISATION-NAME> considers that while the protection profile assessment is not of the implemented operating system (iOS 18), the recency of the assessment of iOS 16 mitigates associated risks.

iOS devices are configured to:

* operate in Supervised Mode
* be remotely wipeable using Intune
* operate with a secure lock screen
* apply the latest security patches released by Apple
* restrict iOS users from installing applications from the App Store on iOS
* restrict iOS users from disabling or modifying security functionality once provisioned.

Mobile device encryption is also inherently enabled for iOS devices’ internal storage.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Mobile device usage

### Applicability

ISM controls relating to mobile devices, including Windows laptops and iOS devices, are applicable to <SYSTEM-NAME> and are covered by this section of the SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational Policies and Processes Implemented

Management of <SYSTEM-NAME> mobile devices and their peripherals is in accordance with the <ORGANISATION-NAME>’s <SYSTEM-NAME> Mobile Device Usage Policy .

Use of <SYSTEM-NAME> mobile devices and their peripherals is in accordance with the <ORGANISATION-NAME>’s <SYSTEM-NAME> Mobile Device Usage Policy .

Procedures related to overseas travel by <SYSTEM-NAME> users are outlined in the Overseas Travel SOP .

<SYSTEM-NAME>’s Mobile Device Emergency Sanitisation Standard Operating Procedure provides advice on the remote sanitisation of mobile devices.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for <SYSTEM-NAME>’s implementation of mobile device usage were configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au), and implements the following technical configurations:

* Windows Defender for Endpoint is configured to restrict allowed peripherals to an approved list
* iOS is configured to restrict allowed peripherals to an approved list.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

* <SYSTEM-NAME>
* <SYSTEM-NAME>

# Evaluated Products

| EOT |
| --- |
| **Instruction** |
| The evaluated products section of a System Security Plan (SSP) should document an organisation’s approach to procuring and using evaluated products. As with other sections of the SSP, information in the evaluated products section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to procuring and using evaluated products. When complete, remove any instructional boxes throughout. |

As <ORGANISATION-NAME>’s approach to implementing controls related to evaluated products is consistent across all controls addressed within this section, it does not delve into subsections but rather addresses the controls as a group. This approach is consistent with ASD’s [*Guidelines for Evaluated Products*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-evaluated-products).

### Applicability

| EOT |
| --- |
| **Blueprint guidance** |
| The below template and guidance are written as they relate to the products used and configured using the Blueprint, including Microsoft Windows and Apple iOS. When using the Blueprint, organisations should pay particular attention to any additional products used within its scope and add further information as required. |

ISM controls relating to the procurement and use of evaluated products including applications, operating systems and devices within <SYSTEM-NAME> are applicable to and covered by this section of the SSP.

<SYSTEM-NAME> uses the following evaluated products:

* Microsoft Windows 10
* Microsoft Windows 11
* Apple iOS 17: iPhones (Apple iOS 16 is the latest release to be certified under Common Criteria - [iOS 16 CC details](https://www.niap-ccevs.org/Product/Compliant.cfm?PID=11349))
* <MICROSOFT WINDOWS SERVER 2022>

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

The procurement and use of evaluated products including applications, operating systems and devices for <SYSTEM-NAME> is performed in accordance with <ORGANISATION-NAME>’s Evaluated Products Policy and associated SOPs:

* <SYSTEM-NAME> <SOP-1>
* <SYSTEM-NAME> <SOP-2>

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for <SYSTEM-NAME>’s management of evaluated products are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au), and includes the following technical configurations:

<DETAIL CONFIGURATION OF EVALUATED PRODUCTS AS APPROPRIATE>

# ICT Equipment

| EOT |
| --- |
| **Instruction** |
| The ICT equipment section of a System Security Plan (SSP) should document an organisation’s approach to ICT equipment use, maintenance, repairs, sanitisation, destruction and disposal. As with other sections of the SSP, information in the ICT equipment section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to managing ICT equipment. When complete, remove any instructional boxes throughout. |

As <ORGANISATION-NAME>’s approach to implementing controls related to ICT equipment is consistent across all controls addressed within this section, it does not delve into subsections but rather addresses the controls as a group. This approach is consistent with ASD’s [*Guidelines for ICT Equipment*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-ict-equipment).

### Applicability

ISM controls relating to the appropriate selection, use, maintenance, repair, sanitisation, destruction, and disposal of <SYSTEM-NAME> equipment listed under technical controls implemented are covered by this section of the SSP.

<SYSTEM-NAME> also relies on the implementation of controls within the following system assessments:

* <ORG-NETWORKING-SYSTEM>
* <ORG-IDENTITY-SYSTEM>

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

Selection, use, maintenance, repairs, sanitisation, destruction and disposal of <SYSTEM-NAME> equipment is performed according to <ORGANISATION-NAME>’s ICT Equipment Management Policy and associated standard operating procedures (SOPs):

* <SYSTEM-NAME> ICT Equipment Maintenance Process
* <SYSTEM-NAME> ICT Equipment Sanitisation Process
* <SYSTEM-NAME> ICT Equipment Destruction Process
* <SYSTEM-NAME> ICT Equipment Disposal Process

In accordance with <ORGANISATION-NAME>’s ICT Equipment Management Policy, all vendors of ICT equipment used for <SYSTEM-NAME> have been assessed by <ORGANISATION-NAME> as demonstrating a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, secure programming practices and maintaining the security of their products more broadly.

* <ORGANISATION-NAME> Vendor Assessment: Microsoft
* <ORGANISATION-NAME> Vendor Assessment: Apple
* <ORGANISATION-NAME> Vendor Assessment: <VENDOR-3>

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

<SYSTEM-NAME> uses the below ICT equipment within its authorisation boundary, with technical controls for <SYSTEM-NAME>’s hardening of ICT equipment performed with reference to the following guidance:

|  |
| --- |
| | Equipment Type | Make/Model | Purpose | Hardening Guides Referenced | | --- | --- | --- | --- | | Laptop Endpoint | <MAKE, MODEL> | Endpoint for general users | ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) | |  |  |  | ASD [*Windows 10 21H1 Hardening Guide*](https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/hardening-microsoft-windows-10-version-21h1-workstations) | | Desktop Endpoint | <MAKE, MODEL> | Endpoint for select office users | ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) | |  |  |  | ASD [*Windows 10 21H1 Hardening Guide*](https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/hardening-microsoft-windows-10-version-21h1-workstations) | | Mobile | Apple iPhone 14 | Mobile phone for general users | ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) | |  |  |  | Apple’s [*iOS 16: iPhones Common Criteria Configuration Guide*](https://www.niap-ccevs.org/MMO/Product/st_vid11349-agd.pdf) | | (Further examples) |  |  |  | | Peripheral - Headset | <MAKE, MODEL> | Use with Microsoft Teams Calls | None | | Peripheral - Dock | <MAKE, MODEL> | Connection of monitor and peripherals to laptops | None | | Peripheral - Monitor | <MAKE, MODEL> | Use with laptop and desktop endpoints | None | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Media

| EOT |
| --- |
| **Instruction** |
| The media section of a System Security Plan (SSP) should document an organisation’s approach to management of usage, sanitisation, destruction and disposal of media. As with other sections of the SSP, information in the media section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to managing media. When complete, remove any instructional boxes throughout. |

As <ORGANISATION-NAME>’s approach to implementing controls related to media is consistent across all controls addressed within this section, it does not delve into subsections but rather addresses the controls as a group. This approach is consistent with ASD’s [*Guidelines for Media*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-media)

### Applicability

ISM controls relating to the appropriate selection usage, sanitisation, destruction, and disposal of media used within <SYSTEM-NAME>’s system boundary are applicable to and covered by this section of the SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

The use, sanitisation, destruction, and disposal of media used with <SYSTEM-NAME> equipment is performed in accordance with <ORGANISATION-NAME>’s Media Management Policy and associated SOPs:

* <SYSTEM-NAME> Media Sanitisation Process
* <SYSTEM-NAME> Media Destruction Process
* <SYSTEM-NAME> Media Disposal Process

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for <SYSTEM-NAME>’s implementation relating to to the use, sanitisation, destruction, and disposal of media are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) and includes the following technical configurations:

* Windows endpoints are configured via Intune to implement Bitlocker AES-256 encryption for internal media

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Operating System Hardening

| EOT |
| --- |
| **Instruction** |
| The operating system hardening section of a System Security Plan (SSP) should document an organisation’s approach to hardening operating systems using vendor and ASD guidance. As with other sections of the SSP, information in the operating system hardening section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to operating system hardening. When complete, remove any instructional boxes throughout. |

Due to the number of applicable controls in ASD’s [*Guidelines for System Hardening*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-hardening), guidance on system hardening has been split into its five sections for the purpose of this SSP. The following controls have been grouped by equipment types and as as they relate to hardening of operating systems within <SYSTEM-NAME>.

## Operating system selection, versions, releases and SOEs

### Applicability

ISM controls relating to the operating system selection, releases and versions and standard operating environments (SOE) within <SYSTEM-NAME>’s system boundary are applicable to and covered by this section of the SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

All vendors of operating systems used within <SYSTEM-NAME> have been assessed by <ORGANISATION-NAME> as demonstrating a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.

* <ORGANISATION-NAME> Vendor Assessment: Microsoft
* <ORGANISATION-NAME> Vendor Assessment: Apple
* <ORGANISATION-NAME> Vendor Assessment: <VENDOR-3>

<SYSTEM-NAME> uses Microsoft Intune for the enrolment and configuration of endpoints (including Windows 10, 11 and iOS endpoints), that serve as the SOE for <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for operating system hardening and SOEs within <SYSTEM-NAME> were configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au), and applied by <ORGANISATION-NAME> with regard to any malicious configurations that may have been injected. These controls will continue to be reviewed on an ongoing basis, with regard to the Blueprint and consideration of any malicious configurations that could be injected.

Operating systems used within <SYSTEM-NAME>’s system boundary, along with their releases and versions, are listed in the Operating System Releases table below. All versions used are 64-bit and are of either the latest or N-1 releases. Windows endpoints are configured via Intune to use Microsoft’s [*General Availability Channel*](https://learn.microsoft.com/windows-server/get-started/servicing-channels-comparison).

|  |
| --- |
| | Component | Vendor | Operating System | Release | Version | | --- | --- | --- | --- | --- | | Endpoints | Microsoft | Windows | 22H2 (Windows 10) | 64-bit | |  |  |  | 23H2 (Windows 11) | (N/A: 64-bit only) | | Mobile Devices | Apple | iOS | 16 | (N/A: 64-bit only) | |  |  |  | 17 | (N/A: 64-bit only) | | <ON-PREM SERVERS> | Microsoft | <WINDOWS SERVER> | <2022> | (N/A: 64-bit only) | | <ON-PREM SERVERS> | <VENDOR> | <LINUX DISTRO> | <RELEASE> | <64-BIT> | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Hardening Windows endpoints

### Applicability

This section of the SSP covers the following control topics within ASD’s ISM’s *Operating System Hardening* section, as they apply to all endpoints and servers within <SYSTEM-NAME>:

* Hardening operating system configurations
* Application management
* Application control
* Command Shell
* PowerShell
* Host-based Intrusion Prevention System
* Software firewall
* Antivirus software
* Device Access

### Organisational policies and processes implemented

<ORGANISATION-NAME> has not implemented any specific organisational policies or processes related to hardening operating system configurations for <SYSTEM-NAME> beyond ensuring implementation of the below technical controls as part of this System Security Plan, and reviewing all below configurations on an annual or more frequent basis.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

<ORGANISATION-NAME> has not implemented any specific organisational policies or processes relating to hardening operating systems within <SYSTEM-NAME> beyond ensuring implementation of the below technical controls as part of this SSP and reviewing the below configurations on at least an annual basis (if not more frequently).

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Hardening server operating systems

| EOT |
| --- |
| **Blueprint guidance** |
| While the Blueprint does provide guidance on hardening operating systems for servers, the section below is provided for organisations to describe their implementation of hardening of operating systems for servers where it is included within the authorisation boundary for system(s) built using the Blueprint, noting that hardening of operating systems for servers is often completed as part of a separate system and SSP specific to those servers. |
| Where an organisation appropriately assesses this within another document, it may choose to remove its implementation and assessment from this SSP. However, it is recommended that organisations consider also documenting their approach to hardening operating systems for servers here for a holistic capture of a system’s context and associated risk. |

### Applicability

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

* <ORGANISATION-NAME>
* <ORGANISATION-NAME>
* <ORGANISATION-NAME>

# User Application Hardening

| EOT |
| --- |
| **Instruction** |
| The user application hardening section of a System Security Plan (SSP) should document an organisation’s approach to hardening applications typically installed on workstations using vendor and ASD guidance, such as office productivity suites, web browsers and their extensions, email clients, PDF software and security products (e.g. antivirus software, device access control software, HIPS and software firewalls), commonly referred to as user applications. As with other sections of the SSP, information in the user application hardening section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to operating system hardening. When complete, remove any instructional boxes throughout. |

Due to the number of applicable controls in ASD’s [*Guidelines for System Hardening*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-hardening), guidance on system hardening has been split into its five sections for the purpose of this SSP.

## User application selection and releases

### Applicability

This section of the SSP is applicable to application selection for the below <SYSTEM-NAME> components:

* Endpoints (Windows laptops and desktops)
* Mobile Devices (iOS)
* <ON-PREMISES SERVERS>

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

All vendors of user applications used within <SYSTEM-NAME> have been assessed by <ORGANISATION-NAME> as demonstrating a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.

* <ORGANISATION-NAME> Vendor Assessment: Microsoft
* <ORGANISATION-NAME> Vendor Assessment: Apple
* <ORGANISATION-NAME> Vendor Assessment: <VENDOR-3>

User applications used for <SYSTEM-NAME>, along with their releases and versions are listed in the <SYSTEM-NAME> Allowed Applications Register.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Allowed applications are deployed to endpoints and configured via Microsoft Intune, with application control implemented as per the information in the section below.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Hardening user application configurations and macros (Windows endpoints)

### Applicability

This section of the SSP is applicable to the hardening of user applications for the below <SYSTEM-NAME> components:

* Endpoints (laptops and desktops)
* Mobile Devices
* <ON-PREMISES SERVERS>

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

<ORGANISATION-NAME> has not implemented any specific organisational policies or processes related to hardening user application configurations within <SYSTEM-NAME> beyond ensuring implementation of the below technical controls as part of this SSP and reviewing the configurations on at least an annual basis (if not more frequently).

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for hardening of user applications and Microsoft Office macros within <SYSTEM-NAME> are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) and includes the following technical configurations:

|  |
| --- |
| |  |  | | --- | --- | | **User Application Configurations:** | Microsoft and built-in web browsers hardening | |  | remove unnecessary functionality, such as Microsoft Access | |  | restrict the use of add-ons to only those deployed via Intune | |  | prevent the installation of Java | |  | enable native Microsoft Edge advertisement blocking | |  | disable Internet Explorer 11 | |  | configure Attack Surface Reduction rules | |  | block Object Linking and Embedding (OLE) | | **Macros:** | only allow Microsoft macros that have been digitally signed by a trusted publisher to execute | |  | disable all macros downloaded from the internet | |  | enable antivirus scanning of Microsoft macros | |  | prevent users from changing macro settings | |  | configure Defender for Endpoint to centrally store EDR logs and send these to Log Analytics | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Hardening user applications on servers

| EOT |
| --- |
| **Blueprint guidance** |
| While the Blueprint does not provide specific guidance for hardening user applications for servers, the section below is provided for organisations to describe their implementation of hardening of user applications for servers where it is included within the authorisation boundary for system(s) built using the Blueprint. As most user applications (such as Microsoft Office) are not installed on servers, with the proper implementation of application control and system monitoring, hardening of user applications for servers is likely to be limited in scope. |
| Where an organisation appropriately assesses hardening user applications for servers within another document, it may choose to remove its implementation and assessment from this SSP. However, it is recommended that organisations consider also documenting their approach to hardening operating systems for servers here for a holistic capture of a system’s context and associated risk. |

### Applicability

<INSERT IMPLEMENTATION DETAILS AS APPROPRIATE>

### Organisational policies and processes implemented

<INSERT IMPLEMENTATION DETAILS AS APPROPRIATE>

### Technical controls implemented

<INSERT IMPLEMENTATION DETAILS AS APPROPRIATE>

# Server Application Hardening

| EOT |
| --- |
| **Instruction** |
| The server application hardening section of a System Security Plan (SSP) should document an organisation’s approach to hardening server applications using vendor and ASD guidance. As with other sections of the SSP, information in the server application hardening section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to operating system hardening. When complete, remove any instructional boxes throughout. |

Due to the number of applicable controls in ASD’s [*Guidelines for System Hardening*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-hardening), guidance on system hardening has been split into its five sections for the purpose of this SSP.

| EOT |
| --- |
| **Blueprint guidance** |
| While applicable to any server applications within the scope of a system built using the Blueprint, this section of a SSP particularly relates to the selection of server applications on servers used for on-premises hybrid services and specifically to those applications developed by Microsoft (notably Entra Connect and Exchange Hybrid Configuration Wizard). Organisations should ensure that server application hardening is appropriately assessed and documented for any other systems within the organisation that are used to support the operation of system(s) built using the Blueprint. |

### Applicability

This section of the SSP is applicable to application hardening of applications on on-premises Active Directory and Exchange servers within the system boundary of <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

All vendors of server applications used within <SYSTEM-NAME> have been assessed by <ORGANISATION-NAME> as demonstrating a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products.

* <ORGANISATION-NAME> Vendor Assessment: Microsoft
* <ORGANISATION-NAME> Vendor Assessment: <VENDOR-2>

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for hardening of Entra Connect and Exchange Hybrid Configuration Wizard within <SYSTEM-NAME> are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) and includes the following technical configurations:

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Authentication Hardening

| EOT |
| --- |
| **Instruction** |
| The authentication hardening section of a System Security Plan (SSP) should document an organisation’s approach to hardening user authentication. As with other sections of the SSP, information in the server application hardening section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to operating system hardening. When complete, remove any instructional boxes throughout. |

Due to the number of applicable controls in ASD’s [*Guidelines for System Hardening*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-hardening), guidance on system hardening has been split into its five sections for the purpose of this SSP.

## Authentication hardening

### Applicability

This section of the SSP is applicable to the hardening of authentication methods within the system boundary of <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

<SYSTEM-NAME> provides a central identity store that governs and grants all user access prior to accessing <SYSTEM-NAME> resources. Users are assigned specific user roles according to their business requirements.

Credentials for Break Glass Accounts, local administrator accounts and service accounts are required to be a minimum of 30 characters, uniquely and unpredictably generated, and managed in accordance with the <SYSTEM-NAME> System Administration Process and Procedures, including ensuring that all service accounts are created as Managed Service Accounts.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for authentication hardening within <SYSTEM-NAME>’s are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) and includes the following technical configurations.

Microsoft Entra ID is configured as the central store for identity and access management within <SYSTEM-NAME>, acting as central management for user authentication and authorisation to various Single Sign On (SSO), including as for access to <SYSTEM-NAME> Windows endpoints. Notably, Entra ID implements SAML 2.0, OpenID Connect, and WS-Federation for authentication and authorisation to Microsoft applications and services, with legacy authentication methods disabled.

Technical controls are implemented according to the relevant ISM control topics listed below:

|  |
| --- |
| |  |  | | --- | --- | | **Authenticating to Systems:** | Microsoft Entra ID is configured to require all users to be authenticated before granting access | | **Insecure Authentication Methods:** | legacy authentication methods are disabled | | **Multi-factor and Single Factor Authentication Methods:** | Microsoft Entra ID MFA is enforced for all standard and privileged users accessing Microsoft 365 services | |  | Microsoft Entra ID MFA requires Microsoft Entra ID password and a phishing-resistant MFA method (Windows Hello for Business, passkeys (FIDO2), certificate-based authentication (multifactor)) | |  | Entra ID password/passphrase complexity enforces a minimum of least 4 random words with a total minimum length of 15 characters | |  | none of the authentication factors on their own can be used for single-factor authentication to another system | |  | all authentication attempts are logged in Microsoft Entra ID Sign-ins | |  | Microsoft Entra ID logs are forwarded to a Log Analytics workspace for long-term secure retention | |  | single factor authentication is disabled for all user accounts | | **Setting and Changing Credentials, including for Break Glass Accounts, Local Administrator Accounts and Service Accounts:** | *these control topics relate solely to processes and procedures described above* | | **Protecting Credentials:** | standard Windows & iOS functionality is to obscure passwords during logon | |  | Windows Defender Credential Guard is enabled for <SYSTEM-NAME> Windows endpoints | |  | credentials are stored within Microsoft Entra ID | |  | only one previous logon is cached for <SYSTEM-NAME> Windows endpoints | | **Account Lockouts:** | Microsoft Entra ID Smart Lockout is configured to lock account after five failed logon attempts | | **Session Termination, Session and Screen Locking, and Logon Banner:** | Intune is used to configure Windows and iOS endpoints with with logon banner that reminds users of their security responsibilities when accessing <SYSTEM-NAME> and its resources, and with native screen lock function after 15 minutes of activity | |  | Microsoft Entra ID Conditional Access limits administrative user sessions to 4 hours and non-administrative user sessions to 12 hours | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Virtualisation Hardening

| EOT |
| --- |
| **Instruction** |
| The virtualisation hardening section of a System Security Plan (SSP) should document an organisation’s approach to use of a software-based isolation mechanism to share a physical server’s hardware (virtualisation hardening). As with other sections of the SSP, information in the virtualisation hardening section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance in the Blueprint. Any implementation implied by the below should not be considered as prescriptive as to how organisations must scope, build, document, or assess a system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to operating system hardening. When complete, remove any instructional boxes throughout. |

Due to the number of applicable controls in ASD’s [*Guidelines for System Hardening*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-hardening), guidance on system hardening has been split into its five sections for the purpose of this SSP.

## Virtualisation hardening

### Applicability

This section of the SSP is not applicable to <SYSTEM-NAME> as it does not utilise system virtualisation and as such the requirements of this section are not directly applicable to this SSP. However, <SYSTEM-NAME> does rely on other systems and services that implement virtualisation as part of their hosting.

In particular, <SYSTEM-NAME> leverages system virtualisation components as implemented by Microsoft as part of its Microsoft 365 services. <ORGANISATION-NAME> has assessed the implementation of these as documented in Microsoft’s IRAP assessments, and available in Microsoft’s [Service Trust Portal](https://servicetrust.microsoft.com/) and is satisfied with their implementation as they relate to <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

If and when system virtualisation is considered for future use as part of <ORGANISATION-NAME>’s <SYSTEM-NAME>, <ORGANISATION-NAME> will assess and implement appropriate security controls in relation to its use at that time.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to virtualisation hardening.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# System Management

| EOT |
| --- |
| **Instruction** |
| The system management section of a System Security Plan (SSP) should document an organisation’s approach to system administration, patching, backups and restoration. As with other sections of the SSP, information in the system management section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance from the Blueprint. Any implementation implied by the below text should not be considered as prescriptive of how organisations must scope, build, document, or assess its system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to system administration, patching and backups and restoration. When complete, remove any instructional boxes throughout. |

## System administration

### Applicability

ISM controls relating to the system administration of <SYSTEM-NAME>’s are applicable to and covered by this section of the SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

Administration of Microsoft services within <SYSTEM-NAME> is performed as per <SYSTEM-NAME>’s System Administration Process via a number of Microsoft portals as listed below:

|  |
| --- |
| | Portal | Purpose | URL | | --- | --- | --- | | Microsoft Entra admin centre | Access and administer Microsoft Entra | <https://entra.microsoft.com> | | Microsoft 365 admin centre | Configuration for Microsoft 365 services, including role and licence management, and Microsoft 365 service updates | <https://admin.microsoft.com> | | Microsoft Purview compliance portal | Access eDiscovery and management of data handling policies | <https://purview.microsoft.com> | | Microsoft Defender portal | Monitor and respond to threat activity, and apply protection and response configuration across the environment | <https://security.microsoft.com> | | Microsoft Endpoint Manager admin centre | Manage and secure organisational devices | <https://endpoint.microsoft.com> | | Microsoft 365 Apps admin centre | Create, modify and export Office applications deployment configurations | <https://config.office.com> | | Exchange admin centre | Exchange Online management centre to manage organisation email settings | <https://admin.exchange.microsoft.com> | | Teams admin centre | Manage and monitor the organisation Teams environment including features, licences, policies, and issues | <https://admin.teams.microsoft.com> | | Power Platform admin centre | The unified portal to administer Power Apps, Power Automate, Power Pages, and Power Virtual Agents | <https://admin.powerplatform.microsoft.com> | | SharePoint admin centre | Inform, configure, and govern management of all aspects of SharePoint Online across the tenant | <https://admin.microsoft.com/sharepoint> | | Defender for Cloud Apps portal | Configure and manage threat detection, session controls, data protections, and Shadow IT detection | <https://portal.cloudappsecurity.com> | | Azure Portal | View and manage all aspects of an organisation’s Azure environment | <https://portal.azure.com> | | Network Connectivity Test Tool | Enables measurement of the connectivity between a device and Microsoft’s network for troubleshooting and tuning | <https://connectivity.office.com/> | | Microsoft Teams Call Quality Dashboard | Shows organisation wide information for call and meeting quality with relation to Microsoft Teams | <https://cqd.teams.microsoft.com> | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for system administration of <SYSTEM-NAME> are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) including the following technical configuration.

Administrative access to the above portals is restricted via conditional access to be performed solely from dedicated Secure Administrative Workstations (SAWs), and with appropriate role and attribute based access control applied.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## System patching

### Applicability

ISM controls relating to the system patching within <SYSTEM-NAME> are applicable to and covered by this section of the SSP.

| EOT |
| --- |
| **Blueprint guidance** |
| Organisations with hybrid configurations build on the Blueprint, should consider inclusion of the following words or similar in this section of the SSP: |
| System patching is also applicable to <SYSTEM-NAME>’s on-premise servers that host hybrid components of this system. |

<SYSTEM-NAME> also uses system components as implemented by Microsoft as part of its Microsoft 365 services, and inherits implementation of patching for those systems. <ORGANISATION-NAME> has assessed the implementation of these systems as documented in Microsoft’s IRAP assessments, and available in Microsoft’s [Service Trust Portal](https://servicetrust.microsoft.com/), and is satisfied with their implementation as they relate to <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

System Patching for <SYSTEM-NAME> is performed in accordance with the <SYSTEM-NAME> Patch Management Process .

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for <SYSTEM-NAME>’s implementation of system patching were configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au), and includes the following technical configurations for <SYSTEM-NAME> endpoints and mobile devices via Intune:

* Intune is configured to provide a centralised approach to patching Windows endpoints, and automatically installs updates within 48-hours on all Windows devices
* Windows Update verifies the integrity of patches before installing them
* Microsoft Defender for Endpoint provides a level of continuous vulnerability management capability for all Windows devices.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Data backup and restoration

| EOT |
| --- |
| **Blueprint guidance** |
| While the Blueprint does not provide specific guidance on the implementation of data backups and restoration, the section below is provided for organisations to describe their specific implementation of backups and restoration, including where this is included within the authorisation boundary of system(s) built using the Blueprint. |
| Where organisations appropriately assess this within another document, they may choose to de-scope it from this SSP. However, it is advised that organisations consider tracking this information here for a holistic overview of a system’s context and the associated risks. |

### Applicability

ISM controls relating to the backups and restoration, to the extent that they relate to <SYSTEM-NAME>, are applicable to and covered by this section of the SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

Backups and restoration, including for information within the system boundary of <SYSTEM-NAME>, are performed in accordance with <ORGANISATION-NAME>’s Digital Preservation Policy and associated SOPs:

* [<SYSTEM-NAME> Data Backup Process
* <SYSTEM-NAME> Data Restoration Process

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical Controls Implemented

Technical controls backups and restoration are configured with reference to <RELEVANT-GUIDANCE> and includes the following technical configurations:

* <TECHNICAL-CONFIGURATION-1>
* <TECHNICAL-CONFIGURATION-2>
* <TECHNICAL-CONFIGURATION-3>

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# System Monitoring

| EOT |
| --- |
| **Instruction** |
| The system monitoring section of a System Security Plan (SSP) should document an organisation’s approach to event logging and monitoring. As with other sections of the SSP, information in the system monitoring section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance from the Blueprint. Any implementation implied by the below text should not be considered as prescriptive of how organisations must scope, build, document, or assess its system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to system administration, patching and backups and restoration. When complete, remove any instructional boxes throughout. |

## Event logging and monitoring

### Applicability

ISM controls relating to the system monitoring of <SYSTEM-NAME>’s are applicable to and covered by this section of the SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

The collection of event logs for monitoring of <SYSTEM-NAME> is performed in accordance with <ORGANISATION-NAME>’s Event Logging Policy .

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for system monitoring of <SYSTEM-NAME> are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) including the following technical configuration:

* Defender for Endpoint and Defender for Microsoft 365 centralise logs relating to the security of devices and Microsoft services
* Windows devices and Microsoft 365 services leverage Microsoft’s Window Time service
* Microsoft Entra ID logs authentication events to Log Analytics
* the following events are logged to the local event log on each Windows endpoint:
  + 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
  + DNS and Hypertext Transfer Protocol (HTTP) 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
* logs include the date and time of the event, the relevant user or process, the event description, and the ICT equipment involved are recorded
* logs stored in Log Analytics are protected from unauthorised access, modification and deletion by the Microsoft Entra ID RBAC model.
* Standard Windows users do not have access to modify the local event logs.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Software Development

| EOT |
| --- |
| **Instruction** |
| The software development section of a System Security Plan (SSP) should document an organisation’s approach to application and web application development. As with other sections of the SSP, information in the software development section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance from the Blueprint. Any implementation implied by the below text should not be considered as prescriptive of how organisations must scope, build, document, or assess its system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to system administration, patching and backups and restoration. When complete, remove any instructional boxes throughout. |

As <ORGANISATION-NAME>’s approach to implementing controls related to software development is consistent across all controls addressed within this section, it does not delve into subsections but rather addresses the controls as a group. This approach is consistent with ASD’s [*Guidelines for Software Development*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-software-development).

### Applicability

This section of the SSP is not applicable as <SYSTEM-NAME> does not include any applications nor web applications developed by <ORGANISATION-NAME>, including as part of <SYSTEM-NAME>’s core operation.

If and when the development of applications or web applications is considered for future use within the system boundary of <SYSTEM-NAME>, <ORGANISATION-NAME> will assess and implement appropriate security controls in relation to their use at that time.

However, <SYSTEM-NAME> does leverage software developed by Microsoft as part of its Microsoft 365 services. <ORGANISATION-NAME> has assessed Microsoft’s practices for the development of software as documented in Microsoft’s IRAP assessments, and available in Microsoft’s [Service Trust Portal](https://servicetrust.microsoft.com/) and is satisfied with their implementation as they relate to <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

* None Identified

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

* None Identified

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Database Systems

| EOT |
| --- |
| **Instruction** |
| The database systems section of a System Security Plan (SSP) should document an organisation’s approach to databases and database servers. As with other sections of the SSP, information in this section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance from the Blueprint. Any implementation implied by the below text should not be considered as prescriptive of how organisations must scope, build, document, or assess its system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to databases and database servers. When complete, remove any instructional boxes throughout. |

This section does not include specific subsections as <ORGANISATION-NAME>’s overall approach to implementing security controls in relation to in *Guidelines for Database Systems* for <SYSTEM-NAME> is consistent for all subsections.

As <ORGANISATION-NAME>’s approach to implementing controls related to database systems is consistent across all controls addressed within this section, it does not delve into subsections but rather addresses the controls as a group. This approach is consistent with ASD’s [*Guidelines for Database Systems*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-database-systems).

### Applicability

This section of the SSP is not applicable as <SYSTEM-NAME> does not include any databases, nor does it leverage the use of databases within <ORGANISATION-NAME>. If and when databases are considered for future use within the system boundary of <SYSTEM-NAME>, <ORGANISATION-NAME> will assess and implement appropriate security controls in relation to their use at that time.

However, <SYSTEM-NAME> does use databases as implemented by Microsoft as part of its Microsoft 365 services. <ORGANISATION-NAME> has assessed the implementation of these as documented in Microsoft’s IRAP assessments, and available in Microsoft’s [Service Trust Portal](https://servicetrust.microsoft.com/) and is satisfied with their implementation as they relate to <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

No organisational policies or processes have been implemented in <SYSTEM-NAME> relating to databases.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical Controls Implemented

No technical controls are implemented in <SYSTEM-NAME> relating to databases.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Email

| EOT |
| --- |
| **Instruction** |
| The email section of a System Security Plan (SSP) should document an organisation’s approach to email gateways and servers and email use. As with other sections of the SSP, information in this section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance from the Blueprint. Any implementation implied by the below text should not be considered as prescriptive of how organisations must scope, build, document, or assess its system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to email gateways and servers and email use. When complete, remove any instructional boxes throughout. |

## Email usage

### Applicability

ISM controls relating to the email usage within <SYSTEM-NAME>’s system boundary are applicable to and covered by this section of the SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

The usage of <SYSTEM-NAME>’s email services by users is performed in accordance with the <ORGANISATION-NAME>’s Email Usage Policy.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for email usage within <SYSTEM-NAME> are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) including the following technical configurations:

* <SYSTEM-NAME> applies protective markings based on the classification of the content of emails, including attachments
* users are required to select the classification of emails to apply protective markings
* only appropriate classification options will be presented to <SYSTEM-NAME> users
* Defender for Microsoft 365 will notify users and administrators of blocked emails.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Email gateways and servers

### Applicability

ISM controls relating to the hardening of email routing, including proper interaction with <ORGANISATION-NAME>’s <GATEWAY-SYSTEM>, within <SYSTEM-NAME>’s system boundary are applicable to and covered by this section of the SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

The usage of <SYSTEM-NAME>’s email services by users is performed in accordance with the <ORGANISATION-NAME>’s Email Usage Policy.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for email gateways and servers within <SYSTEM-NAME> are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) including the following technical configurations:

<SYSTEM-NAME> uses Exchange Online within the Microsoft 365 platform. Native Exchange Online security capabilities are enabled to mitigate against email-related threats such as spoofing, phishing and malware.

The advanced features of Defender for Microsoft 365 are enabled within <SYSTEM-NAME> including Safe Attachments and Safe Links, which provide sandboxing of attachments and inspection of hyperlinks respectively. This provides email content filtering and expands on the default protections offered by Exchange Online Protection (EOP).

Exchange Online is configured to:

* ensure OFFICIAL emails *are not routed* through <ORGANISATION-NAME>’s GATEWAY-SYSTEM
* ensure OFFICIAL:Sensitive and above emails *are routed* through <ORGANISATION-NAME>’s GATEWAY-SYSTEM
* encrypt traffic between external users with TLS 1.2, and then forward emails to <ORGANISATION-NAME>’s GATEWAY-SYSTEM via an Exchange connector
* not act as an open relay
* implement TLS 1.2 for opportunistic TLS encryption where supported by the other mail server
* implement Mail Transfer Agent - Strict Transport Security (MTA-STS) for outbound mail flow
* configure Sender Policy Framework (SPF) using a hard fail record
* keep SPF blocks visible to the recipients
* configure the appropriate use of DomainKeys Identified Mail (DKIM)
* verify DKIM signatures on received emails
* implement <ORGANISATION-NAME>’s Domain-based Message Authentication, Reporting and Conformance (DMARC) records

Defender for Microsoft 365 provides content filtering including sandboxing of attachments (Safe Attachments) and inspection of links (Safe Links).

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

* <ORGANISATION-NAME>

# Networking

| EOT |
| --- |
| **Instruction** |
| The networking section of a System Security Plan (SSP) should document an organisation’s approach to networking design and configuration, wireless networks and service continuity for online services. As with other sections of the SSP, information in this section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance from the Blueprint. Any implementation implied by the below text should not be considered as prescriptive of how organisations must scope, build, document, or assess its system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to networking design and configuration, wireless networks and service continuity for online services. When complete, remove any instructional boxes throughout. |

## Network design and configuration

### Applicability

This section of the SSP is not applicable as physical networks are not implemented as part of <SYSTEM-NAME>. Instead, <SYSTEM-NAME> utilises <ORGANISATION-NAME>’s WIRELESS-NETWORK-SYSTEM and/or WIRED-NETWORK-SYSTEM to provide these services for <SYSTEM-NAME> ICT equipment. However, <SYSTEM-NAME> does implement extensive logical data flows for connecting to and between Microsoft 365 services and this section is applicable to the management of these data flows.

<SYSTEM-NAME> also uses both physical and logical networking components as implemented by Microsoft as part of its Microsoft 365 services. <ORGANISATION-NAME> has assessed the implementation of these as documented in Microsoft’s IRAP assessments, and available in Microsoft’s [Service Trust Portal](https://servicetrust.microsoft.com/), and is satisfied with their implementation as they relate to <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

Technical documentation of <SYSTEM-NAME>’s logical data flows for connecting to and between Microsoft services are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) including the Microsoft 365 design, which includes a high-level network diagram showing the components that are considered in-scope and a last updated date.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for logical networking for connecting to and between Microsoft services associated with <SYSTEM-NAME> are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) including the following technical configurations:

* all communication between <SYSTEM-NAME>’s Windows endpoints and Microsoft 365 components is encrypted by TLS
* conditional Access policies are configured to restrict access to only specified geographic regions within Australia
* <SYSTEM-NAME> also uses Microsoft Entra ID Identity Protection to analyse sign-in logs to identify and notify administrators when users are identified as originating from anonymous proxy IP addresses.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Wireless networks

### Applicability

This section of the SSP is not applicable as <SYSTEM-NAME> does not implement wireless networks. Instead, <SYSTEM-NAME> utilises <ORGANISATION-NAME>’s WIRELESS-NETWORK-SYSTEM to provide these services for <SYSTEM-NAME> endpoints.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

No organisational policies or processes have been implemented in <SYSTEM-NAME> relating to wireless networks.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to wireless networks.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Service continuity for online services

### Applicability

This section of the SSP is not directly applicable to <SYSTEM-NAME> as <SYSTEM-NAME> does not include the hosting of online services, nor does it leverage the use of online services within <ORGANISATION-NAME> as part of its operation.

If and when <SYSTEM-NAME> is considered for hosting online services, <ORGANISATION-NAME> will assess and implement security controls relating to ensuring their service continuity at that time.

However, <SYSTEM-NAME> does use online services as implemented by Microsoft as part of its Microsoft 365 services. <ORGANISATION-NAME> has assessed the implementation of these as documented in Microsoft’s IRAP assessments, and available in Microsoft’s [Service Trust Portal](https://servicetrust.microsoft.com/) and is satisfied with their implementation as they relate to <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

No organisational policies or processes have been implemented in <SYSTEM-NAME> relating to the hosting of online services.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to the hosting of online services.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Cryptography

| EOT |
| --- |
| **Instruction** |
| The cryptography section of a System Security Plan (SSP) should document an organisation’s approach to cryptography, TLS, SSH, S/MiME and IPSec. As with other sections of the SSP, information in this section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance from the Blueprint. Any implementation implied by the below text should not be considered as prescriptive of how organisations must scope, build, document, or assess its system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to cryptography, TLS, SSH, S/MiME and IPSec. When complete, remove any instructional boxes throughout. |

## Cryptographic fundamentals

### Applicability

ISM controls relating to cryptography, including cryptographic algorithms as implemented by Microsoft as part of its Microsoft 365 services, within <SYSTEM-NAME>’s system boundary are applicable to and covered by this section of the SSP. <ORGANISATION-NAME> has assessed the implementation of these components as documented in Microsoft’s IRAP assessments, and available in Microsoft’s [Service Trust Portal](https://servicetrust.microsoft.com/), and is satisfied with their implementation as they relate to <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

No organisational policies or processes have been implemented in <SYSTEM-NAME> relating to cryptographic fundamentals.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for <SYSTEM-NAME>’s implementation of cryptography are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) including the following technical configurations:

* Microsoft BitLocker is configured on endpoints for disk encryption leveraging AES which is an AACA
* Microsoft BitLocker is configured to provide full disk encryption of <SYSTEM-NAME>’s mobile devices, implementing AES-256
* BitLocker recovery keys are stored in Microsoft Entra ID
* TLS with AES is used to protect traffic to and from Azure and Microsoft 365 servers over the internet.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## ASD-approved cryptographic algorithms

### Applicability

ISM controls relating to cryptography, including cryptographic algorithms as implemented by Microsoft as part of its Microsoft 365 services, within <SYSTEM-NAME>’s system boundary are applicable to and covered by this section of the SSP. <ORGANISATION-NAME> has assessed the implementation of these components as documented in Microsoft’s IRAP assessments, and available in Microsoft’s [Service Trust Portal](https://servicetrust.microsoft.com/), and is satisfied with their implementation as they relate to <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

No organisational policies or processes have been implemented in <SYSTEM-NAME> relating to ASD-approved cryptographic algorithms.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for <SYSTEM-NAME>’s implementation of AACAs are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) including the following technical configurations:

* BitLocker is configured to use AES-256 encryption.

<SYSTEM-NAME>’s use of Microsoft 365 also inherits the following technical configurations from Microsoft:

* Microsoft Azure and Microsoft 365 services:
* implement AACAs where possible
* implement Elliptic-Curve Diffie-Hellman Ephemeral (ECDHE) as the preferred algorithm
* do not use Diffie-Hellman (DH)
* do not use Digital Signature Algorithm (DSA)
* implement National Institute of Standards and Technology (NIST) P-256 and P-384
* use a 256-bit key where possible for Elliptic-Curve Diffie-Hellman (ECDH)
* use a 2048-bit key for Rivest–Shamir–Adleman (RSA)
* use separate RSA key pairs for these purposes
* use SHA-384 as the preferred hashing algorithm for Microsoft 365 TLS components.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## ASD-approved cryptographic protocols

### Applicability

ISM controls relating to cryptography, including cryptographic algorithms as implemented by Microsoft as part of its Microsoft 365 services, within <SYSTEM-NAME>’s system boundary are applicable to and covered by this section of the SSP. <ORGANISATION-NAME> has assessed the implementation of these controls as documented in Microsoft’s IRAP assessments, and available in Microsoft’s [Service Trust Portal](https://servicetrust.microsoft.com/) and is satisfied with their implementation as they relate to <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

No organisational policies or processes have been implemented in <SYSTEM-NAME> relating to ASD-approved cryptographic protocols.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical Controls Implemented

<SYSTEM-NAME>’s use of Microsoft 365 inherits the following technical controls from Microsoft:

* Microsoft Azure and Microsoft 365 services implement AACPs where possible.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Transport Layer Security (TLS)

### Applicability

ISM controls relating to implementation of TLS, including TLS as implemented by Microsoft as part of its Microsoft 365 services, within <SYSTEM-NAME>’s system boundary are applicable to and covered by this section of the SSP. <ORGANISATION-NAME> has assessed the implementation of these components as documented in Microsoft’s IRAP assessments, and available in Microsoft’s [Service Trust Portal](https://servicetrust.microsoft.com/), and is satisfied with their implementation as they relate to <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

No organisational policies or processes have been implemented in <SYSTEM-NAME> relating to TLS.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

<SYSTEM-NAME>’s use of Microsoft 365 inherits the following technical controls from Microsoft:

* Microsoft Azure and Microsoft 365 services:
* implement TLS
* however, <ORGANISATION-NAME> notes that Microsoft services do not currently allow organisations to select which TLS versions to use
* implement AES in Galois Counter Mode (GCM)
* implement secure renegotiation
* implement ECDHE as the preferred algorithm
* Perfect Forward Secrecy is used when ECDHE is prioritised
* use SHA-2 based certificates
* use SHA-2 as part of the Message Authentication Code and Pseudo-Random Function
* disable TLS compression.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Secure Shell (SSH)

### Applicability

The section of the SSP is not applicable as <SYSTEM-NAME> does not directly implement Secure Shell (SSH) in its administration or configuration. However, <SYSTEM-NAME> does rely on other systems and services that implement SSH as part of their administration and configuration.

In particular, <SYSTEM-NAME> uses both physical and logical networking components as implemented by Microsoft as part of its Microsoft 365 services. <ORGANISATION-NAME> has assessed the implementation of these components as documented in Microsoft’s IRAP assessments, and available in Microsoft’s [Service Trust Portal](https://servicetrust.microsoft.com/), and is satisfied with their implementation as they relate to <SYSTEM-NAME>.

If and when SSH is implemented in future use as part of <SYSTEM-NAME>, <ORGANISATION-NAME> will assess and implement appropriate security controls in relation to its configuration at that time.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

No organisational policies or processes have been implemented in <SYSTEM-NAME> relating to SSH.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to SSH.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Secure/Multipurpose Internet Mail Extension (S/MiME)

### Applicability

This section of the SSP is not applicable as <SYSTEM-NAME> does not implement S/MIME in its administration or configuration, nor does it leverage the use of S/MIME within <ORGANISATION-NAME>.

If and when S/MIME is implemented in future use as part of <SYSTEM-NAME>, <ORGANISATION-NAME> will assess and implement appropriate security controls in relation to its configuration at that time.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

No organisational policies or processes have been implemented in <SYSTEM-NAME> relating to S/MiME.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to S/MiME.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Internet Protocol Security (IPsec)

### Applicability

The section of the SSP is not applicable as <SYSTEM-NAME> does not directly implement IPsec in its administration or configuration. However, <SYSTEM-NAME> does rely on other systems and services that implement IPsec as part of their administration and configuration.

In particular, <SYSTEM-NAME> leverages both physical and logical networking components as implemented by Microsoft as part of its Microsoft 365 services. <ORGANISATION-NAME> has assessed the implementation of these components as documented in Microsoft’s IRAP assessments, and available in Microsoft’s [Service Trust Portal](https://servicetrust.microsoft.com/), and is satisfied with their implementation as they relate to <SYSTEM-NAME>.

If and when IPSec is implemented in future use as part of <SYSTEM-NAME>, <ORGANISATION-NAME> will assess and implement appropriate security controls in relation to its configuration at that time.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

No organisational policies or processes have been implemented in <SYSTEM-NAME> relating to IPsec.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to IPsec.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Gateways

| EOT |
| --- |
| **Instruction** |
| The gateways section of a System Security Plan (SSP) should document an organisation’s approach to gateways, cross domain solutions, firewalls, diodes, web proxies and content filtering and peripheral switches. As with other sections of the SSP, information in this section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance from the Blueprint. Any implementation implied by the below text should not be considered as prescriptive of how organisations must scope, build, document, or assess its system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to gateways, cross domain solutions, firewalls, diodes, web proxies and content filtering and peripheral switches. When complete, remove any instructional boxes throughout. |

## Gateways

| EOT |
| --- |
| **Blueprint guidance** |
| The Blueprint does not cover management of gateways and the below template excludes these from the scope of a SSP for systems built on the Blueprint. However, the implementation of demilitarised zones, traffic inspections and filtering is often conducted as part of a separate system specific to these services and should be documented elsewhere. |
| Where organisations decides to implement their own internal gateways, cross domain solutions or diodes within the boundary of a system built on the Blueprint, they are responsible for assessing and documenting the risk and applicability associated with each individual security control and describing the implementation of these controls here. |

### Applicability

This section of the SSP is not applicable as <SYSTEM-NAME> does not include gateways. Instead, <SYSTEM-NAME> utilises <ORGANISATION-NAME>’s GATEWAY-SYSTEM to provide these services.

<SYSTEM-NAME> also leverages gateways as implemented by Microsoft as part of its Microsoft 365 services. <ORGANISATION-NAME> has assessed the implementation of these as documented in Microsoft’s IRAP assessments, and available in Microsoft’s [Service Trust Portal](https://servicetrust.microsoft.com/), and is satisfied with their implementation as they relate to <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

No organisational policies or processes have been implemented in <SYSTEM-NAME> relating to

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to gateways.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Cross domain solutions (CDS)

### Applicability

The section of the SSP is not applicable as <SYSTEM-NAME> does not include any CDSs, nor does it leverage the use of any CDSs within <ORGANISATION-NAME>. If and when CDSs are considered for future use as part of <SYSTEM-NAME>, <ORGANISATION-NAME> will assess and implement appropriate security controls in relation to their use at that time.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

No organisational policies or processes have been implemented in <SYSTEM-NAME> relating to CDSs.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to CDSs.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Firewalls

### Applicability

The section of the SSP is not applicable as <SYSTEM-NAME> does not include any firewalls. Instead, <SYSTEM-NAME> leverages the use of <ORGANISATION-NAME>’s GATEWAY-SYSTEM to provide these services.

<SYSTEM-NAME> also leverages firewalls as implemented by Microsoft as part of its Microsoft 365 services. <ORGANISATION-NAME> has assessed the implementation of these as documented in Microsoft’s IRAP assessments, and available in Microsoft’s [Service Trust Portal](https://servicetrust.microsoft.com/), and is satisfied with their implementation as they relate to <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

No organisational policies or processes have been implemented in <SYSTEM-NAME> relating to firewalls.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to firewalls.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Diodes

### Applicability

This section of the SSP is not applicable as <SYSTEM-NAME> does not include any diodes, nor does it leverage the use of any diodes within <ORGANISATION-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

No organisational policies or processes have been implemented in <SYSTEM-NAME> relating to diodes.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to diodes.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Web proxies

| EOT |
| --- |
| **Blueprint guidance** |
| While Microsoft Defender for Cloud Apps configured as a Cloud Access Security Broker (CASB) can provide proxy functionality for Microsoft 365 traffic, use of CASB is generally in addition to an organisation’s gateway and as such their configuration is not currently covered by the Blueprint. |

### Applicability

ISM controls relating to the use of web proxies, including generated logs configured as part of <ORGANISATION-NAME>’s GATEWAY-SYSTEM, within <SYSTEM-NAME>’s system boundary are applicable to and covered by this section of the SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

<ORGANISATION-NAME> has developed a Web Usage Policy that governs appropriate web usage on <SYSTEM-NAME>.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

All <SYSTEM-NAME> web access, including that of internal servers, is configured to be conducted through <ORGANISATION-NAME>’s GATEWAY-SYSTEM web proxy.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Web content filters

### Applicability

ISM controls relating to the web content filters within <SYSTEM-NAME>’s system boundary are applicable to and covered by this section of the SSP as <SYSTEM-NAME> uses <ORGANISATION-NAME>’s GATEWAY-SYSTEM for effective holistic management of web content filtering. Please see the GATEWAY-SYSTEM SSP and IRAP assessment for its implementation of the relevant controls.

However, <SYSTEM-NAME> does implement a defence-in-depth approach to its implementation of web content filtering, particularly for web content accessed via the Edge browser on Intune configured Windows endpoints, as configured by Windows Defender for Endpoint. The controls discussed in this section of the SSP relate to implementation of these controls.

Notably, this web filtering relates only to this scenario and not to other browsers on Intune configured Windows endpoints, nor to other systems such as Windows Server or iOS devices. These devices rely solely on the aforementioned gateway level implementation of web content filtering.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

Web content filtering as implemented within <SYSTEM-NAME> is performed according to allowed web categories as per <ORGANISATION-NAME>’s Web Usage Policy .

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for <SYSTEM-NAME>’s implementation of web content filtering (as scoped above) are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) including the following technical configurations on Windows endpoints:

* web content filtering is enabled for Windows devices using Microsoft Defender for Endpoint
* client-side active content, including all Java and Flash content, is blocked on all Windows devices
* Microsoft Defender for Endpoint blocks specific web categories that are maintained by Microsoft.

For information on implementation of web content filtering via <ORGANISATION-NAME>’s GATEWAY-SYSTEM, please see the GATEWAY-SYSTEM SSP and IRAP assessment.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Content filtering

### Applicability

ISM controls relating to the content filtering within <SYSTEM-NAME>’s system boundary are applicable to and covered by this section of the SSP as <SYSTEM-NAME> uses <ORGANISATION-NAME>’s GATEWAY-SYSTEM for effective holistic management of web content filtering. Please see the GATEWAY-SYSTEM SSP and IRAP assessment for its implementation of the relevant controls.

However, <SYSTEM-NAME> does implement a defence-in-depth approach to its implementation of web content filtering, particularly in leveraging Microsoft 365 capabilities including Defender for Microsoft 365 and Exchange Online Protection to inspect and manage email traffic.

Notably, this web filtering relates only to this scenario and not to other parts of <SYSTEM-NAME>, including Windows Server or iOS devices. These devices rely solely on the aforementioned gateway level implementation of content filtering.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

Content filtering as implemented within <SYSTEM-NAME> is performed to meet allowed web categories as allowed by the <SYSTEM-NAME> System Usage Policy.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for <SYSTEM-NAME>’s implementation of web content filtering (as scoped above) are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) including the following technical configurations on Windows endpoints:

* Exchange Online Protection and Defender for Microsoft 365 are configured to prevent specific file types from entering <SYSTEM-NAME> via email
* Defender for Microsoft 365 provides content filtering including sandboxing of attachments (Safe Attachments) and inspection of links (Safe Links)
* multiple scanning engines are provided by Exchange Online Protection, Defender for Microsoft 365 and Defender for Endpoint
* archives are scanned for malware
* Defender for Microsoft 365 alerts are configured
* integrity of patches is verified before installation.

For implementation of content filtering by <ORGANISATION-NAME>’s GATEWAY-SYSTEM, please see the GATEWAY-SYSTEM SSP and IRAP assessment.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Peripheral switches

### Applicability

This section of the SSP is not applicable as <SYSTEM-NAME> does not include any peripheral switches, nor does it leverage the use of peripheral switches within <ORGANISATION-NAME>. If and when peripheral switches are considered for future use as part of <SYSTEM-NAME>, <ORGANISATION-NAME> will assess and implement appropriate security controls in relation to their use at that time.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

No organisational policies or processes have been implemented in <SYSTEM-NAME> relating to peripheral switches.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

No technical controls are implemented in <SYSTEM-NAME> relating to peripheral switches.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

* <ORGANISATION-NAME> GATEWAY-SYSTEM
* <ORGANISATION-NAME> GATEWAY-SYSTEM
* <SYSTEM-NAME>
* <SYSTEM-NAME>

# Data Transfers

| EOT |
| --- |
| **Instruction** |
| The cryptography section of a System Security Plan (SSP) should document an organisation’s approach to data transfers. As with other sections of the SSP, information in this section should be documented according to the relevant controls outlined in ASD’s ISM and the SSP Annex. |
| All template text refers to a typical implementation of a system built using the Blueprint, and includes reference to organisational policies, processes and technical configurations to be implemented in addition to the technical controls that may be configured using guidance from the Blueprint. Any implementation implied by the below text should not be considered as prescriptive of how organisations must scope, build, document, or assess its system. |
| When completing the below template, organisations should insert and update information where relevant to ensure it accurately represents their approach to data transfers. When complete, remove any instructional boxes throughout. |

## Data transfers

### Applicability

ISM controls relating to data transfers within <SYSTEM-NAME>’s system boundary are applicable to and covered by this section of the SSP.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Organisational policies and processes implemented

Data transfers associated with <SYSTEM-NAME> are performed in accordance with <SYSTEM-NAME>’s Data Transfer Process , which outlines the processes and methods that can be used to transfer data into or out of <SYSTEM-NAME>.

<ORGANISATION-NAME>’s Security Operations Centre (SOC) will monitor data transfer logs in accordance with <SYSTEM-NAME>’s Continuous Monitoring Plan .

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Technical controls implemented

Technical controls for <SYSTEM-NAME>’s implementation of data transfers are configured with reference to ASD’s [*Blueprint for Secure Cloud*](https://blueprint.asd.gov.au) including the following technical configurations:

* Defender for Endpoint will scan all data copied onto Windows 11 devices
* event logs are generated when data is transferred from a Windows 11 endpoint to external media. These Logs are then centrally stored and monitored.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

* <SYSTEM-NAME>
* <SYSTEM-NAME>