Essential Eight Documentation | Template

This template provides the content of ASD’s Essential Eight Maturity Model 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

# Essential Eight

| EOT |
| --- |
| **Instruction** |
| The Essential Eight sections of a System Security Plan (SSP) should document the Essential Eight Maturity levels associated with implementation of a system. 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 the organisation 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 the Essential Eight Maturity levels associated with implementation of their system. When complete, remove any instructional boxes throughout. |

| EOT |
| --- |
| **Blueprint guidance** |
| As with implementation of ISM controls, the Blueprint does not itself *achieve* any particular Essential Eight Maturity levels, but rather assists organisations in designing and building systems to achieve their desired maturity level based on their own operating context. |

<SYSTEM-NAME> targets the following maturity levels against each Essential Eight Mitigation Strategy:

|  |
| --- |
| | Mitigation Strategy | Targeted Maturity Level | Current Assessed Maturity Level | | --- | --- | --- | | Patch applications | <TARGET-LEVEL> | <ASSESSED-LEVEL> | | Patch operating systems | <TARGET-LEVEL> | <ASSESSED-LEVEL> | | Multi-factor authentication | <TARGET-LEVEL> | <ASSESSED-LEVEL> | | Restrict administrative privileges | <TARGET-LEVEL> | <ASSESSED-LEVEL> | | Application control | <TARGET-LEVEL> | <ASSESSED-LEVEL> | | Restrict Microsoft Office macros | <TARGET-LEVEL> | <ASSESSED-LEVEL> | | User application hardening | <TARGET-LEVEL> | <ASSESSED-LEVEL> | | Regular backups | <TARGET-LEVEL> | <ASSESSED-LEVEL> | |  |  |  | |
|  |

# Patch Applications

| EOT |
| --- |
| **Instruction** |
| The Essential Eight sections of a System Security Plan (SSP) should document the Essential Eight Maturity levels associated with implementation of a system. 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 the organisation 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 the Essential Eight Maturity levels associated with implementation of their system. When complete, remove any instructional boxes throughout. |

| EOT |
| --- |
| **Blueprint guidance** |
| For applicable government organisations to meet the minimum requirements established under the [*Protective Security Policy Framework* (PSPF)](https://www.protectivesecurity.gov.au/publications-library/policy-10-safeguarding-data-cyber-threats) maturity model, these organisations must implement Maturity Level Two for each of the below components of ASD’s [*Essential Eight Maturity Model*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight). |
| As with implementation of ISM controls, the Blueprint does not itself *achieve* any particular Essential Eight Maturity levels, but rather assists organisations in designing and building systems to achieve their desired maturity level based on their own operating context. |

## Applicability

The Patch Applications mitigation strategy is applicable to the appropriate patching of applications for the following components of <SYSTEM-NAME>:

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

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Maturity Level

|  |
| --- |
| |  |  | | --- | --- | | Targeted: | <TARGET-LEVEL> | | Currently Assessed: | <ASSESSED-LEVEL> | |
|  |

## Implementation

### Asset discovery

| EOT |
| --- |
| **Essential Eight guidance** |
| All maturity levels require that an automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities. |

| EOT |
| --- |
| **Blueprint guidance** |
| The Blueprint design does not provide guidance for direct management of asset discovery, though the below template serves as a guide of a typical implementation of this section for systems built using the Blueprint. |

<ASSET-DISCOVERY-TOOL> is used to scan for all assets within <SYSTEM-NAME>.

<ASSET-DISCOVERY-TOOL> performs an asset discovery scan on a <FORTNIGHTLY> basis.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Vulnerability scanning

| EOT |
| --- |
| **Essential Eight guidance** |
| All maturity levels require that a vulnerability scanner is used to identify missing patches or updates for vulnerabilities in a variety of applications per the below table, that this vulnerability scanner uses an up-to-date vulnerability database. |
| | Application Type | ML1 | ML2 | ML3 | | --- | --- | --- | --- | | Online services: | Daily | Daily | Daily | | Core applications:\* | Weekly | Weekly | Weekly | | Other applications: | - | Fortnightly | Fortnightly | |
| \**For the purposes of the above table, are defined as office productivity suites, web browsers and their extensions, email clients, PDF software and security products.* |

| EOT |
| --- |
| **Blueprint guidance** |
| The Blueprint design does not provide guidance for direct management of vulnerability scanning, though the below template serves as a guide of a typical implementation of this section for systems built using the Blueprint. |
| Given that scanning is generally performed on an asset basis rather than an application basis, the below describes the scanning of all applications on endpoints on a weekly basis, while on-premise servers are described as being scanned on a daily basis (to account for the requirements outlined in *Patch Operating Systems*), particularly to account for internet facing servers including Exchange servers. |
| It is assumed for the below that the system built using the Blueprint does not host online services. |

<VULNERABILITY-SCANNING-TOOL> is used to scan for all application vulnerabilities on endpoints and servers within <SYSTEM-NAME>. <VULNERABILITY-SCANNING-TOOL> is configured to update its vulnerability database on a <nightly> basis.

#### Windows endpoints

<VULNERABILITY-SCANNING-TOOL> is configured to scan all Windows endpoints discovered by <ASSET-DISCOVERY-TOOL>, performing vulnerability scans on a weekly basis.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

#### Hybrid servers

<VULNERABILITY-SCANNING-TOOL> is configured to scan all hybrid servers discovered by <ASSET-DISCOVERY-TOOL>, performing vulnerability scans on a daily basis.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

#### Servers for online services

<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, and as such the scanning of vulnerabilities in these services is not applicable.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Patching

| EOT |
| --- |
| **Essential Eight guidance** |
| The below table outlines the time-frames for different application types, as well as the criticality or exploitability of vulnerabilities in these applications. |
| | Application Type | Critical Vulnerabilityor Exploit Available | ML1 | ML2 | ML3 | | --- | --- | --- | --- | --- | | Online services: | Yes | 48 Hours | 48 Hours | 48 Hours | |  | No | 2 Weeks | 2 Weeks | 2 Weeks | |  |  |  |  |  | | Core applications:\* | Yes | 2 Weeks | 2 Weeks | 48 Hours | |  | No | 2 Weeks | 2 Weeks | 2 Weeks | |  |  |  |  |  | | Other applications: | Yes | - | 1 Month | 1 Month | |  | No | - | 1 Month | 1 Month | |
| \**For the purposes of the above table, are defined as office productivity suites, web browsers and their extensions, email clients, PDF software and security products.* |

| EOT |
| --- |
| **Blueprint guidance** |
| The Blueprint provides guidance for using Microsoft Intune to deploy applications and patches to workstations, though the use of this mechanism generally relies on manual processes to choose to deploy relevant patches. |

#### Windows endpoints

Patches for all applications on windows endpoints are managed and deployed using Microsoft Intune, and applied using Microsoft Defender for Endpoint.

In accordance with the <SYSTEM-NAME> Vulnerability and Patch Management Process, vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products discovered by <VULNERABILITY-SCANNING-TOOL> are applied within 48 hours where these vulnerabilities are assessed as critical by vendors or when working exploits exist, and applied within 2 weeks otherwise.

Patches for vulnerabilities in all other applications on <SYSTEM-NAME> endpoints are applied within 1 month.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

#### Hybrid servers

Patches for all applications on hybrid servers are applied using <server patch deployment mechanism>.

In accordance with the <SYSTEM-NAME> Vulnerability and Patch Management Process, vulnerabilities in web browsers and security products discovered by <VULNERABILITY-SCANNING-TOOL> are applied within 48 hours where these vulnerabilities are assessed as critical by vendors or when working exploits exist, and applied within 2 weeks otherwise.

<SYSTEM-NAME> hybrid servers do not have office productivity suites, web browser extensions, email clients, PDF software (other than web browsers), or Adobe Flash Player installed.

Patches for vulnerabilities in all other applications on <SYSTEM-NAME> hybrid servers are applied within 1 month.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

#### Servers for online services

<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, and as such the application of patches for these services is not applicable.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Removal of unsupported applications

| EOT |
| --- |
| **Essential Eight guidance** |
| All maturity levels require that online services, as well as any office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed. |

#### Windows endpoints

In accordance with the <SYSTEM-NAME> Vulnerability and Patch Management Process, <ORGANISATION-NAME> will monitor vendor support of applications used for all <SYSTEM-NAME> components, and ensure that all unsupported applications are removed prior to this support ending.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

#### Hybrid servers

In accordance with the <SYSTEM-NAME> Vulnerability and Patch Management Process, <ORGANISATION-NAME> will monitor vendor support of applications used for all <SYSTEM-NAME> components, and ensure that all unsupported applications are removed prior to this support ending.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

#### Servers for online services

<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, and as such the removal of unsupported online services is not applicable.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Patch Operating Systems

| EOT |
| --- |
| **Instruction** |
| The Essential Eight sections of a System Security Plan (SSP) should document the Essential Eight Maturity levels associated with implementation of a system. 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 the organisation 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 the Essential Eight Maturity levels associated with implementation of their system. When complete, remove any instructional boxes throughout. |

| EOT |
| --- |
| **Blueprint guidance** |
| For applicable government organisations to meet the minimum requirements established under the [*Protective Security Policy Framework* (PSPF)](https://www.protectivesecurity.gov.au/publications-library/policy-10-safeguarding-data-cyber-threats) maturity model, these organisations must implement Maturity Level Two for each of the below components of ASD’s [*Essential Eight Maturity Model*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight). |
| As with implementation of ISM controls, the Blueprint does not itself *achieve* any particular Essential Eight Maturity levels, but rather assists organisations in designing and building systems to achieve their desired maturity level based on their own operating context. |

## Applicability

The Patch Operating Systems mitigation strategy is applicable to the appropriate patching of operating systems for the following components of <SYSTEM-NAME>:

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

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Maturity Level

|  |
| --- |
| |  |  | | --- | --- | | Targeted: | <TARGET-LEVEL> | | Currently Assessed: | <ASSESSED-LEVEL> | |
|  |

## Implementation

### Asset discovery

| EOT |
| --- |
| **Blueprint guidance** |
| The Blueprint design does not provide guidance for management of asset discovery, though the below template serves as a guide of a typical implementation of this section for systems built using the Blueprint. |
| All maturity levels require that an automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities. |

<ASSET-DISCOVERY-TOOL> is used to scan for all assets within <SYSTEM-NAME>.

<ASSET-DISCOVERY-TOOL> performs an asset discovery scan on a <FORTNIGHTLY> basis.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Vulnerability scanning

| EOT |
| --- |
| **Essential Eight guidance** |
| All maturity levels require that a vulnerability scanner is used to identify missing patches or updates for vulnerabilities in a variety of applications per the below table, that this vulnerability scanner uses an up-to-date vulnerability database. |
| | Asset Type | Layer | ML1 & ML2 | ML3 | | --- | --- | --- | --- | | Internet-facing servers/network devices: | Operating System | Daily | Daily | |  | Drivers | Fortnightly | Fortnightly | |  | Firmware | Fortnightly | Fortnightly | |  |  |  |  | | Other (including workstations): | Operating System | Fortnightly | Fortnightly | |  | Drivers | Fortnightly | Fortnightly | |  | Firmware | Fortnightly | Fortnightly | |

| EOT |
| --- |
| **Blueprint guidance** |
| The Blueprint design does not provide guidance for management of vulnerability scanning, though the below template serves as a guide of a typical implementation of this section for systems built using the Blueprint. |
| Given that scanning is generally performed on an asset basis rather than an application basis, and that the patching of applications calls for weekly scans to be run the below describes the scanning of endpoints on a weekly basis, while on-premise servers are described as being scanned on a daily basis, particularly to account for internet facing servers including Exchange servers. |

<VULNERABILITY-SCANNING-TOOL> is used to scan for all operating system, DRIVER, AND FIRMWARE vulnerabilities on endpoints and servers AND NETWORK DEVICES within <SYSTEM-NAME>. <VULNERABILITY-SCANNING-TOOL> is configured to update its vulnerability database on a <nightly> basis.

#### Windows Endpoints

<VULNERABILITY-SCANNING-TOOL> is configured to scan all Windows endpoints discovered by <ASSET-DISCOVERY-TOOL>, performing vulnerability scans on a WEEKLY basis.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

#### Hybrid 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 its implementation for the system, where this management is included within the authorisation boundary for the system built using the Blueprint. However, implementation of this hardening is also often completed as part of a separate system specific to these servers. |
| Where an organisation appropriately assesses this within another document, it may choose to remove its implementation and assessment from this particular SSP, though it is advised that organisations consider tracking this here for a holistic capture of the system context and associated risk. |

<VULNERABILITY-SCANNING-TOOL> is configured to scan all hybrid servers discovered by <ASSET-DISCOVERY-TOOL>, performing vulnerability scans on a daily basis.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Patching

| EOT |
| --- |
| **Essential Eight guidance** |
| The below table outlines the time-frames for different application types, as well as the criticality or exploitability of vulnerabilities in these applications. |
| Internet-facing servers/network devices |
| | Asset Type | Layer | Critical Vulnerability or Exploit Available | ML1 & ML2 | ML3 | | --- | --- | --- | --- | --- | | Internet-facing servers/network devices: | Operating System: | Yes | 48 Hours | 48 Hours | |  |  | No | 2 Weeks | 2 Weeks | |  | Drivers: | Yes | - | 48 Hours | |  |  | No | - | 1 Month | |  | Firmware: | Yes | - | 48 Hours | |  |  | No | - | 1 Month | | Other (including workstations): | Operating System: | Yes | 1 Month | 48 Hours | |  |  | No | 1 Month | 1 Month | |  | Drivers: | Yes | - | 48 Hours | |  |  | No | - | 1 Month | |  | Firmware: | Yes | - | 48 Hours | |

| EOT |
| --- |
| **Blueprint guidance** |
| The Blueprint provides guidance for using Microsoft Intune to deploy applications and patches to workstations, though the use of this mechanism generally relies on manual processes to choose to deploy relevant patches. The patching schedule described below aligns with Maturity Level Three, but should be adjusted to what is implemented within an organisation. |
| The below implementation also treats all on-premise hybrid servers as if they are internet connected for the purposes of the above table, but this should similarly be adjusted to what is implemented within the organisation. |

#### Windows endpoints

Patches for operating systems on windows endpoints are managed and deployed using Microsoft Intune, and applied using Microsoft Defender for Endpoint.

In accordance with the <SYSTEM-NAME> Vulnerability and Patch Management Process, vulnerabilities in operating systems, DRIVERS AND FIRMWARE discovered by <VULNERABILITY-SCANNING-TOOL> are applied within 48 HOURS where these vulnerabilities are assessed as critical by vendors or when working exploits exist, and applied within ONE MONTH otherwise.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

#### Hybrid servers

Patches for operating systems, DRIVERS AND FIRMWARE on hybrid servers are applied using <SERVER PATCH DEPLOYMENT MECHANISM>.

In accordance with the <SYSTEM-NAME> Vulnerability and Patch Management Process, vulnerabilities in operating systems, drivers and firmware discovered by <VULNERABILITY-SCANNING-TOOL> are applied within 48 hours where these vulnerabilities are assessed as critical by vendors or when working exploits exist, and applied within 2 weeks otherwise.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Removal of unsupported operating systems

| EOT |
| --- |
| **Essential Eight Guidance** |
| All maturity levels require that operating systems that are no longer supported by vendors are removed. |
| Maturity Level Three requires that the latest release, or the previous release, of operating systems are used. |

#### Windows endpoints

In accordance with the <SYSTEM-NAME> Vulnerability and Patch Management Process, <ORGANISATION-NAME> will monitor Microsoft support for Windows, and ensure that all operating systems on workstations are removed prior to this support ending.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

#### Hybrid servers

In accordance with the <SYSTEM-NAME> Vulnerability and Patch Management Process, <ORGANISATION-NAME> will monitor Microsoft support for Windows, and ensure that all operating systems on servers are removed prior to this support ending.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Multi-factor Authentication

| EOT |
| --- |
| **Instruction** |
| The Essential Eight sections of a System Security Plan (SSP) should document the Essential Eight Maturity levels associated with implementation of a system. 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 the organisation 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 the Essential Eight Maturity levels associated with implementation of their system. When complete, remove any instructional boxes throughout. |

| EOT |
| --- |
| **Blueprint guidance** |
| For applicable government organisations to meet the minimum requirements established under the [*Protective Security Policy Framework* (PSPF)](https://www.protectivesecurity.gov.au/publications-library/protective-security-policy-framework-pspf-assessment-report-2023-24) maturity model, these organisations must implement Maturity Level Two for each of the below components of ASD’s [*Essential Eight Maturity Model*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight). |
| As with implementation of ISM controls, the Blueprint does not itself *achieve* any particular Essential Eight Maturity levels, but rather assists organisations in designing and building systems to achieve their desired maturity level based on their own operating context. |

## Applicability

The Multi-Factor Authentication (MFA) mitigation strategy is applicable to all access management within <SYSTEM-NAME>.

In particular, this is applicable to the configuration of Microsoft Entra ID AND ON PREMISES ACTIVE DIRECTORY to provide identity and access management (IAM) services for <SYSTEM-NAME>, particularly for governing access to Microsoft 365 services and to managed <SYSTEM-NAME> Windows endpoints.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Maturity level

|  |
| --- |
| |  |  | | --- | --- | | Targeted: | <TARGET-LEVEL> | | Currently Assessed: | <ASSESSED-LEVEL> | |
|  |

## Implementation

### Authentication methods used

| EOT |
| --- |
| **Essential Eight guidance** |
| The Essential Eight Maturity Model requires that all MFA used is either: |
| * something users have and something users know, or * something users have that is unlocked by something users know or are. |
| Applicability to online services is determined by the following table: |
| | System/Service | Who | That process, store or communicate | ML1 | ML2 | ML3 | | --- | --- | --- | --- | --- | --- | | Third-party Online Services: | Users | Sensitive orNon-sensitive Data: | Any | Phishing Resistant*Only* | Phishing Resistant*Only* | | Organisation’s Online Services: | Users | Sensitive Data: | Any | Phishing Resistant*Only* | Phishing Resistant*Only* | | Third-party Online Customer Services: | Users | Sensitive Customer Data: | Any | Phishing Resistant*Only* | Phishing Resistant*Only* | | Organisation’s Online Customer Services: | Users | Sensitive Customer Data: | Any | Phishing Resistant*Only* | Phishing Resistant*Only* | | Online Customer Services: | Customers | Sensitive Customer Data: | Any | Phishing Resistant*Option* | Phishing Resistant*Only* | |
| Applicability to other systems and services is determined by the following table: |
| | System/Service | Who | ML1 | ML2 | ML3 | | --- | --- | --- | --- | --- | | Systems: | Privileged Users: | - | Phishing Resistant*Only* | Phishing Resistant*Only* | |  | Unprivileged Users: | - | Phishing Resistant*Only* | Phishing Resistant*Only* | | Data Repositories: | Privileged Users: | - | - | Phishing Resistant*Only* | |  | Unprivileged Users: | - | - | Phishing Resistant*Only* | |

| EOT |
| --- |
| **Blueprint guidance** |
| The use of Microsoft services constitutes user access to online services per the above table, which at Maturity Level two and three requires phishing-resistant multifactor authentication to be used. For consideration of options for authentication factors, see Blueprint Design: Authentication, noting that use of the Microsoft Authenticator application meets a maximum of Maturity Level Three. |
| Similarly, authentication to Windows endpoints constitutes access to other systems, and should similarly require phishing resistant multifactor authentication as described above. |

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) services, including as for access to <SYSTEM-NAME> Windows endpoints.

Microsoft Entra ID is configured to utilise the following authentication methods:

|  |
| --- |
| | User group | Authentication method | Notes | | --- | --- | --- | | Unprivileged users: | <Authentication method-1> |  | |  | <Authentication method-2> |  | | Privileged users: | <Authentication method-1> |  | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Logging

| EOT |
| --- |
| **Essential Eight guidance** |
| Maturity Levels 2 and 3 require that |
| * all successful and unsuccessful MFA events to be captured from all systems and services and centrally logged * event logs are protected from unauthorised modification and deletion. |

The collection of event logs for monitoring of <SYSTEM-NAME> is performed in accordance with <ORGANISATION-NAME>’s Event Logging Policy, and includes the aggregation of the following logs into Microsoft Log Analytics:

|  |
| --- |
| | MFA Event (Microsoft 365 services) | Forwarded to Log Analytics | | --- | --- | | Successful MFA: | <YES> | | Unsuccessful MFA: | <YES> | |
|  |

|  |
| --- |
| | MFA Event (Workstations) | Forwarded to Log Analytics | | --- | --- | | Successful MFA: | <YES> | | Unsuccessful MFA: | <YES> | |
|  |

|  |
| --- |
| | MFA Event (<Internet-facing servers>) | Forwarded to Log Analytics | | --- | --- | | Successful MFA: | <YES> | | Unsuccessful MFA: | <YES> | |
|  |

|  |
| --- |
| | MFA Event (<Non-internet-facing servers>) | Forwarded to Log Analytics | | --- | --- | | Successful MFA: | <YES> | | Unsuccessful MFA: | <YES> | |
|  |

|  |
| --- |
| | MFA Event (<OTHER-SERVICE-1>) | Forwarded to Log Analytics | | --- | --- | | Successful MFA: | <YES> | | Unsuccessful MFA: | <YES> | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Monitoring and response

| EOT |
| --- |
| **Essential Eight guidance** |
| Maturity Levels 2 and 3 require all successful and unsuccessful MFA event logs from the following systems to be analysed in a timely manner to detect cyber security events: |
| | System | ML2 | ML3 | | --- | --- | --- | | Internet-facing servers: | Yes | Yes | | Non-internet-facing servers: | - | Yes | | Workstations: | - | Yes | |
| Both Maturity Levels 2 and 3 also require the following: |
| * cyber security events are analysed in a timely manner to identify cyber security incidents * as soon as possible after a cyber security incident occurs or is discovered the: * cyber security incident response plan is enacted. * incident is reported to the CISO, or one of their delegates * incident is reported to ASD. |

| EOT |
| --- |
| **Blueprint guidance** |
| The Blueprint provides limited guidance to support organisations in developing an approach for the response to cyber security incidents. However, 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.

This includes the processing, analysis, and response to the following event logs in a timely manner:

|  |
| --- |
| | MFA Event | Microsoft 365 Services | Workstations | <INTERNET-FACING-SERVERS> | <NON-INTERNET-FACING-SERVERS> | <OTHER SERVICES> | | --- | --- | --- | --- | --- | --- | | Successful MFA: | <YES> | <YES> | <IMPLEMENTATION> | <IMPLEMENTATION> | <IMPLEMENTATION> | | Unsuccessful MFA: | <YES> | <YES> | <IMPLEMENTATION> | <IMPLEMENTATION> | <IMPLEMENTATION> | |
|  |

<ORGANISATION-NAME> has established a Security Operations Centre (SOC) to analyse cyber security events in a timely manner, a Cyber Security Incident Register and Incident Response Plan to facilitate the response to detected cyber security events in a timely and appropriate manner. This plan includes reporting all incidents to the <ORGANISATION-NAME> CISO and to ASD in a timely manner.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Restrict Administrative Privileges

| EOT |
| --- |
| **Instruction** |
| The Essential Eight sections of a System Security Plan (SSP) should document the Essential Eight Maturity levels associated with implementation of a system. 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 the organisation 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 the Essential Eight Maturity levels associated with implementation of their system. When complete, remove any instructional boxes throughout. |

| EOT |
| --- |
| **Blueprint guidance** |
| For applicable government organisations to meet the minimum requirements established under the [*Protective Security Policy Framework* (PSPF)](https://www.protectivesecurity.gov.au/publications-library/policy-10-safeguarding-data-cyber-threats) maturity model, these organisations must implement Maturity Level Two for each of the below components of ASD’s [*Essential Eight Maturity Model*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight). |
| As with implementation of ISM controls, the Blueprint does not itself *achieve* any particular Essential Eight Maturity levels, but rather assists organisations in designing and building systems to achieve their desired maturity level based on their own operating context. |

## Applicability

The Restrict Administrative Privileges mitigation strategy is applicable to restricting and hardening all administrative access used for any components of <SYSTEM-NAME>.

## Maturity Level

|  |
| --- |
| |  |  | | --- | --- | | Targeted: | <TARGET-LEVEL> | | Currently Assessed: | <ASSESSED-LEVEL> | |
|  |

## Implementation

### Privileged access requests

| EOT |
| --- |
| **Essential Eight guidance** |
| | Privileged Access to: | What | ML1 | ML2 | ML3 | | --- | --- | --- | --- | --- | | Systems and Applications: | Validated when first requested: | Yes | Yes | Yes | |  | Disabled after 12 months unless revalidated: | - | Yes | Yes | |  | Disabled after 45 days of inactivity: | - | Yes | Yes | |  |  |  |  |  | | Data Repositories: | Validated when first requested: | Yes | Yes | Yes | |  | Disabled after 12 months unless revalidate: | - | Yes | Yes | |

| EOT |
| --- |
| **Blueprint guidance** |
| The Blueprint does not currently provide guidance for automating the disabling of accounts. Organisations building a system using the Blueprint should implement appropriate organisational processes for both validating initial privileged access requests, and disabling them where appropriate. |

<DETAIL PROCESSES FOR PRIVILEGED ACCESS REQUESTS AS APPROPRIATE>

### Operating environments

| EOT |
| --- |
| **Essential Eight guidance** |
| All maturity levels require that privileged users use separate privileged and unprivileged operating environments, with the following restrictions: |
| | For Unprivileged Operating Environments: | ML1 | ML2 | ML3 | | --- | --- | --- | --- | | Privileged accounts (excluding local administrator accounts) cannot logon to the environment. | Yes | Yes | Yes | |
| | For Privileged Operating Environments: | ML1 | ML2 | ML3 | | --- | --- | --- | --- | | Unprivileged accounts cannot logon to the environment: | Yes | Yes | Yes | | The environment is not virtualised within an unprivileged operating environment: | - | Yes | Yes | | Administrative activities are conducted through jump servers: | - | Yes | Yes | | Administrative activities are conducted on Secure Admin Workstations: | - | - | Yes | |

| EOT |
| --- |
| **Blueprint guidance** |
| The Blueprint does not currently provide guidance for implementing hardened operating environments administrative activities, including jump servers of Secure Administrative Workstations. The implementation below describes a typical Maturity Level Three implementation for a system built using the Blueprint, and should be adapted to whatever implementation is used for the final system. |

#### Unprivileged operating environment

<SYSTEM-NAME> standard workstations utilise Microsoft Entra ID as the source of identity and access management, and Conditional Access prevents privileged accounts from logging on.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

#### Privileged operating environment

<SYSTEM-NAME> utilises dedicated Secure Admin Workstations for privileged users.

These workstations utilise Microsoft Entra ID as the source of identity and access management, and Conditional Access prevents unprivileged accounts from logging on.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Privileged access

| EOT |
| --- |
| **Essential Eight guidance** |
| The following restrictions are required for privileged accounts: |
| | Privileged account type | Restriction | ML1 | ML2 | ML3 | | --- | --- | --- | --- | --- | | Privileged accounts explicitly authorised to access online services | Prevented from accessing the internet, email and web services | - | - | - | |  | Access is strictly limited to only what is required for users and services to undertake their duties | Yes | Yes | Yes | |  | Just-in-time administration is used |  |  | Yes | |  |  |  |  |  | | Other privileged accounts | Prevented from accessing the internet, email and web services | Yes | Yes | Yes | |  | Access is strictly limited to only what is required for users and services to undertake their duties | - | - | Yes | |  | Just-in-time administration is used | - | - | Yes | |

| EOT |
| --- |
| **Blueprint guidance** |
| The Blueprint does not currently provide guidance for restricting privileged account activities. The implementation below describes a typical Maturity Level Three implementation for a system built using the Blueprint, and should be adapted to whatever implementation is used for the final system. |

Privileged accounts for <SYSTEM-NAME> users are accounts are restricted from accessing the internet, email and web services, and are only able to access relevant Microsoft management portals.

Furthermore, these accounts have appropriate Role Based Access Control applied, with just-in-time administration required for each role to be granted to privileged users.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Management of credentials

| EOT |
| --- |
| **Essential Eight guidance** |
| Maturity Levels Two and Three require that credentials for the following account types are long, unique, unpredictable and managed: |
| * Break Glass Accounts * Local Administrator Accounts * Service Accounts |

<SYSTEM-NAME> provides a central identity store that governs and grants all user access prior to accessing resources on the system. 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>

### Protecting credentials

| EOT |
| --- |
| **Essential Eight guidance** |
| Maturity Level Three Requires the following functionality to be enabled for protecting accounts: |
| * Memory integrity * Local Security Authority protection * Credential Guard * Remote Credential Guard |

<SYSTEM-NAME> implements the following required protections for user accounts:

|  |
| --- |
| | Protection | Configured | | --- | --- | | Memory integrity | <YES> | | Local Security Authority protection | <YES> | | Credential Guard | <YES> | | Remote Credential Guard | <N/A> | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Logging

| EOT |
| --- |
| **Essential Eight guidance** |
| Maturity Levels Two and Three require that |
| * all Allowed and blocked application control events to be captured from all systems and services and centrally logged * event logs are protected from unauthorised modification and deletion. |

The collection of event logs for monitoring of <SYSTEM-NAME> is performed in accordance with <ORGANISATION-NAME>’s Event Logging Policy, and includes the aggregation of the following logs into Microsoft Log Analytics:

|  |
| --- |
| | Event (Entra ID) | Forwarded to Log Analytics | | --- | --- | | Privileged access: | <YES> | | Privileged account management: | <YES> | | Privileged group management: | <YES> | |
|  |

|  |
| --- |
| | System / Service | Event | Forwarded to Log Analytics | | --- | --- | --- | | Microsoft 365 services: | Privileged access event | <YES> | | Workstations: | Privileged access event | <YES> | | <Internet-facing servers>: | Privileged access event | <YES> | | <Non-Internet-facing servers>: | Privileged access event | <YES> | | <OTHER-SERVICE-1>: | Privileged access event | <YES> | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Monitoring and response

| EOT |
| --- |
| **Essential Eight guidance** |
| Maturity Levels Two and Three require all Privileged access, privileged account, and group management event logs from the following systems to be analysed in a timely manner to detect cyber security events: |
| | System | ML2 | ML3 | | --- | --- | --- | | Internet-facing servers: | Yes | Yes | | Non-internet-facing servers: | - | Yes | | Workstations: | - | Yes | |
| Both Maturity Levels Two and Three also require the following: |
| * cyber security events are analysed in a timely manner to identify cyber security incidents * as soon as possible after a cyber security incident occurs or is discovered the: * cyber security incident response plan is enacted * incident is reported to the Chief Information Security Officer, or one of their delegates * incident is reported to ASD. |

| 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.

This includes the processing, analysis, and response to the following event logs in a timely manner:

|  |
| --- |
| | Event | Workstations | <Hybrid servers> | | --- | --- | --- | | Privileged access: | Yes | <Detail implementation> | | Privileged account: | Yes | <Detail implementation> | | Group management: | Yes | <Detail implementation> | |
|  |

<ORGANISATION-NAME> has established a Security Operations Centre (SOC) to analyse cyber security events in a timely manner, and a Cyber Security Incident Register, and Incident Response Plan to facilitate the response to detected cyber security events in a timely and appropriate manner. This plan includes reporting all incidents to the <ORGANISATION-NAME> CISO and to ASD in a timely manner.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Application Control

| EOT |
| --- |
| **Instruction** |
| The Essential Eight sections of a System Security Plan (SSP) should document the Essential Eight Maturity levels associated with implementation of a system. 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 the organisation 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 the Essential Eight Maturity levels associated with implementation of their system. When complete, remove any instructional boxes throughout. |

| EOT |
| --- |
| **Blueprint guidance** |
| For applicable government organisations to meet the minimum requirements established under the [*Protective Security Policy Framework* (PSPF)](https://www.protectivesecurity.gov.au/publications-library/policy-10-safeguarding-data-cyber-threats) maturity model, these organisations must implement Maturity Level Two for each of the below components of ASD’s [*Essential Eight Maturity Model*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight). |
| As with implementation of ISM controls, the Blueprint does not itself *achieve* any particular Essential Eight Maturity levels, but rather assists organisations in designing and building systems to achieve their desired maturity level based on their own operating context. |

## Applicability

The application control mitigation strategy is applicable to the management of applications on the following <SYSTEM-NAME> components:

* Windows Endpoints
* <HYBRID SERVERS>

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Maturity level

|  |
| --- |
| |  |  | | --- | --- | | Targeted: | <TARGET-LEVEL> | | Currently Assessed: | <ASSESSED-LEVEL> | |
|  |

## Implementation

### Windows endpoints

| EOT |
| --- |
| **Essential Eight guidance** |
| Application control on workstations is required to apply to the following profiles and locations: |
| | Profiles and locations | ML1 | ML2 | ML3 | | --- | --- | --- | --- | | User profiles | Yes | Yes | Yes | | Temporary folders used by operating systems, web browsers and email clients | Yes | Yes | Yes | | All other locations | - | Yes | Yes | |
| Application control on workstations is required to restrict the following filetypes: |
| | Filetypes | ML1 | ML2 | ML3 | | --- | --- | --- | --- | | Executables | Yes | Yes | Yes | | Software libraries | Yes | Yes | Yes | | Scripts | Yes | Yes | Yes | | Installers | Yes | Yes | Yes | | Compiled HTML | Yes | Yes | Yes | | HTML applications | Yes | Yes | Yes | | Control panel applets | Yes | Yes | Yes | | Drivers | - | - | Yes | |
| In addition, the following Microsoft blocklists should be implemented: |
| | Blocklists | ML1 | ML2 | ML3 | | --- | --- | --- | --- | | Microsoft’s recommended application blocklist | - | Yes | Yes | | Microsoft’s vulnerable driver blocklist | - | - | Yes | |
| **Validation of rule-set** |
| Maturity Levels 2 and 3 additionally require that application control rule-sets on workstations are validated on an annual basis (if not more frequently). |

Windows Defender Application Control (WDAC) is used to apply application control on <SYSTEM-NAME> workstations and is configured via Microsoft Intune to:

* prevent users (other than local administrators) from installing or uninstalling applications
* utilise a combination of hash, publisher certificate and path rules in enforcing defined application control policies
* restrict the execution of the following filetypes to a <ORGANISATION-NAME> approved set:
* executables
* software libraries
* scripts
* installers
* compiled html
* HTML applications
* control panel applets
* drivers
* implement [Microsoft’s recommended application blocklist](https://docs.microsoft.com/windows/security/threat-protection/windows-defender-application-control/Microsoft-recommended-block-rules) and [Microsoft’s vulnerable driver blocklist](https://docs.microsoft.com/windows/security/threat-protection/windows-defender-application-control/Microsoft-recommended-driver-block-rules).

A current list of <SYSTEM-NAME> allowed applications can be found in the <SYSTEM-NAME> Intune portal. As per <SYSTEM-NAME>’s System Administration Process, <ORGANISATION-NAME> will continually review the list of allowed applications within these filetypes for relevant groups of users, including a specific annual review.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Internet-facing servers

| EOT |
| --- |
| **Essential Eight guidance** |
| Application control on internet-facing servers is required to apply to the following profiles and locations: |
| | Profiles and locations | ML1 | ML2 | ML3 | | --- | --- | --- | --- | | User profiles | - | Yes | Yes | | Temporary folders used by operating systems, web browsers and email clients | - | Yes | Yes | | All other locations | - | Yes | Yes | |
| Application control on internet-facing servers is required to restrict the following filetypes: |
| | Filetype | ML1 | ML2 | ML3 | | --- | --- | --- | --- | | Executables | - | Yes | Yes | | Software libraries | - | Yes | Yes | | Scripts | - | Yes | Yes | | Installers | - | Yes | Yes | | Compiled HTML | - | Yes | Yes | | HTML applications | - | Yes | Yes | | Control panel applets | - | Yes | Yes | | Drivers | - | - | Yes | |
| In addition, the following Microsoft blocklists should be implemented |
| | Blocklist | ML1 | ML2 | ML3 | | --- | --- | --- | --- | | Microsoft’s recommended application blocklist | - | Yes | Yes | | Microsoft’s vulnerable driver blocklist | - | - | Yes | |
| **Validation of rule-set** |
| Maturity Levels 2 and 3 additionally require that application control rule-sets on internet-facing servers are validated on an annual basis (if not more frequently). |

| EOT |
| --- |
| **Blueprint guidance** |
| This section typically applies where the system built using the Blueprint implements an on-premise Microsoft Exchange server. |
| The Blueprint does not provide guidance for implementing application control on servers, though it is generally implemented using Group Policy, and should be detailed below. |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Non-internet-facing servers

| EOT |
| --- |
| **Essential Eight guidance** |
| Application control on non-internet-facing servers is required to apply to the following profiles and locations: |
| | Profiles and locations | ML1 | ML2 | ML3 | | --- | --- | --- | --- | | User profiles: | - | - | Yes | | Temporary folders used by operating systems, web browsers and email clients: | - | - | Yes | | All other locations: | - | - | Yes | |
| Application control on non-internet-facing servers is required to restrict the following filetypes: |
| | Filetypes | ML1 | ML2 | ML3 | | --- | --- | --- | --- | | Executables: | - | - | Yes | | Software libraries: | - | - | Yes | | Scripts: | - | - | Yes | | Installers: | - | - | Yes | | Compiled HTML: | - | - | Yes | | HTML applications: | - | - | Yes | | Control panel applets: | - | - | Yes | | Drivers: | - | - | Yes | |
| In addition, the following Microsoft blocklists should be implemented: |
| | Blocklist | ML1 | ML2 | ML3 | | --- | --- | --- | --- | | Microsoft’s recommended application blocklist: | - | - | Yes | | Microsoft’s vulnerable driver blocklist: | - | - | Yes | |
| **Validation of rule-set** |
| Maturity Levels 2 and 3 additionally require that application control rule-sets on non-internet-facing servers are validated on an annual basis (if not more frequently). |

| EOT |
| --- |
| **Blueprint guidance** |
| This section typically applies where the system built using the Blueprint implements an on-premise server for Active Directory services. |
| The Blueprint does not provide guidance for implementing application control on servers, though it is generally implemented using Group Policy, and should be detailed below. |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Logging

| EOT |
| --- |
| **Essential Eight guidance** |
| Maturity Levels 2 and 3 require that: |
| * all allowed and blocked application control events are to be captured from all of the following and centrally logged: * workstations * internet-facing servers * non-internet-facing servers * event logs are protected from unauthorised modification and deletion. |

The collection of event logs for monitoring of <SYSTEM-NAME> is performed in accordance with <ORGANISATION-NAME>’s Event Logging Policy, and includes the aggregation of the following logs into Microsoft Log Analytics:

|  |
| --- |
| | Application Control Event (Workstations) | Forwarded to Log Analytics | | --- | --- | | Allowed application execution: | <YES> | | Blocked application execution: | <YES> | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

|  |
| --- |
| | Application Control Event (<Internet-facing servers>) | Forwarded to Log Analytics | | --- | --- | | Allowed application execution: | <YES> | | Blocked application execution: | <YES> | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

|  |
| --- |
| | Application Control Event (<Non-Internet-facing servers>) | Forwarded to Log Analytics | | --- | --- | | Allowed application execution: | <YES> | | Blocked application execution: | <YES> | |
|  |

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Monitoring and response

| EOT |
| --- |
| **Essential Eight guidance** |
| Maturity Levels 2 and 3 require all allowed and blocked application control event logs from the following systems to be analysed in a timely manner to detect cyber security events: |
| | System | ML2 | ML3 | | --- | --- | --- | | Internet-facing servers: | Yes | Yes | | Non-internet-facing servers: | - | Yes | | Workstations: | - | Yes | |
| Both Maturity Levels 2 and 3 also require the following: |
| * cyber security events are analysed in a timely manner to identify cyber security incidents * as soon as possible after a cyber security incident occurs or is discovered the: * cyber security incident response plan is enacted * incident is reported to the Chief Information Security Officer (CISO), or one of their delegates * incident is reported to ASD. |

| EOT |
| --- |
| **Blueprint guidance** |
| The Blueprint provides limited guidance on developing an approach for response to cyber security incidents. However, the section below is provided for organisations to describe the measures implemented within their system(s) built on the Blueprint. |
| 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.

This includes the processing, analysis, and response to the following event logs in a timely manner:

|  |
| --- |
| | Application Control Event | Workstations | <HYBRID SERVERS> | | --- | --- | --- | | Allowed application execution: | YES | <IMPLEMENTATION> | | Blocked application execution: | YES | <IMPLEMENTATION> | |
|  |

<ORGANISATION-NAME> has established a Security Operations Centre (SOC) to analyse cyber security events in a timely manner, a Cyber Security Incident Register and Incident Response Plan to facilitate the response to detected cyber security events in a timely and appropriate manner. This plan includes reporting all incidents to <ORGANISATION-NAME>’s Chief Information Security Officer (CISO) and to ASD in a timely manner.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Restrict Microsoft Office Macros

| EOT |
| --- |
| **Instruction** |
| The Essential Eight sections of a System Security Plan (SSP) should document the Essential Eight Maturity levels associated with implementation of a system. 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 the organisation 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 the Essential Eight Maturity levels associated with implementation of their system. When complete, remove any instructional boxes throughout. |

| EOT |
| --- |
| **Blueprint guidance** |
| For applicable government organisations to meet the minimum requirements established under the [*Protective Security Policy Framework* (PSPF)](https://www.protectivesecurity.gov.au/publications-library/policy-10-safeguarding-data-cyber-threats) maturity model, these organisations must implement Maturity Level Two for each of the below components of ASD’s [*Essential Eight Maturity Model*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight). |
| As with implementation of ISM controls, the Blueprint does not itself *achieve* any particular Essential Eight Maturity levels, but rather assists organisations in designing and building systems to achieve their desired maturity level based on their own operating context. |

## Applicability

The Restrict Microsoft Office Macros mitigation strategy is applicable to restricting the execution of Microsoft Office Macros on all <SYSTEM-NAME> workstations and servers.

## Maturity Level

|  |
| --- |
| |  |  | | --- | --- | | Targeted: | <TARGET-LEVEL> | | Currently Assessed: | <ASSESSED-LEVEL> | |
|  |

## Implementation

| EOT |
| --- |
| **Essential Eight guidance** |
| All Maturity levels require that for all systems and users: |
| * all Microsoft Office macros are disabled, unless the user has a demonstrated business requirement * Microsoft Office macros in files originating from the internet are blocked * Microsoft Office macro antivirus scanning is enabled * Microsoft Office macro security settings cannot be changed by users. |
| Maturity Levels Two and Three also require that for user accounts that have a demonstrated business requirement to run Microsoft Office macros: |
| * these macros are blocked from making Win32 API calls. |
| Maturity Level Three also requires that for user accounts that have a demonstrated business requirement to run Microsoft Office macros: |
| * Microsoft Office macros are only allowed to execute where they are running in one of the following conditions: * running from within a sandboxed environment, * running from a Trusted Location, or * are digitally signed by a trusted publisher. * that before being digitally signed or placed within Trusted Locations: * Microsoft Office macros are checked to ensure they are free of malicious code * Microsoft Office macros cannot be enabled via the Message Bar or Backstage View where they have been digitally signed by either: * an untrusted publisher * signatures other than V3 signatures. |

### Windows endpoints

<SYSTEM-NAME> restricts macro execution to only those signed by a trusted digital certificate in accordance with ASD’s [*Microsoft Office Macro Security*](https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/restricting-microsoft-office-macros) guidance. This includes blocking Microsoft Office macros originating from the internet and preventing standard users from modifying macro security settings in all Microsoft Office applications.

Microsoft Defender Antivirus and Defender for Endpoint provide antivirus scanning of all Microsoft Office file types, including embedded macros. This leverages the [Antimalware Scan Interface](https://www.microsoft.com/security/blog/2018/09/12/office-vba-amsi-parting-the-veil-on-malicious-macros/) (AMSI) to enable inspecting macros at runtime.

Microsoft Office macros are blocked from making Win32 API calls using Attack Surface Reduction (ASR) rules as per ASD’s [*Hardening Microsoft Windows 10 version 21H1 Workstations*](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) and [*Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016*](https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/hardening-microsoft-365-office-2021-office-2019-and-office-2016) hardening guides.

<SYSTEM-NAME> uses Defender for Endpoint to centrally store Endpoint Detection & Response (EDR) logs for all Windows endpoints, which includes the execution of macro-enabled documents and resulting behaviours (such as attempts to make Win32 API calls).

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

### Hybrid 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 for a system, where this management is included within the authorisation boundary for a system built using the Blueprint. |
| Generally, much of the applicable software (such as Microsoft Office) is not installed on servers, and so together with the proper implementation of application control and system monitoring, is likely to be limited in scope. However, implementation of this hardening is also often completed as part of a separate system specific to these servers. |
| Where the organisation appropriately assesses this within another document, it may choose to remove its implementation and assessment from this particular SSP Annex, though it is advised that organisations consider tracking this here for a holistic capture of the system context and associated risk. |

Office productivity suites are not installed on <SYSTEM-NAME> servers.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# User Application Hardening

| EOT |
| --- |
| **Instruction** |
| The Essential Eight sections of a System Security Plan (SSP) should document the Essential Eight Maturity levels associated with implementation of a system. 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 the organisation 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 the Essential Eight Maturity levels associated with implementation of their system. When complete, remove any instructional boxes throughout. |

| EOT |
| --- |
| **Blueprint guidance** |
| For applicable government organisations to meet the minimum requirements established under the [*Protective Security Policy Framework* (PSPF)](https://www.protectivesecurity.gov.au/publications-library/policy-10-safeguarding-data-cyber-threats) maturity model, these organisations must implement Maturity Level Two for each of the below components of ASD’s [*Essential Eight Maturity Model*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight). |
| As with implementation of ISM controls, the Blueprint does not itself *achieve* any particular Essential Eight Maturity levels, but rather assists organisations in designing and building systems to achieve their desired maturity level based on their own operating context. |

## Applicability

The User Application Hardening mitigation strategy is applicable to hardening of user applications on all <SYSTEM-NAME> workstations and servers.

## Maturity Level

|  |
| --- |
| |  |  | | --- | --- | | Targeted: | <TARGET-LEVEL> | | Currently Assessed: | <ASSESSED-LEVEL> | |
|  |

## Implementation

### User application hardening

| EOT |
| --- |
| **Essential Eight guidance** |
| All maturity levels require: |
| * Internet Explorer 11 is disabled or removed * web browsers: * security settings cannot be changed by users * do not process Java from the internet * do not process web advertisements from the internet. |
| In addition, Maturity Levels Two and Three require: |
| * web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur * office productivity suites: * security settings cannot be changed by users * are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur * Microsoft Office: * is blocked from creating child processes * is blocked from creating executable content * is blocked from injecting code into other processes * is configured to prevent activation of Object Linking and Embedding packages * PDF software * security settings cannot be changed by users * is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur * is blocked from creating child processes. |
| In addition, Maturity Level Three requires: |
| * .NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed, * Windows PowerShell 2.0 is disabled or removed, and * PowerShell is configured to use Constrained Language Mode. |

#### Workstations

**Internet Explorer 11**

Internet Explorer is not installed on <SYSTEM-NAME> workstations.

**Web browsers**

The following web browsers are allowed to operate on <SYSTEM-NAME> workstations:

|  |
| --- |
| | Microsoft Edge | Restriction Applied | | --- | --- | | Security settings cannot be changed by users: | YES - RESTRICTED VIA WDAC | | Does not process Java from the internet: | YES - RESTRICTED VIA WDAC | | Does not process web advertisements from the internet: | Yes - RESTRICTED VIA WDAC USING BUILT IN EDGE FUNCTIONALITY, AND BLOCKED VIA <ORGANISATION-NAME> <GATEWAY-SYSTEM> | |
|  |

|  |
| --- |
| | e.g. GOOGLE CHROME | Restriction Applied | | --- | --- | | Security settings cannot be changed by users: | <IMPLEMENTATION> | | Does not process Java from the internet: | <IMPLEMENTATION> | | Does not process web advertisements from the internet: | <IMPLEMENTATION> | |
|  |

**Office productivity suites**

<SYSTEM-NAME> uses Microsoft Office as its sole office productivity suite, with the following hardening applied:

|  |
| --- |
| | Microsoft Office | Restriction Applied | | --- | --- | | Security settings cannot be changed by users: | YES - RESTRICTED VIA WDAC | | Hardened using the following guides: | <GUIDES USED> | | Blocked from creating child processes: | YES - RESTRICTED VIA WDAC | | Blocked from creating executable content: | YES - RESTRICTED VIA WDAC | | Blocked from injecting code into other processes: | YES - RESTRICTED VIA WDAC | | Configured to prevent activation of Object Linking and Embedding packages: | YES - RESTRICTED VIA WDAC | |
|  |

**PDF software**

The following PDF software is allowed to operate on <SYSTEM-NAME> workstations:

|  |
| --- |
| | e.g. ADOBE ACROBAT | Restriction Applied | | --- | --- | | Security settings cannot be changed by users: | YES - RESTRICTED VIA WDAC | | Hardened using the following guides: | <GUIDES USED> | | Blocked from creating child processes: | YES - RESTRICTED VIA WDAC | |
|  |

**Other software**

|  |
| --- |
| | Software | Restriction Applied | | --- | --- | | .NET Framework 3.5 (includes .NET 2.0 and 3.0:) | <ENABLED>/<DISABLED>/<REMOVED> | | Windows PowerShell 2.0: | <ENABLED>/<DISABLED>/<REMOVED> | | PowerShell: | <CONFIGURED TO USE CONFINED LANGUAGE MODE | |
|  |

#### Servers

**Internet Explorer 11**

Internet Explorer is not installed on <SYSTEM-NAME> servers.

**Web browsers**

The following web browsers are allowed to operate on <SYSTEM-NAME> servers:

|  |
| --- |
| | Microsoft Edge | Restriction Applied | | --- | --- | | Security settings cannot be changed by users: | YES - RESTRICTED VIA WDAC | | Does not process Java from the internet: | YES - RESTRICTED VIA WDAC | | Does not process web advertisements from the internet: | Yes - RESTRICTED VIA WDAC USING BUILT IN EDGE FUNCTIONALITY, AND BLOCKED VIA <ORGANISATION-NAME> <GATEWAY-SYSTEM> | |
|  |

|  |
| --- |
| | e.g. GOOGLE CHROME | Restriction Applied | | --- | --- | | Security settings cannot be changed by users: | <IMPLEMENTATION> | | Does not process Java from the internet: | <IMPLEMENTATION> | | Does not process web advertisements from the internet: | <IMPLEMENTATION> | |
|  |

**Office productivity suites**

Office productivity suites are not installed on <SYSTEM-NAME> servers.

**PDF software**

PDF software is not installed on <SYSTEM-NAME> servers.

**Other software**

|  |
| --- |
| | Software | Restriction Applied | | --- | --- | | .NET Framework 3.5 (includes .NET 2.0 and 3.0:) | <ENABLED>/<DISABLED>/<REMOVED> | | Windows PowerShell 2.0: | <ENABLED>/<DISABLED>/<REMOVED> | | PowerShell: | <CONFIGURED TO USE CONFINED LANGUAGE MODE | |
|  |

### Logging

| EOT |
| --- |
| **Essential Eight guidance** |
| Maturity Levels Two and Three require that |
| * all command line process creation, PowerShell module logging, script block logging and transcription events to be captured from all of the following: * workstations * internet-facing servers * non-internet-facing servers * event logs are protected from unauthorised modification and deletion. |

The collection of event logs for monitoring of <SYSTEM-NAME> is performed in accordance with <ORGANISATION-NAME>’s Event Logging Policy, and includes the aggregation of the following logs into Microsoft Log Analytics:

|  |
| --- |
| | Application Event (Workstations) | Forwarded to Log Analytics | | --- | --- | | Command line process creation: | <YES> | | PowerShell module logging: | <YES> | | Script block logging: | <YES> | | Transcription: | <YES> | |
|  |

|  |
| --- |
| | Application Event (<Internet-Facing Servers>) | Forwarded to Log Analytics | | --- | --- | | Command line process creation: | <YES> | | PowerShell module logging: | <YES> | | Script block logging: | <YES> | | Transcription: | <YES> | |
|  |

|  |
| --- |
| | Application Event (<Non-Internet-Facing Servers>) | Forwarded to Log Analytics | | --- | --- | | Command line process creation: | <YES> | | PowerShell module logging: | <YES> | | Script block logging: | <YES> | | Transcription: | <YES> | |
|  |

### Monitoring and response

| EOT |
| --- |
| **Essential Eight guidance** |
| Maturity Levels Two and Three require all command line process creation, PowerShell module logging, script block logging and transcription event logs from the following systems to be analysed in a timely manner: |
| | System | ML2 | ML3 | | --- | --- | --- | | Internet-facing servers: | Yes | Yes | | Non-internet-facing servers: | - | Yes | | Workstations: | - | Yes | |
| Both Maturity Levels Two and Three also require the following: |
| * cyber security events are analysed in a timely manner to identify cyber security incidents * as soon as possible after a cyber security incident occurs or is discovered the: * cyber security incident response plan is enacted * incident is reported to the Chief Information Security Officer, or one of their delegates * incident is reported to ASD. |

| 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.

This includes the processing, analysis, and response to the following event logs in a timely manner:

|  |
| --- |
| | Event | Workstations | <HYBRID SERVERS> | | --- | --- | --- | | Command line process creation: | <YES> | <YES> | | PowerShell module logging: | <YES> | <YES> | | Script block logging: | <YES> | <YES> | | Transcription: | <YES> | <YES> | |
|  |

<ORGANISATION-NAME> has established a Security Operations Centre (SOC) to analyse cyber security events in a timely manner, and a Cyber Security Incident Register, and Incident Response Plan to facilitate the response to detected cyber security events in a timely and appropriate manner. This plan includes reporting all incidents to the <ORGANISATION-NAME> CISO and to ASD in a timely manner.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

# Regular Backups

| EOT |
| --- |
| **Instruction** |
| The Essential Eight sections of a System Security Plan (SSP) should document the Essential Eight Maturity levels associated with implementation of a system. 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 the organisation 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 the Essential Eight Maturity levels associated with implementation of their system. When complete, remove any instructional boxes throughout. |

| EOT |
| --- |
| **Blueprint guidance** |
| For applicable government organisations to meet the minimum requirements established under the [*Protective Security Policy Framework* (PSPF)](https://www.protectivesecurity.gov.au/publications-library/policy-10-safeguarding-data-cyber-threats) maturity model, these organisations must implement Maturity Level Two for each of the below components of ASD’s [*Essential Eight Maturity Model*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight). |
| As with implementation of ISM controls, the Blueprint does not itself *achieve* any particular Essential Eight Maturity levels, but rather assists organisations in designing and building systems to achieve their desired maturity level based on their own operating context. |

## Applicability

The Regular Backups mitigation strategy is applicable to mitigating the risk of losing system availability or important <SYSTEM-NAME> data as part of a ransomware attack, or other form of destructive attack, and ensuring that in the event of such an attack, <SYSTEM-NAME> services and data can be quickly restored.

<INSERT ADDITIONAL INFORMATION AS APPROPRIATE>

## Maturity Level

|  |
| --- |
| |  |  | | --- | --- | | Targeted: | <TARGET-LEVEL> | | Currently Assessed: | <ASSESSED-LEVEL> | |
|  |

## Implementation

### Performing backups

| EOT |
| --- |
| **Essential Eight guidance** |
| All maturity levels require that backups of data, applications and settings are: |
| * performed and retained in accordance with business criticality and business continuity requirements * synchronised to enable restoration to a common point in time * retained in a secure and resilient manner. |

| EOT |
| --- |
| **Blueprint guidance** |
| While the Blueprint does not provide specific guidance on performing data backups, the section below is provided for organisations to describe their specific implementation, including where this is included within the authorisation boundary of system(s) built using the Blueprint. |

<DESCRIBE APPROACH TO PERFORMING BACKUPS AS APPROPRIATE>

### Restoring from backups

| EOT |
| --- |
| **Essential Eight guidance** |
| All maturity levels require that the organisation performs disaster recovery exercises that include testing the restoration of data, applications and settings from backups to a common point in time. |

| EOT |
| --- |
| **Blueprint guidance** |
| While the Blueprint does not provide specific guidance on performing disaster recovery exercises or otherwise restoring from data backups performed, the section below is provided for organisations to describe their approach to implementing and testing restoration procedures. |

<DESCRIBE APPROACH TO RESTORING FROM BACKUPS AS APPROPRIATE>

### Hardening backups

| EOT |
| --- |
| **Essential Eight guidance** |
| Required hardening for backups is determined by the following table: |
| | Account Type | Restriction Applied | ML1 | ML2 | ML3 | | --- | --- | --- | --- | --- | | Unprivileged Accounts: | Cannot access backups belonging to other accounts: | Yes | Yes | Yes | |  | Prevented from modifying and deleting backups: | Yes | Yes | Yes | |  | Cannot access their own backups: | - | - | Yes | |  |  |  |  |  | | Privileged accounts (excluding backup administrator accounts): | Cannot access backups belonging to other accounts: | - | Yes | Yes | |  | Prevented from modifying and deleting backups: | - | Yes | Yes | |  | Cannot access their own backups: | - | - | Yes | |  |  |  |  |  | | Backup administrator accounts: | Prevented from modifying and deleting backups during their retention period: | - | - | Yes | |

| EOT |
| --- |
| **Blueprint guidance** |
| While the Blueprint does not provide specific guidance on hardening data backups, the section below is provided for organisations to describe their specific implementation, including where this is included within the authorisation boundary of system(s) built using the Blueprint. |

<DESCRIBE APPROACH TO HARDENING BACKUPS AS APPROPRIATE>