# Essential 8 - Maturity Level 3

## Policies and Procedures




Prepared for: Client Company

Prepared by: YourIT Company

YourIT!
Your Logo Goes Here

# Table of Contents

# Purpose

To ensure that the business being measured can confirm to the requirements in the Essential 8 Maturity Model for compliance to insurance and general Cyber Security best practices as outlined by the Australian Cyber Security Centre. These best practices will minimize Cyber Security risk.

# Scope

The Essential 8 Maturity Model applies across all IT systems in use by your organisation to assess their compliance to the Maturity Level 3

# Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy.  Legal actions also may be taken for violations of applicable regulations and laws.

# Essential 8 AC-1 - Application Control (3)

| Essential 8 - Maturity Level 3 | Other Requirements |
| --- | --- |
| AC-1<br><br>Application Control (3) | N/A |

**Policy**

**Guidance**
Any type of executable including, applications, scripts, installers, control panel applets, compiled HTML and HTML applications must be strictly controlled on workstations and servers. There needs to be a clearly defined set of these to show which are allowed and all others should be blocked. This could be achieved through Microsoft security controls on Windows or through 3rd part endpoint security systems that contain this kind of approve/deny approach to execution.

**Responsibilities**
The Security Officer is responsible for ensuring the implementation of this policy.

**Related Internal Controls**
- E8-M3-AC-1 - Application Control (3): Application control is implemented on workstations and servers to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set

**References**
- ASCS Essential 8 Maturity Model - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

# Essential 8 AC-2 - Application Control (5)

| Essential 8 - Maturity Level 3 | Other Requirements |
| --- | --- |
| AC-2<br><br>Application Control (5) | N/A |

**Policy**
Microsoft's 'recommended block rules' are implemented.

**Guidance**
Follow Microsoft's Guidelines for application block rules using the Windows Defender Application Control feature.

**Responsibilities**
The Security Officer is responsible for ensuring the implementation of this policy.

**Related Internal Controls**
- E8-M3-AC-2 - Application Control (5): Microsoft's 'recommended block rules' are implemented.

**References**
- ASCS Essential 8 Maturity Model - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
- Microsoft Guidelines for application blocking - https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules

# Essential 8 AC-3 - Application Control (6)

| Essential 8 - Maturity Level 3 | Other Requirements |
| --- | --- |
| AC-3<br><br>Application Control (6) | N/A |

**Policy**
Microsoft's 'recommended driver block rules' are implemented.

**Guidance**
Follow Microsoft's Guidelines for driver block rules using the Windows Defender Application Control feature.

**Responsibilities**
The Security Officer is responsible for ensuring the implementation of this policy.

**Related Internal Controls**
- E8-M3-AC-3 - Application Control (6): Microsoft's 'recommended driver block rules' are implemented.

**References**
- ASCS Essential 8 Maturity Model - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
- Microsoft Guidelines for driver blocking - https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-driver-block-rules

# Essential 8 AC-4 - Application Control (7)

| Essential 8 - Maturity Level 3 | Other Requirements |
| --- | --- |
| AC-4<br><br>Application Control (7) | N/A |

**Policy**
Application control rulesets are validated on an annual or more frequent basis.

**Guidance**
Show that there is a documented policy and a process which reviews and validates on at least an annual basis all application control rulesets.

**Responsibilities**
The Security Officer is responsible for ensuring the implementation of this policy.

**Related Internal Controls**
- E8-M3-AC-4 - Application Control (7): Application control rulesets are validated on an annual or more frequent basis.

**References**
- ASCS Essential 8 Maturity Model - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

# Essential 8 AC-5 - Application Control (8)

| Essential 8 - Maturity Level 3 | Other Requirements |
| --- | --- |
| AC-5<br><br>Application Control (8) | N/A |

**Policy**

**Guidance**
There should be a log which shows all allowed and blocked executions of applications for internet facing servers and workstations. These logs should be replicated and stored centrally in a system such as a SIEM or dedicated logging system where they can be monitored and protected. These logs are an important source of security information and should be available as a part of investigations for a cyber security event. The logs themselves should trigger an incident if any signs of compromise are detected.

**Responsibilities**
The Security Officer is responsible for ensuring the implementation of this policy.

**Related Internal Controls**
- E8-M3-AC-5 - Application Control (8): Allowed and blocked executions on workstations and servers are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

**References**
- ASCS Essential 8 Maturity Model - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model

# Essential 8 CO-1 - Configure Office Macro Settings (3)

| Essential 8 - Maturity Level 3 | Other Requirements |
| --- | --- |
| CO-1<br><br>Configure Office Macro Settings (3) | N/A |

**Policy**
Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.

**Guidance**
To meet this requirement it is necessary to have a list of users that do have a demonstrated business requirement, it is best practice to list that business requirement and review it regularly as a part of security policy. Macro's must be disabled via reliable method such as the built in Microsoft security controls.

**Responsibilities**
The Security Officer is responsible for ensuring the implementation of this policy.

**Related Internal Controls**
- E8-M3-CO-1 - Configure Office Macro Settings (3): Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.

**References**
- ASCS Essential 8 Maturity Model - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
- ACSC Guide for Office Macros - https://www.cyber.gov.au/acsc/view-all-content/publications/microsoft-office-macro-security

# Essential 8 CO-10 - Configure Office Macro Settings (4)

| Essential 8 - Maturity Level 3 | Other Requirements |
| --- | --- |
| CO-10<br><br>Configure Office Macro Settings (4) | N/A |

**Policy**
Allowed and blocked Microsoft Office macro executions are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

**Guidance**
There should be a log which shows all allowed and blocked executions of Microsoft Office macros. These logs should be replicated and stored centrally in a system such as a SIEM or similar secure dedicated logging system where they can be monitored and protected. These logs are an important source of security information and should be available as a part of investigations for a cyber security event. The logs themselves should trigger an incident if any signs of compromise are detected.

**Responsibilities**
The Security Officer is responsible for ensuring the implementation of this policy.

**Related Internal Controls**
- E8-M3-CO-10 - Configure Office Macro Settings (4): Allowed and blocked Microsoft Office macro executions are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

**References**
- ASCS Essential 8 Maturity Model - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
- ACSC Guide for Office Macros - https://www.cyber.gov.au/acsc/view-all-content/publications/microsoft-office-macro-security

# Essential 8 CO-2 - Configure Office Macro Settings (7)

| Essential 8 - Maturity Level 3 | Other Requirements |
| --- | --- |
| CO-2<br><br>Configure Office Macro Settings (7) | N/A |

**Policy**
Microsoft Office macros in files originating from the internet are blocked.

**Guidance**
Microsoft Group Policy and/or Microsoft Attack Surface Reduction (ASR) can be leveraged to ensure Macros originating from the internet are blocked.

**Responsibilities**
The Security Officer is responsible for ensuring the implementation of this policy.

**Related Internal Controls**
- E8-M3-CO-2 - Configure Office Macro Settings (7): Microsoft Office macros in files originating from the internet are blocked.

**References**
- ASCS Essential 8 Maturity Model - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
- ACSC Guide for Office Macros - https://www.cyber.gov.au/acsc/view-all-content/publications/microsoft-office-macro-security

# Essential 8 CO-3 - Configure Office Macro Settings (10)

| Essential 8 - Maturity Level 3 | Other Requirements |
| --- | --- |
| CO-3<br><br>Configure Office Macro Settings (10) | N/A |

**Policy**
Microsoft Office macros in files originating from the internet are blocked.

**Guidance**
You must show that you have a process to block Office files originating from the internet that contain Macros. This could be via local controls such as Microsoft OS Group P{policy or Intune which disables all office Macros, or by using security controls at access points such as Firewall or Browser content blocking as well as Email filtering such as Microsoft Officer Defender or a 3rd Party equivalent.

**Responsibilities**
The Security Officer is responsible for ensuring the implementation of this policy.

**Related Internal Controls**
- E8-M3-CO-3 - Configure Office Macro Settings (10): Microsoft Office macros in files originating from the internet are blocked.

**References**
- ASCS Essential 8 Maturity Model - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
- ACSC Guide for Office Macros - https://www.cyber.gov.au/acsc/view-all-content/publications/microsoft-office-macro-security

# Essential 8 CO-4 - Configure Office Macro Settings (13)

| Essential 8 - Maturity Level 3 | Other Requirements |
| --- | --- |
| CO-4<br><br>Configure Office Macro Settings (13) | N/A |

**Policy**
Microsoft Office macro security settings cannot be changed by users.

**Guidance**
By default settings in Microsoft Office allows users to change the Macro security settings. These should be changed to ensure that no user can change the macro settings.

**Responsibilities**
The Security Officer is responsible for ensuring the implementation of this policy.

**Related Internal Controls**
- E8-M3-CO-4 - Configure Office Macro Settings (13): Microsoft Office macro security settings cannot be changed by users.

**References**
- ASCS Essential 8 Maturity Model - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
- ACSC Guide for Office Macros - https://www.cyber.gov.au/acsc/view-all-content/publications/microsoft-office-macro-security

# Essential 8 CO-5 - Configure Office Macro Settings (15)

| Essential 8 - Maturity Level 3 | Other Requirements |
| --- | --- |
| CO-5<br><br>Configure Office Macro Settings (15) | N/A |

**Policy**
Microsoft Office macros are blocked from making Win32 API calls.

**Guidance**
Microsoft Office macros are blocked from making Win32 API calls using Attack Surface Reduction (ASR) rules as per the ACSC Windows 10 and Microsoft Office hardening guides.

**Responsibilities**
The Security Officer is responsible for ensuring the implementation of this policy.

**Related Internal Controls**
- E8-M3-CO-5 - Configure Office Macro Settings (15): Microsoft Office macros are blocked from making Win32 API calls.

**References**
- ASCS Essential 8 Maturity Model - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
- ACSC Guide for Office Macros - https://www.cyber.gov.au/acsc/view-all-content/publications/microsoft-office-macro-security

# Essential 8 CO-6 - Configure Office Macro Settings (17)

| Essential 8 - Maturity Level 3 | Other Requirements |
| --- | --- |
| CO-6<br><br>Configure Office Macro Settings (17) | N/A |

**Policy**
Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute.

**Guidance**
Where there is a need to run Macro's in the environment a process must be implemented which ensures the security of macros or blocks them from causing harm in the environment. For any macro that needs to run in your environment it must be done via one of the 3 methods outlined: 1. From a Sandbox environment 2. Trusted Location (i.e. preloaded to a known secure on prem location accessible from browser which controls only running Macros from a "Trusted Location") 3. Macros Digitally signed by trusted publisher. All 3 may also be implemented to ensure heightened security.

**Responsibilities**
The Security Officer is responsible for ensuring the implementation of this policy.

**Related Internal Controls**
- E8-M3-CO-6 - Configure Office Macro Settings (17): Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute.

**References**
- ASCS Essential 8 Maturity Model - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
- ACSC Guide for Office Macros - https://www.cyber.gov.au/acsc/view-all-content/publications/microsoft-office-macro-security

# Essential 8 CO-7 - Configure Office Macro Settings (18)

| Essential 8 - Maturity Level 3 | Other Requirements |
| --- | --- |
| CO-7<br><br>Configure Office Macro Settings (18) | N/A |

**Policy**
Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.

**Guidance**
There should be a defined set of users who have the necessary education and experience to correctly validate the security of Macro's that controls the dissemination of these via controlled channels to a Trusted Location within the secure environment that can then be accessed by users with Office or Browsers setup with those Trusted Locations.

**Responsibilities**
The Security Officer is responsible for ensuring the implementation of this policy.

**Related Internal Controls**
- E8-M3-CO-7 - Configure Office Macro Settings (18): Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.

**References**
- ASCS Essential 8 Maturity Model - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
- ACSC Guide for Office Macros - https://www.cyber.gov.au/acsc/view-all-content/publications/microsoft-office-macro-security

**Truncated Sample Report**