Essential 8 - Maturity Level 2

Policies and Procedures

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Prepared for: Client Company

Prepared by: YourIT Company

05/30/2022

YourIT!
Your Logo Goes Here

Table of Contents

PROPRIETARY & CONFIDENTIAL

PROPRIETARY & CONFIDENTIAL

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.

PROPRIETARY & CONFIDENTIAL

Scope

The Essential 8 Maturity Model applies across all IT systems in use by your organisation to assess their compliance to the Maturity Level 2

PROPRIETARY & CONFIDENTIAL

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.

PROPRIETARY & CONFIDENTIAL

Essential 8 AC-1 - Application Control (2)

Essential 8 - Maturity Level 2	Other Requirements
AC-1 Application Control (2)	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-M2-AC-1 - Application Control (2): Application control is implemented on workstations and internet-facing 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

PROPRIETARY & CONFIDENTIAL

Essential 8 AC-2 - Application Control (4)

Essential 8 - Maturity Level 2	Other Requirements
AC-2 Application Control (4)	N/A

Policy
Allowed and blocked executions on workstations and internet-facing servers are logged.

Guidance
There should be a log which shows all allowed and blocked executions of applications for internet facing servers and workstations.

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

Related Internal Controls
- E8-M2-AC-2 - Application Control (4): Allowed and blocked executions on workstations and internet-facing servers are logged.

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

PROPRIETARY & CONFIDENTIAL

Essential 8 CO-1 - Configure Office Macro Settings (2)

Essential 8 - Maturity Level 2	Other Requirements
CO-1 Configure Office Macro Settings (2)	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-M2-CO-1 - Configure Office Macro Settings (2): 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

PROPRIETARY & CONFIDENTIAL

Essential 8 CO-2 - Configure Office Macro Settings (6)

Essential 8 - Maturity Level 2	Other Requirements
CO-2 Configure Office Macro Settings (6)	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-M2-CO-2 - Configure Office Macro Settings (6): 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

PROPRIETARY & CONFIDENTIAL

Essential 8 CO-3 - Configure Office Macro Settings (9)

Essential 8 - Maturity Level 2	Other Requirements
CO-3 Configure Office Macro Settings (9)	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-M2-CO-3 - Configure Office Macro Settings (9): 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

PROPRIETARY & CONFIDENTIAL

Essential 8 CO-4 - Configure Office Macro Settings (12)

Essential 8 - Maturity Level 2	Other Requirements
CO-4 Configure Office Macro Settings (12)	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-M2-CO-4 - Configure Office Macro Settings (12): 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

PROPRIETARY & CONFIDENTIAL

Essential 8 CO-5 - Configure Office Macro Settings (14)

Essential 8 - Maturity Level 2	Other Requirements
CO-5 Configure Office Macro Settings (14)	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-M2-CO-5 - Configure Office Macro Settings (14): 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

PROPRIETARY & CONFIDENTIAL

Essential 8 CO-6 - Configure Office Macro Settings (16)

Essential 8 - Maturity Level 2	Other Requirements
CO-6 Configure Office Macro Settings (16)	N/A

Policy
Allowed and blocked Microsoft Office macro executions are logged.

Guidance
There should be a log which shows all allowed and blocked executions of Microsoft Office macros.

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

Related Internal Controls
- E8-M2-CO-6 - Configure Office Macro Settings (16): Allowed and blocked Microsoft Office macro executions are logged.

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

PROPRIETARY & CONFIDENTIAL

Essential 8 MA-1 - Multi-factor Authentication (2)

Essential 8 - Maturity Level 2	Other Requirements
MA-1 Multi-factor Authentication (2)	N/A

Policy
Multi-factor authentication is used by an organisation's users if they authenticate to their organisation’s internet-facing services.

Guidance
This applies specifically to the organisations own internet facing services and that they should support MFA and that all users should be using it.

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

Related Internal Controls
- E8-M2-MA-1 - Multi-factor Authentication (2): Multi-factor authentication is used by an organisation's users if they authenticate to their organisation’s internet-facing services.

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

PROPRIETARY & CONFIDENTIAL

Essential 8 MA-2 - Multi-factor Authentication (5)

Essential 8 - Maturity Level 2	Other Requirements
MA-2 Multi-factor Authentication (5)	N/A

Policy
Multi-factor authentication is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.

Guidance
For any internet facing services from 3rd parties such as Microsoft Office, Mailchimp, HubSpot, Salesforce etc. that process, store or can communicate sensitive data, they must support the use of Multi-factor authentication.

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

Related Internal Controls
- E8-M2-MA-2 - Multi-factor Authentication (5): Multi-factor authentication is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data.

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

PROPRIETARY & CONFIDENTIAL

Essential 8 MA-3 - Multi-factor Authentication (8)

Essential 8 - Maturity Level 2	Other Requirements
MA-3 Multi-factor Authentication (8)	N/A

Policy
Multi-factor authentication (where available) is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.

Guidance

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

Related Internal Controls
- E8-M2-MA-3 - Multi-factor Authentication (8): Multi-factor authentication (where available) is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data.

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

PROPRIETARY & CONFIDENTIAL

Essential 8 MA-4 - Multi-factor Authentication (11)

Essential 8 - Maturity Level 2	Other Requirements
MA-4 Multi-factor Authentication (11)	N/A

Policy
Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services.

Guidance
For any external (non-organisational) users that access internet facing systems, such as on-premises systems access externally, they should be prompted to add and use Multi-factor authentication by default, i.e. the users should not have to turn on this capability after logging in.

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

Related Internal Controls
- E8-M2-MA-4 - Multi-factor Authentication (11): Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services.

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

PROPRIETARY & CONFIDENTIAL

Essential 8 MA-5 - Multi-factor Authentication (13)

Essential 8 - Maturity Level 2	Other Requirements
MA-5 Multi-factor Authentication (13)	N/A

Policy
Multi-factor authentication is used to authenticate privileged users of systems.

Guidance
For any administrators of systems (e.g. On-perm AD and Azure AD) they must use MFA to authenticate. On Office365 this should be enforced and it is recommended that Conditional Access is used. This requirement also extends to all privileged users across all systems, so administrators of 3rd party systems, Xero, Salesforce, HubSpot etc., all must use MFA. Using either firewall logs or a broker such as Microsoft Cloud App security will enable the business to get a clear picture of what systems are in use so that this can be accurately accessed.

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

Related Internal Controls
- E8-M2-MA-5 - Multi-factor Authentication (13): Multi-factor authentication is used to authenticate privileged users of systems.

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

PROPRIETARY & CONFIDENTIAL

Essential 8 MA-6 - Multi-factor Authentication (15)

Essential 8 - Maturity Level 2	Other Requirements
MA-6 Multi-factor Authentication (15)	N/A

Policy
Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.

Guidance
This requirement is to ensure the MFA is done via secure and controlled functions and not via something which can be readily circumvented (e.g. Text based 2FA codes). MFA should be done via an application on a locked device (mobile device) or locked Password Manager (that should also have MFA on it) or a dedicated hardware style MFA device.

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

Related Internal Controls
- E8-M2-MA-6 - Multi-factor Authentication (15): Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are.

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

Truncated Sample Report

PROPRIETARY & CONFIDENTIAL