Essential 8 - Maturity Level 1

Policies and Procedures

Prepared for: Client Company

Prepared by: Your IT Company

YourIT!
Your Logo Goes Here

Table of Contents

01 Purpose
02 Scope
03 Sanctions/Compliance
04 Essential 8 AC-1 - Application Control (1)
05 Essential 8 CO-1 - Configure Office Macro Settings (1)
06 Essential 8 CO-2 - Configure Office Macro Settings (5)
07 Essential 8 CO-3 - Configure Office Macro Settings (8)
08 Essential 8 CO-4 - Configure Office Macro Settings (11)
09 Essential 8 MA-1 - Multi-factor Authentication (1)
10 Essential 8 MA-2 - Multi-factor Authentication (4)
11 Essential 8 MA-3 - Multi-factor Authentication (7)
12 Essential 8 MA-4 - Multi-factor Authentication (10)
13 Essential 8 PA-1 - Patch Applications (1)
14 Essential 8 PA-2 - Patch Applications (4)
15 Essential 8 PA-3 - Patch Applications (7)
16 Essential 8 PA-4 - Patch Applications (10)
17 Essential 8 PA-5 - Patch Applications (13)
18 Essential 8 PO-1 - Patch Operating Systems (1)
19 Essential 8 PO-2 - Patch Operating Systems (4)
20 Essential 8 PO-3 - Patch Operating Systems (7)
21 Essential 8 PO-4 - Patch Operating Systems (10)
22 Essential 8 PO-5 - Patch Operating Systems (13)
23 Essential 8 RA-1 - Restrict Administrative Privileges (1)
24 Essential 8 RA-2 - Restrict Administrative Privileges (13)
25 Essential 8 RA-3 - Restrict Administrative Privileges (16)
26 Essential 8 RA-4 - Restrict Administrative Privileges (19)
27 Essential 8 RA-5 - Restrict Administrative Privileges (22)
28 Essential 8 RB-1 - Regular Backups (1)
29 Essential 8 RB-2 - Regular Backups (4)
30 Essential 8 RB-3 - Regular Backups (7)
31 Essential 8 RB-4 - Regular Backups (10)

32 Essential 8 UA-1 - User Application Hardening (1)
33 Essential 8 UA-2 - User Application Hardening (7)
34 Essential 8 UA-3 - User Application Hardening (11)
35 Essential 8 UA-4 - User Application Hardening (15)

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 1

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 (1)

Essential 8 - Maturity Level 1	Other Requirements
AC-1 Application Control (1)	N/A

Policy
The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients.

Guidance
Threats may be able to use common user operating environments to execute, this must be prevented so that anything that is downloaded via common user entry points cannot execute from the users file structure. This should be tested by trying to execute an example of each type within the outlined locations.

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

Related Internal Controls
- E8-M1-AC-1 - Application Control (1): The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients.

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 (1)

Essential 8 - Maturity Level 1	Other Requirements
CO-1 Configure Office Macro Settings (1)	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-M1-CO-1 - Configure Office Macro Settings (1): 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-2 - Configure Office Macro Settings (5)

Essential 8 - Maturity Level 1	Other Requirements
CO-2 Configure Office Macro Settings (5)	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) or similar 3rd party capability should be leveraged to ensure Macros originating from the internet are blocked and cannot be executed.

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

Related Internal Controls
- E8-M1-CO-2 - Configure Office Macro Settings (5): 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 (8)

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

Policy
Microsoft Office macro antivirus scanning is enabled

Guidance
Ensure that the Antivirus scanner that you use has support for Microsoft AMSI and that it actively scans Office Macros.

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

Related Internal Controls
- E8-M1-CO-3 - Configure Office Macro Settings (8): Microsoft Office macro antivirus scanning is enabled

References
- ASCS Essential 8 Maturity Model - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model
- Microsoft AMSI - https://www.microsoft.com/security/blog/2018/09/12/office-vba-amsi-parting-the-veil-on-malicious-macros/

Essential 8 CO-4 - Configure Office Macro Settings (11)

Essential 8 - Maturity Level 1	Other Requirements
CO-4 Configure Office Macro Settings (11)	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-M1-CO-4 - Configure Office Macro Settings (11): 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 MA-1 - Multi-factor Authentication (1)

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

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

Guidance
For all internet facing systems in use run internally must use Multi-factor authentication. This includes VPN's, Remote access and productivity systems such as On-prem Microsoft services which are accessed remotely.

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

Related Internal Controls
- E8-M1-MA-1 - Multi-factor Authentication (1): 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

Essential 8 MA-2 - Multi-factor Authentication (4)

Essential 8 - Maturity Level 1	Other Requirements
MA-2 Multi-factor Authentication (4)	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-M1-MA-2 - Multi-factor Authentication (4): 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

Essential 8 MA-3 - Multi-factor Authentication (7)

Essential 8 - Maturity Level 1	Other Requirements
MA-3 Multi-factor Authentication (7)	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-M1-MA-3 - Multi-factor Authentication (7): 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

Essential 8 MA-4 - Multi-factor Authentication (10)

Essential 8 - Maturity Level 1	Other Requirements
MA-4 Multi-factor Authentication (10)	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-M1-MA-4 - Multi-factor Authentication (10): 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

Essential 8 PA-1 - Patch Applications (1)

Essential 8 - Maturity Level 1	Other Requirements
PA-1 Patch Applications (1)	N/A

Policy
Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.

Guidance
You must have a process to patch internet facing services (i.e. any systems that are run which are accessible from the internet) within 2 weeks of the vendor releasing a patch and within 48 hours if there is a known exploit. This means having threat intelligence to be aware of the vulnerability, scanning the environment for these vulnerabilities and having a system to deploy patches.

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

Related Internal Controls
- E8-M1-PA-1 - Patch Applications (1): Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists.

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

Essential 8 PA-2 - Patch Applications (4)

Essential 8 - Maturity Level 1	Other Requirements
PA-2 Patch Applications (4)	N/A

Policy
Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.

Guidance
Have a process to patch productivity software (anything in use by end users) within 2 weeks of the vendor releasing a patch. This means having threat intelligence to be aware of the vulnerability, scanning the environment for these vulnerabilities and having a system to deploy patches.

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

Related Internal Controls
- E8-M1-PA-2 - Patch Applications (4): Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.

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

Essential 8 PA-3 - Patch Applications (7)

Essential 8 - Maturity Level 1	Other Requirements
PA-3 Patch Applications (7)	N/A

Policy
A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services.

Guidance
For any internet facing services show that they have a process that runs daily to look for missing patches and updates, for example scanning the Operating System and any Applications.

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

Related Internal Controls
- E8-M1-PA-3 - Patch Applications (7): A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services.

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

Essential 8 PA-4 - Patch Applications (10)

Essential 8 - Maturity Level 1	Other Requirements
PA-4 Patch Applications (10)	N/A

Policy
A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.

Guidance
Missing patches and updates must be scanned across the defined types, for Microsoft Office this can be Windows Update is run at least fortnightly, this can also cover email clients and browsers if only using Microsoft. Security products should have their own update scanners that also need to be run at least fortnightly. Ensure any PDF software's inbuilt scanner is running at least fortnightly. Alternatively a 3rd party solution can be used to scan for vulnerabilities across all items.

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

Related Internal Controls
- E8-M1-PA-4 - Patch Applications (10): A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.

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

Essential 8 PA-5 - Patch Applications (13)

Essential 8 - Maturity Level 1	Other Requirements
PA-5 Patch Applications (13)	N/A

Policy
Internet-facing services, 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.

Guidance
At risk software needs to be removed from the environment and software no longer supported by vendors is likely to have unreported vulnerabilities. It is critical to stay on current supported versions of software. Ensure that you have an audit and/or Asset Management approach that allows you to identify all out of date systems so they can be removed. Any system running software that cannot be updated must be segregated from the network and not be accessible from the internet, it should also be added as a Risk to risk register and be considered as a part of ongoing risk management.

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

Related Internal Controls
- E8-M1-PA-5 - Patch Applications (13): Internet-facing services, 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.

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

Truncated Sample Report