Essential 8 - Maturity Level 1

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

Table of Contents

Purpose

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

Scope

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

AC 1.1 - Application control - 1

Essential 8 - Maturity Level 1	Other Requirements
AC 1.1 Application control - 1	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.

Guidance
It is important to note that depending on the application control solution implemented, it may not support compiled Hypertext Markup Language (HTML) (.chm files), HTML applications (.hta files) and control panel applets (.cpl files), this capability needs to be tested and addressed.

To implement application control it must also cover attempts to run benign executable files. The executables tested should cover at least .exe, .com, .dll, .ocx, .ps1, .bat, .vbs, .js, .msi, .mst, .msp, .chm, .hta, and .cpl.

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

Related Internal Controls
- E8.R4.AC1.1-1657 - Application Control - 3:
  Control: ISM-1657; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3

  Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.

  Procedure
  - Due to the complexity of advanced file system permissions, and various user groups that a user account may belong to, the only truly effective way to check application control implementations is to attempt to write to and execute from all locations accessible to a user on the file system. There are several free tools available to support the assessment of this control, including ASD's Essential Eight Maturity Verification Tool (E8MVT) and Application Control Verification Tool (ACVT), AirLock Digital's Application Whitelist Auditor, and CyberArk's Evasor. There are also several paid tools available. In choosing a tool to use, make sure that it has been thoroughly tested beforehand to ensure it is fit-for-purpose.
  - If the system owner is only willing to allow the use of trusted Microsoft tools, the SysInternals AccessChk application can be used to generate the output of folder permissions, noting this is only relevant to path-based implementations. For example, by running 'accesschk -dsuvw [path] > report.txt', it is possible to generate a list of all writable paths and their access permissions for all users. Note, the 'whoami /groups' command would also need to be run to determine which user groups a typical standard user belonged to in order to determine the effective permissions for each path. Alternatively, PowerShell cmdlets can be used to test and review AppLocker policy where applicable.

- For a system on which tools cannot be run, assuming a path-based implementation is used, screenshots of the ‘effective access’ permissions for specified folders can be requested. This, however, has limitations as unless screenshots of access permissions are requested for every folder and sub-folder (for which there may be many), it will not be possible to comprehensively assess whether read, write and execute permissions exist for a given user. At a minimum, screenshots for key paths (such as temporary folders used by the operating system, web browsers and email clients) should be requested and examined to determine whether inheritance is set, noting that at any point in a path application control inheritance previously set by an operating system may be disabled by an application installer.

References

- ACSC Implementing Application Control - https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/implementing-application-control

AC 1.2 - Application control - 2

Essential 8 - Maturity Level 1	Other Requirements
AC 1.2 Application control - 2	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Application control is implemented on workstations.

Guidance
At this maturity level, the use of an application control solution is required. This may be one of the in-built solutions from Microsoft (e.g. AppLocker or Windows Defender Application Control - as covered in ACSC Application control Guidance) or it may be a third-party solution (e.g. AirLock Digital's AirLock or Threat Locker).

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

Related Internal Controls
- E8.R4.AC1.2-0843 - Application Control - 1:
  Control: ISM-0445; Revision: 7; Updated: Sep-23; Applicability: All; Essential Eight: ML2, ML3

  Privileged users are assigned a dedicated privileged account to be used solely for duties requiring privileged access.

References
- ACSC Strategies to Mitigate Cyber Incidents. NB: See 'Application Control' section on this page. - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents/strategies-mitigate-cyber-security-incidents-mitigation-details
- ACSC Implementing Application Control - https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/implementing-application-control

AC 1.3 - Application control - 3

Essential 8 - Maturity Level 1	Other Requirements
AC 1.3 Application control - 3	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.

Guidance
When conducting application control, paths for standard user profiles and temporary folders used by operating systems, web browsers and email clients can include those listed below. Note, depending on the system configuration, there may be overlap (e.g. %temp% and %tmp% generally reside within %userprofile%*).
- %userprofile%*
- %temp%*
- %tmp%*
- %windir%\Temp*

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

Related Internal Controls
- E8.R4.AC1.3-1870 - Application Control - 2:
  Control: ISM-1814; Revision: 0; Updated: Dec-22; Applicability: All; Essential Eight: ML2, ML3

  Unprivileged accounts are prevented from modifying and deleting backups.

References
- ACSC Implementing Application Control - https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/implementing-application-control

MA 1.1 - Multi-factor authentication - 1

Essential 8 - Maturity Level 1	Other Requirements
MA 1.1 Multi-factor authentication - 1	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.

Guidance
For all internet facing systems in use, these should use Multi-factor authentication. This includes VPN's, Remote access, and productivity systems such as On-prem Microsoft services which are accessed remotely over the internet. It should not be possible to authenticate to any system via the internet which only has legacy authentication methods (i.e., just a username and password).

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

Related Internal Controls

- E8.R4.MA1.1-1504 - Multi-factor Authentication Control - 1:
  Control: ISM-1504; Revision: 3; Updated: Dec-23; Applicability: All; Essential Eight: ML1, ML2, ML3

  Multi-factor authentication is used to authenticate users to their organisation’s online services that process, store or communicate their organisation’s sensitive data.

  Procedure
  - Achieve ACSC Essential Eight MFA maturity level 1 with Microsoft Entra: https://learn.microsoft.com/en-us/compliance/essential-eight/e8-mfa-maturity-level-1

References

- ACSC Implementing Multi-Factor Authentication - https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/implementing-multi-factor-authentication

MA 1.2 - Multi-factor authentication - 2

Essential 8 - Maturity Level 1	Other Requirements
MA 1.2 Multi-factor authentication - 2	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Multi-factor authentication is used to authenticate users to third-party online 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.

For simplicity it would be sensible where there are multiple such systems to use a shared iDP or SSO mechanism, or alternatively a 'password' manager which allows the storing of MFA to minimize sprawl and/or complexity which would lead users to want to try and bypass such authentication mechanisms.

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

Related Internal Controls
- E8.R4.MA1.2-1679 - Multi-factor Authentication Control - 2:
  Control: ISM-1679; Revision: 1; Updated: Sep-23; Applicability: All; Essential Eight: ML2, ML3

  Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation’s sensitive data.

References
- ACSC Implementing Multi-Factor Authentication - https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/implementing-multi-factor-authentication

MA 1.3 - Multi-factor authentication - 3

Essential 8 - Maturity Level 1	Other Requirements
MA 1.3 Multi-factor authentication - 3	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their organisation's non-sensitive data.

Guidance
While similar to requirement MA1.2 this requirement is specifically for non-sensitive data. This requires a clear understanding of the type(s) of data that are in any systems that would be covered by the requirement and what is considered "non-sensitive".

A typical, quantitative Security Posture on such subjects would take a conservative approach - that is to say that data can only be considered 'non-sensitive' if it meets such criteria such as being 'publicly available' (i.e., the data is already publicly available elsewhere and so not proprietary or private), and furthermore that the business would not be effected by the loss of this data.

The use of 'where available' in this context would give rise to the possibly accepting the use of legacy authentication for communication systems run by third parties where nothing sensitive is ever stored or transmitted and that the credential is not shared with any other system. However it would mean constant monitoring to ensure that nothing falling outside the criteria of 'non-sensitive' is ever transmitted or stored and that the credential is never used elsewhere (identity monitoring). It can be argued that in most circumstances this would create a greater burden than instead just insisting on all systems supporting MFA.

Except in exceptional circumstances such as; a legacy systems that an organisation is dependant on for operation that cannot be updated to support MFA - because the original source code is no longer available. In such circumstances a definitive plan to migrate away from such systems and implementation of other forms of security on top of them to mitigate these risks should be considered critical.

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

Related Internal Controls
- E8.R4.MA1.3-1680 - Multi-factor Authentication Control - 3:
  Control: ISM-1680; Revision: 1; Updated: Sep-23; Applicability: All; Essential Eight: ML2, ML3

  Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store, or communicate their organisation’s non-sensitive data.

References

- ACSC Implementing Multi-Factor Authentication - https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/implementing-multi-factor-authentication

MA 1.4 - Multi-factor authentication - 4

Essential 8 - Maturity Level 1	Other Requirements
MA 1.4 Multi-factor authentication - 4	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data.

Guidance
For your online customer services (systems that your customers access e.g. ticketing systems, customer portals or any service that contains their personal, health or identity related data), such as hosted or SaaS systems, your users should use Multi-factor authentication to access these.

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

Related Internal Controls
- E8.R4.MA1.4-1892 - Multi-factor Authentication Control - 4:
  Control: ISM-1892; Revision: 0; Updated: Dec-23; Applicability: All; Essential Eight: ML1, ML2, ML3

  Multi-factor authentication is used to authenticate users to their organisation’s online customer services that process, store or communicate their organisation’s sensitive customer data.

References
- ACSC Implementing Multi-Factor Authentication - https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/implementing-multi-factor-authentication

MA 1.5 - Multi-factor authentication - 5

Essential 8 - Maturity Level 1	Other Requirements
MA 1.5 Multi-factor authentication - 5	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data.

Guidance
For third-party online customer services (systems that your customers access e.g. ticketing systems, customer portals or any service that contains their personal, health or identity related data), such as hosted or SaaS systems, your users should use Multi-factor authentication.

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

Related Internal Controls
- E8.R4.MA1.5-1893 - Multi-factor Authentication Control - 5:
  Control: ISM-1893; Revision: 0; Updated: Dec-23; Applicability: All; Essential Eight: ML1, ML2, ML3

  Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation’s sensitive customer data.

References
- ACSC Implementing Multi-Factor Authentication - https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/implementing-multi-factor-authentication

MA 1.6 - Multi-factor authentication - 6

Essential 8 - Maturity Level 1	Other Requirements
MA 1.6 Multi-factor authentication - 6	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.

Guidance
For other online customer services (systems that your customers access e.g. ticketing systems, customer portals or any service that contains their personal, health or identity related data), such as hosted or SaaS systems, Customers 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, it should be presented by default.

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

Related Internal Controls
- E8.R4.MA1.6-1681 - Multi-factor Authentication Control - 6:
  Control: ISM-1681; Revision: 3; Updated: Dec-23; Applicability: All; Essential Eight: ML1, ML2, ML3

  Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.

References
- ACSC Implementing Multi-Factor Authentication - https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/implementing-multi-factor-authentication

MA 1.7 - Multi-factor authentication - 7

Essential 8 - Maturity Level 1	Other Requirements
MA 1.7 Multi-factor authentication - 7	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

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
Previously (prior to E8 November 2023), Maturity Level One did not specify the types of authentication factors that could be used for multi-factor authentication (MFA). This led to the adoption of weaker forms of MFA that used biometrics, security questions or Trusted Signals', none of which are recognised as valid authentication factors within standards. In response, the minimum standard that requires something users have', in addition to something users know', has been adopted. Be sure to read the ACSC guidelines on multi-factor authentication which clearly outline which types are supported by the Standard.

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

Related Internal Controls
- E8.R4.MA1.7-1401 - Multi-factor Authentication Control - 7:
  Control: ISM-1401; Revision: 5; Updated: Sep-21; Applicability: All; Essential Eight: ML1, ML2, ML3

  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
- ACSC Implementing Multi-Factor Authentication - https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-hardening/implementing-multi-factor-authentication

PA 1.1 - Patch applications - 1

Essential 8 - Maturity Level 1	Other Requirements
PA 1.1 Patch applications - 1	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.

Guidance
In order to patch it is critical to know what is there. You need to be using some kind of asset discovery tool such as an RMM to find all applications in your environment do you always have an up-to-date list to assess.

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

Related Internal Controls

- E8.R4.PA1.1-1807 - Patch Applications Control - 1:
  Control: ISM-1807; Revision: 0; Updated: Dec-22; Applicability: All; Essential Eight: ML2, ML3

  An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.

  Procedure
  - Ask for a demonstration of a method of asset discovery being used in an automated manner to identify assets associated with the system, such as workstations, servers, and network devices. This may be a dedicated asset discovery tool, or it may be equivalent functionality built into a vulnerability scanner. In addition, request evidence of previous automated asset discovery scans and pay attention to the date/time stamp and their scope.
  - Note, while an automated method of asset discovery should be used at least fortnightly, system owners may elect to align the frequency of asset discovery scans to more frequent timeframes used for vulnerability scans (such as daily or weekly) in order to perform both activities at the same time for optimal effect.
  - Finally, in addition to identifying assets for follow-on vulnerability scanning activities, automated asset discovery can also be used to identify any unauthorised assets that may have been connected to a system between scheduled scans. If unknown assets are identified as part of asset discovery scans, they should be immediately investigated and treated as suspicious until confirmed otherwise.

References

- ACSC Essential 8 Maturity Model - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

PA 1.2 - Patch applications - 2

Essential 8 - Maturity Level 1	Other Requirements
PA 1.2 Patch applications - 2	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.

Guidance
Any tool you are using to scan for vulnerabilities in your environment needs to use a reliable, reputable, and regularly updated source of information to populate what vulnerabilities are available. Examples of reliable sources would be NIST NVD, Greenbone (OpenVAS) and Mitre.

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

Related Internal Controls

- E8.R4.PA1.2-1808 - Patch Applications Control - 2:
  Control: ISM-1808; Revision: 0; Updated: Dec-22; Applicability: All; Essential Eight: ML2, ML3

  A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.

  Procedure
  - Ask for a demonstration of a method of asset discovery being used in an automated manner to identify assets associated with the system, such as workstations, servers, and network devices. This may be a dedicated asset discovery tool, or it may be equivalent functionality built into a vulnerability scanner. In addition, request evidence of previous automated asset discovery scans and pay attention to the date/time stamp and their scope.
  - Note, while an automated method of asset discovery should be used at least fortnightly, system owners may elect to align the frequency of asset discovery scans to more frequent timeframes used for vulnerability scans (such as daily or weekly) in order to perform both activities at the same time for optimal effect.
  - Finally, in addition to identifying assets for follow-on vulnerability scanning activities, automated asset discovery can also be used to identify any unauthorised assets that may have been connected to a system between scheduled scans. If unknown assets are identified as part of asset discovery scans, they should be immediately investigated and treated as suspicious until confirmed otherwise.

References

- NIST National Vulnerability Database - https://nvd.nist.gov/
- Mitre CVE Cyber Vulnerabilities Catalog - https://cve.mitre.org/

Truncated Sample Document