Essential 8 2023 - Maturity Level 2

Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

Table of Contents

33	MA 1.16 - Multi-factor authentication - 16
34	MA 1.17 - Multi-factor authentication - 17
35	MA 1.18 - Multi-factor authentication - 18
36	MA 1.19 - Multi-factor authentication - 19
37	PA 1.1 - Patch applications - 1
38	PA 1.2 - Patch applications - 2
39	PA 1.3 - Patch applications - 3
40	PA 1.4 - Patch applications - 4
41	PA 1.5 - Patch applications - 5
42	PA 1.6 - Patch applications - 6
43	PA 1.7 - Patch applications - 7
44	PA 1.8 - Patch applications - 8
45	PA 1.9 - Patch applications - 9
46	PA 1.10 - Patch applications - 10
47	PA 1.11 - Patch applications - 11
48	PO 1.1 - Patch operating systems - 1
49	PO 1.2 - Patch operating systems - 2
50	PO 1.3 - Patch operating systems - 3
51	PO 1.4 - Patch operating systems - 4
52	PO 1.5 - Patch operating systems - 5
53	PO 1.6 - Patch operating systems - 6
54	PO 1.7 - Patch operating systems - 7
55	PO 1.8 - Patch operating systems - 8
56	RA 1.1 - Restrict administrative privileges - 1
57	RA 1.2 - Restrict administrative privileges - 2
58	RA 1.3 - Restrict administrative privileges - 3
59	RA 1.4 - Restrict administrative privileges - 4
60	RA 1.5 - Restrict administrative privileges - 5
61	RA 1.6 - Restrict administrative privileges - 6
62	RA 1.7 - Restrict administrative privileges - 7
63	RA 1.8 - Restrict administrative privileges - 8
64	RA 1.9 - Restrict administrative privileges - 9
65	RA 1.10 - Restrict administrative privileges - 10
66	RA 1.11 - Restrict administrative privileges - 11

67	RA 1.12 - Restrict administrative privileges - 12
68	RA 1.13 - Restrict administrative privileges - 12
69	RA 1.14 - Restrict administrative privileges - 14
70	RA 1.15 - Restrict administrative privileges - 15
71	RA 1.16 - Restrict administrative privileges - 16
72	RA 1.17 - Restrict administrative privileges - 17
73	RA 1.18 - Restrict administrative privileges - 18
74	RA 1.19 - Restrict administrative privileges - 19
75	RA 1.20 - Restrict administrative privileges - 20
76	RB 1.1 - Regular backups - 1
77	RB 1.2 - Regular backups - 2
78	RB 1.3 - Regular backups - 3
79	RB 1.4 - Regular backups - 4
80	RB 1.5 - Regular backups - 5
81	RB 1.6 - Regular backups - 6
82	RB 1.7 - Regular backups - 7
83	RB 1.8 - Regular backups - 8
84	RM 1.1 - Restrict Microsoft Office macros - 1
85	RM 1.2 - Restrict Microsoft Office macros - 2
86	RM 1.3 - Restrict Microsoft Office macros - 3
87	RM 1.4 - Restrict Microsoft Office macros - 4
88	RM 1.5 - Restrict Microsoft Office macros - 5
89	UA 1.1 - User application hardening - 1
90	UA 1.2 - User application hardening - 2
91	UA 1.3 - User application hardening - 3
92	UA 1.4 - User application hardening - 4
93	UA 1.5 - User application hardening - 5
94	UA 1.6 - User application hardening - 6
95	UA 1.7 - User application hardening - 7
96	UA 1.8 - User application hardening - 8
97	UA 1.9 - User application hardening - 9
98	UA 1.10 - User application hardening - 10
99	UA 1.11 - User application hardening - 11
100	UA 1.12 - User application hardening - 12

101	UA 1.13 - User application hardening - 13
102	UA 1.14 - User application hardening - 14
103	UA 1.15 - User application hardening - 15
104	UA 1.16 - User application hardening - 16
105	UA 1.17 - User application hardening - 17
106	UA 1.18 - User application hardening - 18
107	UA 1.19 - User application hardening - 19
108	UA 1.20 - User application hardening - 20
109	UA 1.21 - User application hardening - 21
110	UA 1.22 - User application hardening - 22

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 2.

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 2023 - Maturity Level 2	Other Requirements
AC 1.1 Application control - 1	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.AC.ISM-0843.21-09.ML1-3 - Application Control:
  Control: ISM-0843; Revision: 9; Updated: Sep-21; Applicability: All; Essential Eight: ML1, ML2, ML3

  Application control is implemented on workstations.

References
- ACSC Essential 8 Maturity Model - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- 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 1.2 - Application control - 2

Essential 8 2023 - Maturity Level 2	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 internet-facing servers.

Guidance
Application control is implemented on 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.

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

Related Internal Controls
- E8.AC.ISM-1490.21-09.ML2-3 - Application Control:
  Control: ISM-1490; Revision: 3; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3

  Application control is implemented on internet-facing servers.

References
- ACSC Essential 8 Maturity Model - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- 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 2023 - Maturity Level 2	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.AC.ISM-1870.23-09.ML1-3 - Application Control:
  Control: ISM-1870; Revision: 0; Updated: Sep-23; Applicability: All; Essential Eight: ML1, ML2, ML3

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

References
- ACSC Essential 8 Maturity Model - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- 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 1.4 - Application control - 4

Essential 8 2023 - Maturity Level 2	Other Requirements
AC 1.4 Application control - 4	N/A

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

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

Guidance
Use the guidance provided in requirement AC1.1 per ACSC Maturity Level One Assessment Guidance, but apply it to all other locations on disk. Maturity Level One Guidance - Check whether the application control solution implementation covers, at a minimum, user profiles and temporary folders used by the operating system, web browsers and email clients. Note, this is only applicable to implementations reliant on path-based rules as the use of publisher-based rules and hash-based rules automatically apply across the entire system.

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

Related Internal Controls
- E8.AC.ISM-1871.23-09.ML2-3 - Application Control:
  Control: ISM-1871; Revision: 0; Updated: Sep-23; Applicability: All; Essential Eight: ML2, ML3

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

References
- ACSC Essential 8 Maturity Model - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- 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 1.5 - Application control - 5

Essential 8 2023 - Maturity Level 2	Other Requirements
AC 1.5 Application control - 5	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.AC.ISM-1657.21-09.ML1-3 - Application Control:
  Control: ISM-1657; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML1, 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 Essential 8 Maturity Model - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- 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 1.6 - Application control - 6

Essential 8 2023 - Maturity Level 2	Other Requirements
AC 1.6 Application control - 6	N/A

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

Microsoft's recommended application blocklist is 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.AC.ISM-1544.23-12.ML2-3 - Application Control:
  Control: ISM-1544; Revision: 3; Updated: Dec-23; Applicability: All; Essential Eight: ML2, ML3

  Microsoft’s recommended application blocklist is implemented.

References
- ACSC Essential 8 Maturity Model - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- 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
- Microsoft Guidelines for application blocking - https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/design/applications-that-can-bypass-wdac

AC 1.7 - Application control - 7

Essential 8 2023 - Maturity Level 2	Other Requirements
AC 1.7 Application control - 7	N/A

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

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.AC.ISM-1582.21-09.ML2-3 - Application Control:
  Control: ISM-1582; Revision: 1; Updated: Sep-21; Applicability: All; Essential Eight: ML2, ML3

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

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

AC 1.8 - Application control - 8

Essential 8 2023 - Maturity Level 2	Other Requirements
AC 1.8 Application control - 8	N/A

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

Allowed and blocked application control events are centrally logged.

Guidance
There should be a log which shows all allowed and blocked application control events. 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.AC.ISM-1660.23-12.ML2-3 - Application Control:
  Control: ISM-1660; Revision: 2; Updated: Dec-23; Applicability: All; Essential Eight: ML2, ML3

  Allowed and blocked application control events are centrally logged.

References
- ACSC Essential 8 Maturity Model - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- ASD - Windows Event Logging and Forwarding - https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/system-hardening-and-administration/system-monitoring/windows-event-logging-and-forwarding
- ASD - Guidelines for System Monitoring - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-monitoring

AC 1.9 - Application control - 9

Essential 8 2023 - Maturity Level 2	Other Requirements
AC 1.9 Application control - 9	N/A

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

Event logs are protected from unauthorised modification and deletion.

Guidance
Event logs are to be protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.

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

Related Internal Controls
- E8.AC.ISM-1815.23-12.ML2-3 - Application Control:
  Control: ISM-1815; Revision: 1; Updated: Dec-23; Applicability: All; Essential Eight: ML2, ML3

  Event logs are protected from unauthorised modification and deletion.

References
- ACSC Essential 8 Maturity Model - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- Guidelines for System Monitoring - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-monitoring

AC 1.10 - Application control - 10

Essential 8 2023 - Maturity Level 2	Other Requirements
AC 1.10 Application control - 10	N/A

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

Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.

Guidance
Logs are only useful if they are analyzed and reviewed, the frequency of review should be at minimum weekly. However real-time or near real-time collection and review is the best way to ensure your organisation can detect and respond to a security incident in a timely manner. Utilizing a SIEM tool will aid in the timely review of logs and help to correlate events across multiple systems.

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

Related Internal Controls
- E8.AC.ISM-1906.23-12.ML2-3 - Application Control:
  Control: ISM-1906; Revision: 0; Updated: Dec-23; Applicability: All; Essential Eight: ML2, ML3

  Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.

References
- ACSC Essential 8 Maturity Model - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- Guidelines for System Monitoring - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-monitoring

AC 1.11 - Application control - 11

Essential 8 2023 - Maturity Level 2	Other Requirements
AC 1.11 Application control - 11	N/A

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

Cyber security events are analysed in a timely manner to identify cyber security incidents.

Guidance
Responses to detected cyber security incidents are managed. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

Preliminarily review incident reports to confirm that they are cyber security related and necessitate incident response activities

Apply criteria to estimate the severity of an incident

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

Related Internal Controls
- E8.AC.ISM-1228.22-03.ML2-3 - Application Control:
  Control: ISM-1228; Revision: 3; Updated: Mar-22; Applicability: All; Essential Eight: ML2, ML3

  Cyber security events are analysed in a timely manner to identify cyber security incidents.

References
- ACSC Essential 8 Maturity Model - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- Guidelines for Cyber Security Incidents - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents

AC 1.12 - Application control - 12

Essential 8 2023 - Maturity Level 2	Other Requirements
AC 1.12 Application control - 12	N/A

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

Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.

Guidance
Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

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

Related Internal Controls
- E8.AC.ISM-0123.23-06.ML2-3 - Application Control:
  Control: ISM-0123; Revision: 4; Updated: Jun-23; Applicability: All; Essential Eight: ML2, ML3

  Cyber security incidents are reported to the Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered.

References
- ACSC Essential 8 Maturity Model - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- Guidelines for Cyber Security Incidents - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents

AC 1.13 - Application control - 13

Essential 8 2023 - Maturity Level 2	Other Requirements
AC 1.13 Application control - 13	N/A

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

Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.

Guidance
Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies. This requires knowing what policies, laws, regulations, legal contracts, and insurance policies require.

Refer to the cyber security incident reporting guidance from the Australian Signals Directorate (ASD) when reporting incidents to the ASD and the ACSC.

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

Related Internal Controls
- E8.AC.ISM-0140.23-09.ML2-3 - Application Control:
  Control: ISM-0140; Revision: 8; Updated: Sep-23; Applicability: All; Essential Eight: ML2, ML3

  Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.

References
- ACSC Essential 8 Maturity Model - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- Guidelines for Cyber Security Incidents - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents
- How the ASD's ACSC can help during a cyber security incident - https://www.cyber.gov.au/report-and-recover/how-asdacsc-can-help-during-cyber-security-incident

AC 1.14 - Application control - 14

Essential 8 2023 - Maturity Level 2	Other Requirements
AC 1.14 Application control - 14	N/A

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

Following the identification of a cyber security incident, the cyber security incident response plan is enacted.

Guidance
Organisations should develop an Incident Response Plan. The plan should cover the internal processes your company will activate in response to a security event; Clear roles, responsibilities, and levels of decision-making authority; Communications and information sharing both inside and outside your company; A process to fix any identified weaknesses in your systems and controls; Procedures for documenting and reporting security events and your company's response; and a post mortem of what happened and a revision of your incident response plan and information security program based on what you learned.

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

Related Internal Controls
- E8.AC.ISM-1819.23-12.ML2-3 - Application Control:
  Control: ISM-1819; Revision: 2; Updated: Dec-23; Applicability: All; Essential Eight: ML2, ML3

  Following the identification of a cyber security incident, the cyber security incident response plan is enacted.

References
- ACSC Essential 8 Maturity Model - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- Guidelines for Cyber Security Incidents - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents

MA 1.1 - Multi-factor authentication - 1

Essential 8 2023 - Maturity Level 2	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.MA.ISM-1504.23-12.ML1-3 - Multi-factor Authentication Control:
  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 Essential 8 Maturity Model - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- 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 2023 - Maturity Level 2	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.MA.ISM-1679.23-09.ML1-3 - Multi-factor Authentication Control:
  Control: ISM-1679; Revision: 1; Updated: Sep-23; Applicability: All; Essential Eight: ML1, 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 Essential 8 Maturity Model - https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model
- 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