Essential 8 - Maturity Level 3

Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

Table of Contents

33	MA 1.11 - Multi-factor authentication - 11
34	MA 1.12 - Multi-factor authentication - 12
35	MA 1.13 - Multi-factor authentication - 13
36	MA 1.14 - Multi-factor authentication - 14
37	MA 1.15 - Multi-factor authentication - 15
38	MA 1.16 - Multi-factor authentication - 16
39	MA 1.17 - Multi-factor authentication - 17
40	MA 1.18 - Multi-factor authentication - 18
41	MA 1.19 - Multi-factor authentication - 19
42	MA 1.20 - Multi-factor authentication - 20
43	MA 1.21 - Multi-factor authentication - 21
44	MA 1.22 - Multi-factor authentication - 22
45	MA 1.23 - Multi-factor authentication - 23
46	PA 1.01 - Patch applications - 1
47	PA 1.02 - Patch applications - 2
48	PA 1.03 - Patch applications - 3
49	PA 1.04 - Patch applications - 4
50	PA 1.05 - Patch applications - 5
51	PA 1.06 - Patch applications - 6
52	PA 1.07 - Patch applications - 7
53	PA 1.08 - Patch applications - 8
54	PA 1.09 - Patch applications - 9
55	PA 1.10 - Patch applications - 10
56	PA 1.11 - Patch applications - 11
57	PA 1.12 - Patch applications - 12
58	PA 1.13 - Patch applications - 13
59	PO 1.01 - Patch operating systems - 1
60	PO 1.02 - Patch operating systems - 2
61	PO 1.03 - Patch operating systems - 3
62	PO 1.04 - Patch operating systems - 4
63	PO 1.05 - Patch operating systems - 5
64	PO 1.06 - Patch operating systems - 6
65	PO 1.07 - Patch operating systems - 7
66	PO 1.08 - Patch operating systems - 8

67	PO 1.09 - Patch operating systems - 9
68	PO 1.10 - Patch operating systems - 10
69	PO 1.11 - Patch operating systems - 11
70	PO 1.12 - Patch operating systems - 12
71	PO 1.13 - Patch operating systems - 13
72	PO 1.14 - Patch operating systems - 14
73	PO 1.15 - Patch operating systems - 15
74	PO 1.16 - Patch operating systems - 16
75	RA 1.01 - Restrict administrative privileges - 1
76	RA 1.02 - Restrict administrative privileges - 2
77	RA 1.03 - Restrict administrative privileges - 3
78	RA 1.04 - Restrict administrative privileges - 4
79	RA 1.05 - Restrict administrative privileges - 5
80	RA 1.06 - Restrict administrative privileges - 6
81	RA 1.07 - Restrict administrative privileges - 7
82	RA 1.08 - Restrict administrative privileges - 8
83	RA 1.09 - Restrict administrative privileges - 9
84	RA 1.10 - Restrict administrative privileges - 10
85	RA 1.11 - Restrict administrative privileges - 11
86	RA 1.12 - Restrict administrative privileges - 12
87	RA 1.13 - Restrict administrative privileges - 13
88	RA 1.14 - Restrict administrative privileges - 14
89	RA 1.15 - Restrict administrative privileges - 15
90	RA 1.16 - Restrict administrative privileges - 16
91	RA 1.17 - Restrict administrative privileges - 17
92	RA 1.18 - Restrict administrative privileges - 18
93	RA 1.19 - Restrict administrative privileges - 19
94	RA 1.20 - Restrict administrative privileges - 20
95	RA 1.21 - Restrict administrative privileges - 21
96	RA 1.22 - Restrict administrative privileges - 22
97	RA 1.23 - Restrict administrative privileges - 23
98	RA 1.24 - Restrict administrative privileges - 24
99	RA 1.25 - Restrict administrative privileges - 25
100	RA 1.26 - Restrict administrative privileges - 26

101	RA 1.27 - Restrict administrative privileges - 27
102	RA 1.28 - Restrict administrative privileges - 28
103	RA 1.29 - Restrict administrative privileges - 29
104	RB 1.01 - Regular backups - 1
105	RB 1.02 - Regular backups - 2
106	RB 1.03 - Regular backups - 3
107	RB 1.04 - Regular backups - 4
108	RB 1.05 - Regular backups - 5
109	RB 1.06 - Regular backups - 6
110	RB 1.07 - Regular backups - 7
111	RB 1.08 - Regular backups - 8
112	RB 1.09 - Regular backups - 9
113	RB 1.10 - Regular backups - 10
114	RB 1.11 - Regular backups - 11
115	RM 1.01 - Restrict Microsoft Office macros - 1
116	RM 1.02 - Restrict Microsoft Office macros - 2
117	RM 1.03 - Restrict Microsoft Office macros - 3
118	RM 1.04 - Restrict Microsoft Office macros - 4
119	RM 1.05 - Restrict Microsoft Office macros - 5
120	RM 1.06 - Restrict Microsoft Office macros - 6
121	RM 1.07 - Restrict Microsoft Office macros - 7
122	RM 1.08 - Restrict Microsoft Office macros - 8
123	RM 1.09 - Restrict Microsoft Office macros - 9
124	RM 1.10 - Restrict Microsoft Office macros - 10
125	RM 1.11 - Restrict Microsoft Office macros - 11
126	UA 1.01 - User application hardening - 1
127	UA 1.02 - User application hardening - 2
128	UA 1.03 - User application hardening - 3
129	UA 1.04 - User application hardening - 4
130	UA 1.05 - User application hardening - 5
131	UA 1.06 - User application hardening - 6
132	UA 1.07 - User application hardening - 7
133	UA 1.08 - User application hardening - 8
134	UA 1.09 - User application hardening - 9

135	UA 1.10 - User application hardening - 10
136	UA 1.11 - User application hardening - 11
137	UA 1.12 - User application hardening - 12
138	UA 1.13 - User application hardening - 13
139	UA 1.14 - User application hardening - 14
140	UA 1.15 - User application hardening - 15
141	UA 1.16 - User application hardening - 16
142	UA 1.17 - User application hardening - 17
143	UA 1.18 - User application hardening - 18
144	UA 1.19 - User application hardening - 19
145	UA 1.20 - User application hardening - 20
146	UA 1.21 - User application hardening - 21
147	UA 1.22 - User application hardening - 22
148	UA 1.23 - User application hardening - 23
149	UA 1.24 - User application hardening - 24
150	UA 1.25 - User application hardening - 25
151	UA 1.26 - User application hardening - 26
152	UA 1.27 - User application hardening - 27

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 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.

AC 1.01 - Application control - 1

Essential 8 - Maturity Level 3	Other Requirements
AC 1.01 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 1.02 - Application control - 2

Essential 8 - Maturity Level 3	Other Requirements
AC 1.02 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 1.03 - Application control - 3

Essential 8 - Maturity Level 3	Other Requirements
AC 1.03 Application control - 3	N/A

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

Application control is implemented on non-internet-facing servers.

Guidance
Application control is implemented on non-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-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

AC 1.04 - Application control - 4

Essential 8 - Maturity Level 3	Other Requirements
AC 1.04 Application control - 4	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-1656.21-09.ML3 - Application Control:
  Control: ISM-1656; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3

  Application control is implemented on non-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 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 1.05 - Application control - 5

Essential 8 - Maturity Level 3	Other Requirements
AC 1.05 Application control - 5	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 1.06 - Application control - 6

Essential 8 - Maturity Level 3	Other Requirements
AC 1.06 Application control - 6	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 1.07 - Application control - 7

Essential 8 - Maturity Level 3	Other Requirements
AC 1.07 Application control - 7	N/A

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

Application control restricts the execution of drivers to an organisation-approved set.

Guidance
Application control can be an effective way to not only prevent malicious code from executing on workstations and servers, but also to ensure only approved applications can execute. When developing application control rulesets, determining approved executables (e.g. .exe and .com files), software libraries (e.g. .dll and.ocx files), scripts (e.g. .ps1, .bat, .cmd, .vbs and .js files), installers (e.g. .msi, .msp and .mst files), compiled HTML (e.g. .chm files), HTML applications (e.g. .hta files), control panel applets (e.g. .cpl files) and drivers based on business requirements is a more secure method than simply approving those already residing on a workstation or server. Furthermore, it is preferable that an organisation defines their own application control rulesets, rather than relying on those from application control vendors, and validate them on an annual or more frequent basis.

In implementing application control, an organisation should use a reliable method, or combination of methods, such as cryptographic hash rules, publisher certificate rules or path rules. Depending on the method chosen, further hardening may be required to ensure that application control mechanisms and application control rulesets cannot be bypassed by malicious actors.

Finally, centrally logging and analysing application control events can assist in monitoring the security posture of systems, detecting malicious behaviour and contributing to investigations following cyber security incidents.

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

Related Internal Controls
- E8.AC.ISM-1658.21-09.ML3 - Application Control:
  Control: ISM-1658; Revision: 0; Updated: Sep-21; Applicability: All; Essential Eight: ML3

  Application control restricts the execution of drivers to an organisation-approved set.

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 1.08 - Application control - 8

Essential 8 - Maturity Level 3	Other Requirements
AC 1.08 Application control - 8	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 1.09 - Application control - 9

Essential 8 - Maturity Level 3	Other Requirements
AC 1.09 Application control - 9	N/A

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

Microsoft's vulnerable driver blocklist is implemented.

Guidance
Per guidance provided by the ASD, Microsoft's vulnerable driver blocklist be implemented using core isolation's memory integrity functionality

Enabling core isolation's memory integrity functionality will automatically enforce Microsoft's vulnerable driver blocklist. This approach is preferred by Microsoft over the use of Windows Defender Application Control (WDAC) to block vulnerable or malicious drivers.

Microsoft reviews their vulnerable driver blocklist every 6-12 months and updates it automatically for organisations that have implemented core isolation's memory integrity functionality. In contrast, organisations using WDAC will need to manually update their application control rulesets when Microsoft releases an updated vulnerable driver blocklist.
From Windows 11 version 22H2 onwards, the vulnerable driver blocklist is enabled by default.

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

Related Internal Controls
- E8.AC.ISM-1659.23-12.ML3 - Application Control:
  Control: ISM-1659; Revision: 1; Updated: Dec-23; Applicability: All; Essential Eight: ML3

  Microsoft’s vulnerable driver 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

AC 1.10 - Application control - 10

Essential 8 - Maturity Level 3	Other Requirements
AC 1.10 Application control - 10	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 1.11 - Application control - 11

Essential 8 - Maturity Level 3	Other Requirements
AC 1.11 Application control - 11	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 1.12 - Application control - 12

Essential 8 - Maturity Level 3	Other Requirements
AC 1.12 Application control - 12	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.ISM-1815.23-12.ML2-3 - Event Log Protection:
  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 1.13 - Application control - 13

Essential 8 - Maturity Level 3	Other Requirements
AC 1.13 Application control - 13	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.ISM-1906.23-12.ML2-3 - Event Log Analysis:
  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 1.14 - Application control - 14

Essential 8 - Maturity Level 3	Other Requirements
AC 1.14 Application control - 14	N/A

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

Event logs from non-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.ISM-1907.23-12.ML3 - Event Log Analysis:
  Control: ISM-1907; Revision: 0; Updated: Dec-23; Applicability: All; Essential Eight: ML3

  Event logs from non-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

AC 1.15 - Application control - 15

Essential 8 - Maturity Level 3	Other Requirements
AC 1.15 Application control - 15	N/A

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

Event logs from workstations 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.ISM-0109.23-12.ML3 - Event Log Analysis:
  Control: ISM-0109; Revision: 9; Updated: Dec-23; Applicability: All; Essential Eight: ML3

  Event logs from workstations 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

Truncated Sample Report