Implementation of Australian Signal Directorate

Essential Eight for a sole trader

First published: February 2024

Introduction

This guide and implementation of the Australian Signals Directorate Essential Eight (E8) is based on the following sole trader utilising only solutions which are included Windows 11 or free/low cost.

Industry: Cryptocurrency Trading

Infrastructure:

* 1 x Windows 11 Pro based computer
* 2 x Monitors
* 1 x Router
* 1 x YubiKey
* Microsoft Office Subscription including OneDrive

Assumptions:

* Only uses online cryptocurrency trading platforms.
* Only uses this computer to conduct business.
* This Windows 11 computer is new and has not been used before.

The appendix title E8 evidence, shows all ISM controls applicable for Maturity Level 1, how the controls have been met, and where there is non compliance a justification has been provided.

Table of Contents

[Implementation 4](#_Toc158646030)

[Automated Components 4](#_Toc158646031)

[Manual Components 4](#_Toc158646032)

[Multi Factor Authentication (MFA) 4](#_Toc158646033)

[User Application Hardening 4](#_Toc158646034)

[Backups 4](#_Toc158646035)

[E8 Strategies 5](#_Toc158646036)

[Patch Applications 5](#_Toc158646037)

[Automated Component 5](#_Toc158646038)

[Manual Component 5](#_Toc158646039)

[Patch Operating Systems 6](#_Toc158646040)

[Automated Component 6](#_Toc158646041)

[Manual Component 6](#_Toc158646042)

[Multi-Factor Authentication 7](#_Toc158646043)

[Manual Component 7](#_Toc158646044)

[Restrict Administrative Privileges 8](#_Toc158646045)

[Manual Component 8](#_Toc158646046)

[Non-Compliance 8](#_Toc158646047)

[Application Control 9](#_Toc158646048)

[Automate Component 9](#_Toc158646049)

[Manual Component 9](#_Toc158646050)

[Restrict Microsoft Office Macros 10](#_Toc158646051)

[Automated Component 10](#_Toc158646052)

[User Application Hardening 11](#_Toc158646053)

[Automated Component 11](#_Toc158646054)

[Manual Component 11](#_Toc158646055)

[Regular Backups 12](#_Toc158646056)

[Manual Component 12](#_Toc158646057)

[Non-Compliance 12](#_Toc158646058)

[Appendix 13](#_Toc158646059)

[Scripts 17](#_Toc158646060)

# Implementation

Following the process to implement the sole trader E8.

## Automated Components

1. Ensure that computer has internet access and you are logged in with the administrative account.
2. Launch Microsoft PowerShell as an Administrator.
3. Running the following command;

$ScriptFromGitHub = Invoke-WebRequest "https://raw.githubusercontent.com/sdunsw/E8/main/Master.ps1"

Invoke-Expression $($ScriptFromGitHub.Content)

This script will take about 10 minutes to complete and will configure any of the automated components.

## Manual Components

Multi Factor Authentication (MFA) – Ensure that you have enabled MFA on all trading platforms using either the YubiKey or Authenticator application on your phone.

### User Application Hardening

1. Ensure that you are logged in with the account that has administrative rights.
2. Open Microsoft Edge and install “[Ad Block Plus](https://adblockplus.org/en/download)” by selecting “Microsoft Edge” and then clicking “Get Adblock plus for Microsoft Edge” and follow any on screen prompts.

### Backups

1. Ensure that you are logged in with the standard user account.
2. Open the system properties > Storage > Advanced storage settings > Back options then select OneDrive folder syncing.
3. When prompted sign in with your office account, accept any of the prompts.
4. One of the options that you will be prompted for what folders to back up. Leave the default options. Then select back up. Now when you create, delete or modify a item in those directories it will be sync’d with OneDrive.

# E8 Strategies

## Patch Applications

Total number of ISM controls: 9

Non applicable ISM controls: 1

ISM controls automated: 6

ISM controls manual: 2

### Automated Component

A schedule task has been configured to execute the patch application script with the following schedule:

|  |  |  |
| --- | --- | --- |
| **Schedule task name** | **Location of Script** | **Frequency** |
| Application Patch – On Start up | C:\Windows\E8\AppPatch\ | On Start up |
| Application Patch – 6 Hours | C:\Windows\E8\AppPatch\ | Every 6 Hours from Midnight |

The script will complete the following actions:

* Check for any applications which require an update.
* Apply and updates available for applications.

### Manual Component

Each month the operator will be required to go the vendors website to confirm, the applications are still in support and remove any upgrade any applications to the latest version. The operator could be assisted by signing up for vendor notification for new versions.

## Patch Operating Systems

Total number of ISM controls: 8

Non applicable ISM controls: 1

ISM controls automated: 6

ISM controls manual: 1

### Automated Component

A schedule task has been configured to execute the patch operating system script with the following schedule:

|  |  |  |
| --- | --- | --- |
| **Schedule task name** | **Location of Script** | **Frequency** |
| OS Patch – On Start up | C:\Windows\E8\OSPatch\ | On Start up |
| OS Patch – Daily | C:\Windows\E8\OSPatch\ | Daily at 12 noon |
|  |  |  |

The script will complete the following actions:

* Apply registry setting to control the behaviour Windows Update Service
* Check for any available patches.
* Apply any available patches.

### Manual Component

Every 3 months the operator will be required to go the [Microsoft Support page](https://learn.microsoft.com/en-us/lifecycle/products/windows-11-home-and-pro) to determine if the operating system is still supported. The current version of Windows 11 is supported until November 11th 2025. If the operating system is no longer supported, the recommend course of action will be to replace the whole device and start again.

## Multi-Factor Authentication

Total number of ISM controls: 7

Non applicable ISM controls: 0

ISM controls automated: 0

ISM controls manual: 7

### Manual Component

The operator will need to configure multi factor authentication on any cloud-based solutions they use manually.

## Restrict Administrative Privileges

Total number of ISM controls: 7

Non applicable ISM controls: 0

ISM controls automated: 0

ISM controls manual: 2

ISM controls non-compliant: 5 (ISM-1175, ISM-1883, ISM-1380, ISM-1688 and ISM-1689)

### Manual Component

Once the master script has been executed the operator will be need to create a standard user account on the computer. This account will be used for the day-to-day operations of the business. Instructions on how to create an account can be found [here](https://support.microsoft.com/en-us/windows/create-a-local-user-or-administrator-account-in-windows-20de74e0-ac7f-3502-a866-32915af2a34d).

### Non-Compliance

Due to the operating environment only containing 1 device, privilege and non-privileged activities cannot be separated. With different gateway hardware it might be possible to restrict administrative users from accessing the internet. An alternate option would be to use a protective domain name service to protect the internet traffic.

## Application Control

Total number of ISM controls: 3

Non applicable ISM controls: 0

ISM controls automated: 3

ISM controls manual: 0

### Automate Component

The master installation script will install all necessary Windows components required for AppLocker to work correctly and apply a base AppLocker policy, which includes Adobe products. The script will also set the associated AppLocker services to protected, preventing the user from disabling the services. This is script is only executed once.

### Manual Component

If the user requires to add additional rules for new software, they will need to log in to the system as the administrator and modify the AppLocker policy. Instructions on how to complete this can be found [here](https://learn.microsoft.com/en-us/windows/security/application-security/application-control/windows-defender-application-control/applocker/edit-an-applocker-policy#editing-an-applocker-policy-by-using-the-local-security-policy-snap-in).

## Restrict Microsoft Office Macros

Total number of ISM controls: 4

Non applicable ISM controls: 0

ISM controls automated: 4

ISM controls manual: 0

### Automated Component

A scheduled task has been configured to execute the macro hardening script with the following schedule

|  |  |  |
| --- | --- | --- |
| **Schedule task name** | **Location of Script** | **Frequency** |
| Macro – On Start up | C:\Windows\E8\Macro\ | On Start up |
| Macro – 6 Hours | C:\Windows\E8\Macro\ | Every 6 Hours from Midnight |

The script configures registry value for the office applications to prevent the followings:

* Disabled all Macro’s from executing.
* Blocked Macro’s originating from the internet.
* Prevent users from modifying security settings.
* Enable Attack Surface Rules for antivirus scanning using Windows Defender.

## User Application Hardening

Total number of ISM controls: 4

Non applicable ISM controls: 1

ISM controls automated: 3

ISM controls manual: 1

### Automated Component

A scheduled task has been configured to execute the user hardening script with the following schedule

|  |  |  |
| --- | --- | --- |
| **Schedule task name** | **Location of Script** | **Frequency** |
| User Hardening – On Start up | C:\Windows\E8\User\ | On Start up |
| User Hardening – 6 Hours | C:\Windows\E8\ User \ | Every 6 Hours from Midnight |

The script configures registry value to prevent the following:

* Stop Java processing.
* Stop the user from being able to modify web browser security settings.

### Manual Component

The operator will have to install a browser based ad blocking application called “[Ad Block Plus](https://adblockplus.org/en/download)” There are versions available for Microsoft Edge and Google Chrome.

## Regular Backups

Total number of ISM controls: 6

Non applicable ISM controls: 0

ISM controls automated: 0

ISM controls manual: 6

ISM controls non-compliant: 2 (ISM-1812 and ISM-1814)

### Manual Component

The operator will need to configure windows back up to use the Microsoft OneDrive as the destination location for backs. This option was selected because it can be accessed from any computer with an internet connection.

### Non-Compliance

There are 2 controls relating to the unprivileged accounts access backups belonging to other accounts and modifying and deleting backs. In this specific scenario, although technically possible to achieve it would add too much complexity around the solution.

## Appendix

**Table 1: E8 evidence**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Mitigation Strategy** | **Essential Eight Requirement** | **ISM Control** | **Applicability** | **Practical** | **Comments\Evidence** |
| **Patch applications** | An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities. | ISM-1807 | No |  | There is only 1 device in this deployment. |
| A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. | ISM-1808 | Yes | Yes | Applicationpatching.ps1 script |
| A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services. | ISM-1698 | Yes | Yes | Applicationpatching.ps1 script |
| A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. | ISM-1699 | Yes | Yes | Applicationpatching.ps1 script |
| Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. | ISM-1876 | Yes | Yes | Applicationpatching.ps1 script |
| Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. | ISM-1690 | Yes | Yes | Applicationpatching.ps1 script |
| Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release. | ISM-1691 | Yes | Yes | Applicationpatching.ps1 script |
| Online services that are no longer supported by vendors are removed. | ISM-1905 | Yes | Yes | Manual check which user is required to complete. |
| 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. | ISM-1704 | Yes | Yes | Manual check which user is required to complete. |
| **Patch operating systems** | An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities. | ISM-1807 | No |  | There is only 1 device in this deployment. |
| A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. | ISM-1808 | Yes | Yes | Ospatching.ps1 script |
| A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices. | ISM-1701 | Yes | Yes | Ospatching.ps1 script |
| A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices. | ISM-1702 | Yes | Yes | Ospatching.ps1script |
| Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. | ISM-1877 | Yes | Yes | Ospatching.ps1 script |
| Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. | ISM-1694 | Yes | Yes | Ospatching.ps1 script |
| Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release. | ISM-1695 | Yes | Yes | Ospatching.ps1 script |
| Operating systems that are no longer supported by vendors are replaced. | ISM-1501 | Yes | Yes | Manual check which user is required to complete. |
| **Multi-factor authentication** | Multi-factor authentication is used to authenticate users to their organisation’s online services that process, store or communicate their organisation’s sensitive data. | ISM-1504 | Yes | Yes | All sensitive data is hosted on 3rd party cloud-based platforms. These platforms require MFA. Whist it is technical possible to have MFA with Windows, the complexity and cost doesn't warrant it in the is application of E8. |
| Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation’s sensitive data. | ISM-1679 | Yes | Yes |
| 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. | ISM-1680 | Yes | Yes |
| 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. | ISM-1892 | Yes | Yes |
| 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. | ISM-1893 | Yes | Yes |
| Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data. | ISM-1681 | Yes | Yes |
| 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. | ISM-1401 | Yes | Yes |
| **Restrict administrative privileges** | Requests for privileged access to systems, applications and data repositories are validated when first requested. | ISM-1507 | Yes | Yes | There is only 1 operator in the solution. They have a valid business case to have an administrative account. |
| Privileged users are assigned a dedicated privileged account to be used solely for duties requiring privileged access. | ISM-0445 | Yes | Yes | Creation of both a privileged and non-privileged account. |
| Privileged accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services. | ISM-1175 | Yes | No | Due to the infrastructure available, this isn't possible to control. |
| Privileged accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties. | ISM-1883 | Yes | No | Due to the only have one device, these controls can't be applied. |
| Privileged users use separate privileged and unprivileged operating environments. | ISM-1380 | Yes | No |
| Unprivileged accounts cannot logon to privileged operating environments. | ISM-1688 | Yes | No |
| Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. | ISM-1689 | Yes | No |
| **Application control** | Application control is implemented on workstations. | ISM-0843 | Yes | Yes | AppLocker.ps1 script |
| Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients. | ISM-1870 | Yes | Yes | AppLocker.ps1 script |
| Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set. | ISM-1657 | Yes | Yes | AppLocker.ps1 script |
| **Restrict Microsoft Office macros** | Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. | ISM-1671 | Yes | Yes | Macro.ps1 script |
| Microsoft Office macros in files originating from the internet are blocked. | ISM-1488 | Yes | Yes | Macro.ps1 script |
| Microsoft Office macro antivirus scanning is enabled. | ISM-1672 | Yes | Yes | Macro.ps1 script |
| Microsoft Office macro security settings cannot be changed by users. | ISM-1489 | Yes | Yes | Macro.ps1 script |
| **User application hardening** | Internet Explorer 11 is disabled or removed. | ISM-1654 | No |  | Windows 11 doesn't include Internet Explorer 11. |
| Web browsers do not process Java from the internet. | ISM-1486 | Yes | Yes | UserHandening.ps1 script |
| Web browsers do not process web advertisements from the internet. | ISM-1485 | Yes | Yes | Adblocker |
| Web browser security settings cannot be changed by users. | ISM-1585 | Yes | Yes | UserHandening.ps1 script |
| **Regular backups** | Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements. | ISM-1511 | Yes | Yes | Sole trader to determine this. |
| Backups of data, applications and settings are synchronised to enable restoration to a common point in time. | ISM-1810 | Yes | Yes | Microsoft OneDrive provides a 90 day recycling bin service, where files can be retrieved from. |
| Backups of data, applications and settings are retained in a secure and resilient manner. | ISM-1811 | Yes | Yes | Microsoft 365 is a secure platform which has undergone security accreditation. The service officers MFA and other security features. |
| Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises. | ISM-1515 | Yes | Yes | SOP to restore. |
| Unprivileged accounts cannot access backups belonging to other accounts. | ISM-1812 | Yes | No | Technical possible, to implement a solution would add to much complexity. |
| Unprivileged accounts are prevented from modifying and deleting backups. | ISM-1814 | Yes | No |

# Scripts

To be included later.