Essential 8 Maturity Levels

FUTURECOMPUTERS
Business IT Solutions

Essential 8 Strategy	Maturity Level 1	Maturity Level 2	Maturity Level 3
Application Control	The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients.	**Application control is implemented on workstations and 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**. **Allowed and blocked executions on workstations and internet-facing servers are logged.**	Application control is implemented on workstations and **servers** to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets **and drivers** to an organisation-approved set. **Microsoft's 'recommended block rules' are implemented.** **Microsoft's 'recommended driver block rules' are implemented.** **Application control rulesets are validated on an annual or more frequent basis.** Allowed and blocked executions on workstations and servers are **centrally** logged **and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.**
Patch Applications	Patches, updates or vendor mitigations for security vulnerabilities in internet- facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release. A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services. A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	Patches, updates or vendor mitigations for security vulnerabilities in internet- facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within **two weeks** of release. **Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month.** A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services. A vulnerability scanner is used at least **weekly** to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. **A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications.** Internet-facing services, office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.	Patches, updates or vendor mitigations for security vulnerabilities in internet- facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release, or **within 48 hours if an exploit exists.** Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month. A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications. **Applications** that are no longer supported by vendors are removed.

Configure Microsoft Office macro settings	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. Microsoft Office macros in files originating from the internet are blocked. Microsoft Office macro antivirus scanning is enabled. Microsoft Office macro security settings cannot be changed by users.	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. Microsoft Office macros in files originating from the internet are blocked. Microsoft Office macro antivirus scanning is enabled. **Microsoft Office macros are blocked from making Win32 API calls.** Microsoft Office macro security settings cannot be changed by users. **Allowed and blocked Microsoft Office macro executions are logged.**	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. **Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute.** **Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.** **Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View.** **Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.** Microsoft Office macros in files originating from the internet are blocked. Microsoft Office macro antivirus scanning is enabled. Microsoft Office macros are blocked from making Win32 API calls. Microsoft Office macro security settings cannot be changed by users. Allowed and blocked Microsoft Office macro executions are **centrally** logged and **protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.**
User application hardening	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 does not process content from the internet. Web browser security settings cannot be changed by users.	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 does not process content from the internet. **Microsoft Office is blocked from creating child processes.** **Microsoft Office is blocked from creating executable content.** **Microsoft Office is blocked from injecting code into other processes.** **Microsoft Office is configured to prevent activation of OLE packages.** **PDF software is blocked from creating child processes.** **ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented.** Web browser, **Microsoft Office and PDF software** security settings cannot be changed by users. **Blocked PowerShell script executions are logged.**	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 is **disabled or removed.** Microsoft Office is blocked from creating child processes. Microsoft Office is blocked from creating executable content. Microsoft Office is blocked from injecting code into other processes. Microsoft Office is configured to prevent activation of OLE packages. PDF software is blocked from creating child processes. ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented. Web browser, Microsoft Office and PDF software security settings cannot be changed by users. **.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.** **Windows PowerShell 2.0 is disabled or removed.** **PowerShell is configured to use Constrained Language Mode.** Blocked PowerShell script executions are **centrally** logged and **protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.**

Restrict administrative privileges	Requests for privileged access to systems and applications are validated when first requested. Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services. Privileged users use separate privileged and unprivileged operating environments. Unprivileged accounts cannot logon to privileged operating environments. Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Requests for privileged access to systems and applications are validated when first requested. **Privileged access to systems and applications is automatically disabled after 12 months unless revalidated.** **Privileged access to systems and applications is automatically disabled after 45 days of inactivity.** Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services. Privileged users use separate privileged and unprivileged operating environments. **Privileged operating environments are not virtualised within unprivileged operating environments.** Unprivileged accounts cannot logon to privileged operating environments. Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. **Administrative activities are conducted through jump servers.** **Credentials for local administrator accounts and service accounts are unique, unpredictable and managed.** **Use of privileged access is logged.** **Changes to privileged accounts and groups are logged.**	Requests for privileged access to systems and applications are validated when first requested. Privileged access to systems and applications is automatically disabled after 12 months unless revalidated. Privileged access to systems and applications is automatically disabled after 45 days of inactivity. **Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties.** Privileged accounts are prevented from accessing the internet, email and web services. Privileged users use separate privileged and unprivileged operating environments. Privileged operating environments are not virtualised within unprivileged operating environments. Unprivileged accounts cannot logon to privileged operating environments. Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. **Just-in-time administration is used for administering systems and applications.** Administrative activities are conducted through jump servers. Credentials for local administrator accounts and service accounts are unique, unpredictable and managed. **Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled.** Use of privileged access is **centrally** logged and **protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.** Changes to privileged accounts and groups are **centrally** logged and **protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.**

Multi-factor authentication	Multi-factor authentication is used by an organisation’s users if they authenticate to their organisation’s internet-facing services. Multi-factor authentication is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their organisation’s sensitive data. Multi-factor authentication (where available) is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their organisation’s non-sensitive data. Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation’s internet- facing services.	Multi-factor authentication is used by an organisation’s users if they authenticate to their organisation’s internet-facing services. Multi-factor authentication is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their organisation’s sensitive data. Multi-factor authentication (where available) is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their organisation’s non-sensitive data. Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation’s internet- facing services. **Multi-factor authentication is used to authenticate privileged users of systems.** **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.** **Successful and unsuccessful multi-factor authentications are logged.**	Multi-factor authentication is used by an organisation’s users if they authenticate to their organisation’s internet-facing services. Multi-factor authentication is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their organisation’s sensitive data. Multi-factor authentication (where available) is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their organisation’s non-sensitive data. Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation’s internet- facing services. Multi-factor authentication is used to authenticate privileged users of systems. **Multi-factor authentication is used to authenticate users accessing important data repositories.** Multi-factor authentication is **verifier impersonation resistant and** uses either: something users have and something users know, or something users have that is unlocked by something users know or are. Successful and unsuccessful multi-factor authentications are **centrally** logged and **protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected.**
Regular backups	Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements. Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises. Unprivileged accounts can only access their own backups. Unprivileged accounts are prevented from modifying or deleting backups	Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements. Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises. Unprivileged accounts, **and privileged accounts (excluding backup administrators)**, can only access their own backups. Unprivileged accounts, **and privileged accounts (excluding backup administrators),** are prevented from modifying or deleting backups.	Backups of important data, software and configuration settings are performed and retained in a coordinated and resilient manner in accordance with business continuity requirements. Restoration of systems, software and important data from backups is tested in a coordinated manner as part of disaster recovery exercises. Unprivileged accounts, and privileged accounts (excluding backup administrators), **cannot access backups**. Unprivileged accounts, and privileged accounts (excluding backup **break glass accounts),** are prevented from modifying or deleting backups.

Patch operating systems	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within one month of release. A vulnerability scanner is used at least daily to identify missing patches for security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least fortnightly to identify missing patches for security vulnerabilities in operating systems of workstations, servers and network devices. Operating systems that are no longer supported by vendors are replaced.	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within **two weeks** of release. A vulnerability scanner is used at least daily to identify missing patches for security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least **weekly** to identify missing patches for security vulnerabilities in operating systems of workstations, servers and network devices. Operating systems that are no longer supported by vendors are replaced.	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release, **or within 48 hours if an exploit exists.** A vulnerability scanner is used at least daily to identify missing patches for security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches for security vulnerabilities in operating systems of workstations, servers and network devices. **The latest release, or the previous release, of operating systems are used for workstations, servers and network devices.** Operating systems that are no longer supported by vendors are replaced.

> "An attacker only needs
> **one vulnerability**
> to damage your business reputation,
> which you have spent years building."

Prevents attacks

- Application Control
- Patch Applications
- Configure Microsoft Office Macros
- User Application Hardening

Limits extent of attacks

- Restrict Admin Privileges
- Patch Operating System
- Multi-Factor Authentication

Recovers data & system availability

- Daily Backups

How does your business measure up with the Essential 8?

Contact us today for help improving your cyber security stance.

07 4058 5700

www.futurecomputers.com.au | enquiries@futurecomputers.com.au

Australian Government
Australian Signals Directorate

ACSC
Australian
Cyber Security
Centre

147 ANDERSON ST, MANUNDA, QLD, AUSTRALIA, 4870