

Australian Government Australian Signals Directorate



# **Essential Eight Maturity Model**

First published: Last updated: June 2017 November 2023

### Introduction

The Australian Signals Directorate (ASD) has developed prioritised mitigation strategies, in the form of the <u>Strategies</u> <u>to Mitigate Cyber Security Incidents</u>, to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the Essential Eight.

The Essential Eight has been designed to protect organisations' internet-connected information technology networks. While the principles behind the Essential Eight may be applied to enterprise mobility and operational technology networks, it was not designed for such purposes and alternative mitigation strategies may be more appropriate to defend against unique cyber threats to these environments.

The *Essential Eight Maturity Model*, first published in June 2017 and updated regularly, supports the implementation of the Essential Eight. It is based on ASD's experience in producing cyber threat intelligence, responding to cyber security incidents, conducting penetration testing and assisting organisations to implement the Essential Eight.

### Implementation

When implementing the Essential Eight, organisations should identify and plan for a target maturity level suitable for their environment. Organisations should then progressively implement each maturity level until that target is achieved.

As the mitigation strategies that constitute the Essential Eight have been designed to complement each other, and to provide coverage of various cyber threats, organisations should plan their implementation to achieve the same maturity level across all eight mitigation strategies before moving onto higher maturity levels.

Organisations should implement the Essential Eight using a risk-based approach. In doing so, organisations should seek to minimise any exceptions and their scope, for example, by implementing compensating controls and ensuring the number of systems or users impacted are minimised. In addition, any exceptions should be documented and approved through an appropriate process. Subsequently, the need for any exceptions, and associated compensating controls, should be monitored and reviewed on a regular basis. Note, the appropriate use of exceptions should not preclude an organisation from being assessed as meeting the requirements for a given maturity level.

As the Essential Eight outlines a minimum set of preventative measures, organisations need to implement additional measures to those within this maturity model where it is warranted by their environment. Further, while the Essential Eight can help to mitigate the majority of cyber threats, it will not mitigate all cyber threats. As such, additional mitigation strategies and controls need to be considered, including those from the <u>Strategies to Mitigate Cyber</u> <u>Security Incidents</u> and the <u>Information Security Manual</u>.



Finally, there is no requirement for organisations to have their Essential Eight implementation certified by an independent party. However, Essential Eight implementations may need to be assessed by an independent party if required by a government directive or policy, by a regulatory authority, or as part of contractual arrangements.

# Maturity levels

To assist organisations with their implementation of the Essential Eight, four maturity levels have been defined (Maturity Level Zero through to Maturity Level Three). With the exception of Maturity Level Zero, the maturity levels are based on mitigating increasing levels of tradecraft (i.e. tools, tactics, techniques and procedures) and targeting, which are discussed in more detail below. Depending on overall capability, malicious actors may exhibit different levels of tradecraft for different operations against different targets. For example, malicious actors capable of advanced tradecraft may use it against one target while using basic tradecraft against another. As such, organisations should consider what level of tradecraft and targeting, rather than which malicious actors, they are aiming to mitigate.

Organisations need to consider that the likelihood of being targeted is influenced by their desirability to malicious actors, and the consequences of a cyber security incident will depend on their requirement for the confidentiality of their data, as well as their requirement for the availability and integrity of their systems and data. This, in combination with the descriptions for each maturity level, can be used to help determine a target maturity level to implement.

Finally, Maturity Level Three will not stop malicious actors that are willing and able to invest enough time, money and effort to compromise a target. As such, organisations still need to consider the remainder of the mitigation strategies from the <u>Strategies to Mitigate Cyber Security Incidents</u> and the <u>Information Security Manual</u>.

### **Maturity Level Zero**

This maturity level signifies that there are weaknesses in an organisation's overall cyber security posture. When exploited, these weaknesses could facilitate the compromise of the confidentiality of their data, or the integrity or availability of their systems and data, as described by the tradecraft and targeting in Maturity Level One below.

### **Maturity Level One**

The focus of this maturity level is malicious actors who are content to simply leverage commodity tradecraft that is widely available in order to gain access to, and likely control of, a system. For example, malicious actors opportunistically using a publicly-available exploit for a vulnerability in an online service which had not been patched, or authenticating to an online service using credentials that were stolen, reused, brute forced or guessed.

Generally, malicious actors are looking for any victim rather than a specific victim and will opportunistically seek common weaknesses in many targets rather than investing heavily in gaining access to a specific target. Malicious actors will employ common social engineering techniques to trick users into weakening the security of a system and launch malicious applications. If user accounts that malicious actors compromise have special privileges they will exploit it. Depending on their intent, malicious actors may also destroy data (including backups).

### **Maturity Level Two**

The focus of this maturity level is malicious actors operating with a modest step-up in capability from the previous maturity level. These malicious actors are willing to invest more time in a target and, perhaps more importantly, in the effectiveness of their tools. For example, these malicious actors will likely employ well-known tradecraft in order to better attempt to bypass controls implemented by a target and evade detection. This includes actively targeting credentials using phishing and employing technical and social engineering techniques to circumvent weak multi-factor authentication.



Generally, malicious actors are likely to be more selective in their targeting but still somewhat conservative in the time, money and effort they may invest in a target. Malicious actors will likely invest time to ensure their phishing is effective and employ common social engineering techniques to trick users to weaken the security of a system and launch malicious applications. If user accounts that malicious actors compromise have special privileges they will exploit it, otherwise they will seek user accounts with special privileges. Depending on their intent, malicious actors may also destroy all data (including backups) accessible to a user account with special privileges.

### **Maturity Level Three**

The focus of this maturity level is malicious actors who are more adaptive and much less reliant on public tools and techniques. These malicious actors are able to exploit the opportunities provided by weaknesses in their target's cyber security posture, such as the existence of older software or inadequate logging and monitoring. Malicious actors do this to not only extend their access once initial access has been gained to a target, but to evade detection and solidify their presence. Malicious actors make swift use of exploits when they become publicly available as well as other tradecraft that can improve their chance of success.

Generally, malicious actors may be more focused on particular targets and, more importantly, are willing and able to invest some effort into circumventing the idiosyncrasies and particular policy and technical controls implemented by their targets. For example, this includes social engineering a user to not only open a malicious document but also to unknowingly assist in bypassing controls. This can also include circumventing stronger multi-factor authentication by stealing authentication token values to impersonate a user. Once a foothold is gained on a system, malicious actors will seek to gain privileged credentials or password hashes, pivot to other parts of a network, and cover their tracks. Depending on their intent, malicious actors may also destroy all data (including backups).

### **Requirements for each maturity level**

Requirements for Maturity Level One through to Maturity Level Three are outlined in Appendices A to C. A comparison of the maturity levels, with changes between maturity levels indicated via bolded text, is outlined in Appendix D.

# **Further information**

The *Essential Eight Maturity Model* is part of a suite of related publications:

- Answers to questions on this maturity model are available in the *Essential Eight Maturity Model FAQ* publication.
- Additional mitigation strategies are available in the <u>Strategies to Mitigate Cyber Security Incidents</u> publication.
- Further Information on patching activities is available in the <u>Patching Applications and Operating Systems</u> publication.
- Further Information on implementing multi-factor authentication is available in the <u>Implementing Multi-Factor</u> <u>Authentication</u> publication.
- Further Information on controlling privileged user accounts is available in the <u>Restricting Administrator Privileges</u> publication.
- Further Information on implementing application control is available in the <u>Implementing Application Control</u> publication.
- Further Information on controlling Microsoft Office macros is available in the <u>Restricting Microsoft Office Macros</u> publication.



# **Contact details**

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).



# Appendix A: Maturity Level One

Mitigation Strategy	Description
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
	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.
	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.
	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.
	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.
	Online services that are no longer supported by vendors are removed.
	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.
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.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	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.
	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.



	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.
	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.
	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.
	Operating systems that are no longer supported by vendors are replaced.
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.
	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.
	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.
	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.
	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.
	Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.
	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.
Restrict administrative	Requests for privileged access to systems, applications and data repositories are validated when first requested.
privileges	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.
	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.
	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.



	Privileged users use separate privileged and unprivileged operating environments.
	Unprivileged user accounts cannot logon to privileged operating environments.
	Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.
Application control	Application control is implemented on workstations.
	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.
	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.
Restrict Microsoft Office macros	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.
User application hardening	Internet Explorer 11 is disabled or removed.
naracining	Web browsers do not process Java from the internet.
	Web browsers do not process web advertisements from the internet.
	Web browser security settings cannot be changed by users.
Regular backups	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.
	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.
	Backups of data, applications and settings are retained in a secure and resilient manner.
	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.
	Unprivileged user accounts cannot access backups belonging to other user accounts.
	Unprivileged user accounts are prevented from modifying and deleting backups.



# Appendix B: Maturity Level Two

Mitigation Strategy	Description
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
	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.
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.
	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.
	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.
	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.
	Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.
	Online services that are no longer supported by vendors are removed.
	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.
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.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.



	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.
	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.
	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.
	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.
	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.
	Operating systems that are no longer supported by vendors are replaced.
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.
	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.
	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.
	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.
	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.
	Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.
	Multi-factor authentication is used to authenticate privileged users of systems.
	Multi-factor authentication is used to authenticate unprivileged 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.



-	Multi-factor authentication used for authenticating users of online services is phishing- resistant.
	Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.
	Multi-factor authentication used for authenticating users of systems is phishing-resistant.
	Successful and unsuccessful multi-factor authentication events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	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.
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Restrict administrative privileges	Requests for privileged access to systems, applications and data repositories are validated when first requested.
privileges	Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated.
	Privileged access to systems and applications is disabled after 45 days of inactivity.
	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.
	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.
	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.
	Privileged users use separate privileged and unprivileged operating environments.
	Privileged operating environments are not virtualised within unprivileged operating environments.



Unprivileged user	accounts canno	t logon to	nrivilaged o	operating environmer	ntc
Unprivileged user	accounts canno	ι ισχυπιτυ	privilegeu	Sperating environner	ILS.

	Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.
	Administrative activities are conducted through jump servers.
	Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.
	Privileged access events are centrally logged.
	Privileged user account and security group management events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	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.
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Application control	Application control is implemented on workstations.
	Application control is implemented on internet-facing servers.
	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.
	Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.
	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.
	Microsoft's recommended application blocklist is implemented.
	Application control rulesets are validated on an annual or more frequent basis.



	Allowed and blocked application control events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	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.
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Restrict Microsoft Office macros	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.
User application hardening	Internet Explorer 11 is disabled or removed.
	Web browsers do not process Java from the internet.
	Web browsers do not process web advertisements from the internet.
	Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
	Web browser security settings cannot be changed by users.
	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 Object Linking and Embedding packages.



	Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
	Office productivity suite security settings cannot be changed by users.
	PDF software is blocked from creating child processes.
	PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
	PDF software security settings cannot be changed by users.
	PowerShell module logging, script block logging and transcription events are centrally logged.
	Command line process creation events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	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.
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Regular backups	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.
	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.
	Backups of data, applications and settings are retained in a secure and resilient manner.
	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.
	Unprivileged user accounts cannot access backups belonging to other user accounts.
	Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts.



Unprivileged user accounts are prevented from modifying and deleting backups.

Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.



# Appendix C: Maturity Level Three

Mitigation Strategy	Description
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
	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.
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.
	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.
	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.
	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 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
	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 when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
	Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.
	Online services that are no longer supported by vendors are removed.
	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.



	Applications other than 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.
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.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	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.
	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.
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in drivers.
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in firmware.
	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.
	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.
	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 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
	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 when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
	Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.



	Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
	Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
	Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
	The latest release, or the previous release, of operating systems are used.
	Operating systems that are no longer supported by vendors are replaced.
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.
	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.
	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.
	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.
	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.
	Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.
	Multi-factor authentication is used to authenticate privileged users of systems.
	Multi-factor authentication is used to authenticate unprivileged users of systems.
	Multi-factor authentication is used to authenticate users of data repositories.
	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.
	Multi-factor authentication used for authenticating users of online services is phishing-resistant.
	Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant.



	Multi-factor authentication used for authenticating users of systems is phishing-resistant.
	Multi-factor authentication used for authenticating users of data repositories is phishing- resistant.
	Successful and unsuccessful multi-factor authentication events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.
	Event logs from workstations are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	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.
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Restrict administrative	Requests for privileged access to systems, applications and data repositories are validated when first requested.
privileges	Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated.
	Privileged access to systems and applications is disabled after 45 days of inactivity.
	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.
	Privileged access to systems, applications and data repositories is limited to only what is required for users and services to undertake their duties.
	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.
	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.



Secure Admin Workstations are used in the performance of administrative activities.

Privileged users use separate privileged and unprivileged operating environments.

Privileged operating environments are not virtualised within unprivileged operating environments.

Unprivileged user accounts cannot logon to privileged operating environments.

Privileged user 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 break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.

Memory integrity functionality is enabled.

Local Security Authority protection functionality is enabled.

Credential Guard functionality is enabled.

Remote Credential Guard functionality is enabled.

Privileged access events are centrally logged.

Privileged user account and security group management events are centrally logged.

Event logs are protected from unauthorised modification and deletion.

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

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

Event logs from workstations are analysed in a timely manner to detect cyber security events.

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

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.



Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Application control is implemented on workstations.
Application control is implemented on internet-facing servers.
Application control is implemented on non-internet-facing servers.
Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.
Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.
Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.
Application control restricts the execution of drivers to an organisation-approved set.
Microsoft's recommended application blocklist is implemented.
Microsoft's vulnerable driver blocklist is implemented.
Application control rulesets are validated on an annual or more frequent basis.
Allowed and blocked application control events are centrally logged.
Event logs are protected from unauthorised modification and deletion.
Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.
Event logs from workstations are analysed in a timely manner to detect cyber security events.
Cyber security events are analysed in a timely manner to identify cyber security incidents.
Cyber security incidents are reported to the Chief Information Security Officer, or one of



	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Restrict Microsoft Office macros	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.
	Microsoft Office macros are checked to ensure they are free of malicious code before being digitally signed or placed within Trusted Locations.
	Only privileged users responsible for checking 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 macros digitally signed by signatures other than V3 signatures 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.
User application	Internet Explorer 11 is disabled or removed.
hardening	Web browsers do not process Java from the internet.
	Web browsers do not process web advertisements from the internet.
	Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
	Web browser security settings cannot be changed by users.
	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 Object Linking and Embedding packages.

Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.

Office productivity suite security settings cannot be changed by users.

PDF software is blocked from creating child processes.

PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.

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.

PowerShell module logging, script block logging and transcription events are centrally logged.

Command line process creation events are centrally logged.

Event logs are protected from unauthorised modification and deletion.

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

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

Event logs from workstations are analysed in a timely manner to detect cyber security events.

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

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.

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



Following the identification of a cyber security incident, the cyber security incident response plan is enacted. **Regular backups** Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements. Backups of data, applications and settings are synchronised to enable restoration to a common point in time. Backups of data, applications and settings are retained in a secure and resilient manner. Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises. Unprivileged user accounts cannot access backups belonging to other user accounts. Unprivileged user accounts cannot access their own backups. Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts. Privileged user accounts (excluding backup administrator accounts) cannot access their own backups. Unprivileged accounts are prevented from modifying and deleting backups. Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups. Backup administrator accounts are prevented from modifying and deleting backups during their retention period.

# Appendix D: Comparison of maturity levels

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	An automated method support the detection activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	A vulnerability scanne vulnerability scanne
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.	A vulnerability scanne updates for vulnerabil
	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.	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.	A vulnerability scanne updates for vulnerabil their extensions, emai
	_	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.	A vulnerability scanne or updates for vulnera suites, web browsers a security products.
	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.	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.	Patches, updates or of services are applied w assessed as critical by
	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.	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.	Patches, updates or or services are applied w assessed as non-critication of the services are applied.
	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.	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.	
	_	_	Patches, updates or o productivity suites, w software, and security when vulnerabilities a exploits exist.
	_	_	Patches, updates or o productivity suites, w software, and security when vulnerabilities a

when vulnerabilitie exploits exist.



nod of asset discovery is used at least fortnightly to on of assets for subsequent vulnerability scanning

ner with an up-to-date vulnerability database is used for ng activities.

ner is used at least daily to identify missing patches or bilities in online services.

ner is used at least weekly to identify missing patches or bilities in office productivity suites, web browsers and nail clients, PDF software, and security products.

ner is used at least fortnightly to identify missing patches erabilities in applications other than office productivity rs and their extensions, email clients, PDF software, and

other vendor mitigations for vulnerabilities in online within 48 hours of release when vulnerabilities are by vendors or when working exploits exist.

other vendor mitigations for vulnerabilities in online within two weeks of release when vulnerabilities are ical by vendors and no working exploits exist.

r other vendor mitigations for vulnerabilities in office web browsers and their extensions, email clients, PDF rity products are applied within 48 hours of release as are assessed as critical by vendors or when working

r other vendor mitigations for vulnerabilities in office web browsers and their extensions, email clients, PDF rity products are applied within two weeks of release as are assessed as non-critical by vendors and no working

	_	Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.	Patches, updates or ot applications other thar extensions, email clien within one month of re
	Online services that are no longer supported by vendors are removed.	Online services that are no longer supported by vendors are removed.	Online services that are
	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.	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.	Office productivity suit PDF software, Adobe F supported by vendors
	_	_	Applications other tha extensions, email clier products that are no lo
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.	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	An automated method support the detection of activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	A vulnerability scanner vulnerability scanning a
	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.	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.	A vulnerability scanner updates for vulnerabili and internet-facing net
	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.	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.	A vulnerability scanner or updates for vulneral internet-facing servers
	_	_	A vulnerability scanne patches or updates for
	_	_	A vulnerability scanne patches or updates for
	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.	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.	Patches, updates or ot systems of internet-fac applied within 48 hour critical by vendors or w
	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.	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.	Patches, updates or otl systems of internet-fac applied within two wee non-critical by vendors
	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.	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.	



other vendor mitigations for vulnerabilities in han office productivity suites, web browsers and their ents, PDF software, and security products are applied f release.

are no longer supported by vendors are removed.

uites, web browsers and their extensions, email clients, e Flash Player, and security products that are no longer rs are removed.

than office productivity suites, web browsers and their ients, PDF software, Adobe Flash Player, and security o longer supported by vendors are removed.

od of asset discovery is used at least fortnightly to on of assets for subsequent vulnerability scanning

ner with an up-to-date vulnerability database is used for ng activities.

ner is used at least daily to identify missing patches or bilities in operating systems of internet-facing servers network devices.

ner is used at least fortnightly to identify missing patches erabilities in operating systems of workstations, noners and non-internet-facing network devices.

ner is used at least fortnightly to identify missing for vulnerabilities in drivers.

ner is used at least fortnightly to identify missing for vulnerabilities in firmware.

other vendor mitigations for vulnerabilities in operating facing servers and internet-facing network devices are ours of release when vulnerabilities are assessed as r when working exploits exist.

other vendor mitigations for vulnerabilities in operating facing servers and internet-facing network devices are weeks of release when vulnerabilities are assessed as ors and no working exploits exist.

\_

	_	_	Patches, updates or oth operating systems of wo internet-facing network when vulnerabilities are exploits exist.
	_	_	Patches, updates or oth operating systems of wo internet-facing network when vulnerabilities are exploits exist.
	_	_	Patches, updates or oth are applied within 48 hc critical by vendors or wh
	_	_	Patches, updates or oth are applied within one r as non-critical by vendo
	_	_	Patches, updates or oth are applied within 48 hc critical by vendors or wh
	_	_	Patches, updates or oth are applied within one r as non-critical by vendo
	_	_	The latest release, or the
	Operating systems that are no longer supported by vendors are replaced.	Operating systems that are no longer supported by vendors are replaced.	Operating systems that a
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.	Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.	Multi-factor authenticat organisation's online ser organisation's sensitive o
	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.	Multi-factor authenticati services that process, sto data.
	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.	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.	Multi-factor authenticati third-party online service organisation's non-sensi
	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.	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.	Multi-factor authenticati organisation's online cus their organisation's sens



ther vendor mitigations for vulnerabilities in workstations, non-internet-facing servers and nonork devices are applied within 48 hours of release are assessed as critical by vendors or when working

ther vendor mitigations for vulnerabilities in workstations, non-internet-facing servers and nonork devices are applied within one month of release are assessed as non-critical by vendors and no working

ther vendor mitigations for vulnerabilities in drivers hours of release when vulnerabilities are assessed as when working exploits exist.

ther vendor mitigations for vulnerabilities in drivers e month of release when vulnerabilities are assessed dors and no working exploits exist.

ther vendor mitigations for vulnerabilities in firmware hours of release when vulnerabilities are assessed as when working exploits exist.

ther vendor mitigations for vulnerabilities in firmware e month of release when vulnerabilities are assessed dors and no working exploits exist.

the previous release, of operating systems are used.

at are no longer supported by vendors are replaced.

ation is used to authenticate users to their services that process, store or communicate their e data.

ation is used to authenticate users to third-party online store or communicate their organisation's sensitive

ation (where available) is used to authenticate users to vices that process, store or communicate their nsitive data.

ation is used to authenticate users to their customer services that process, store or communicate nsitive customer data.

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.	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.	Multi-factor authentica customer services that sensitive customer data
Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.	Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.	Multi-factor authentica customer services that data.
_	Multi-factor authentication is used to authenticate privileged users of systems.	Multi-factor authentica systems.
_	Multi-factor authentication is used to authenticate unprivileged users of systems.	Multi-factor authentica systems.
_	_	Multi-factor authentica repositories.
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.	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.	Multi-factor authentica users know, or somethi know or are.
_	Multi-factor authentication used for authenticating users of online services is phishing-resistant.	Multi-factor authentica phishing-resistant.
_	Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.	
	_	Multi-factor authentica customer services is ph
_	Multi-factor authentication used for authenticating users of systems is phishing-resistant.	Multi-factor authentica phishing-resistant.
_	_	Multi-factor authentica repositories is phishing
_	Successful and unsuccessful multi-factor authentication events are centrally logged.	Successful and unsucce logged.
_	Event logs are protected from unauthorised modification and deletion.	Event logs are protected
_	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.	Event logs from interne detect cyber security ev
_	_	Event logs from non-in manner to detect cybe
_	_	Event logs from workst cyber security events.



ication is used to authenticate users to third-party online at process, store or communicate their organisation's ata.

ication is used to authenticate customers to online at process, store or communicate sensitive customer

cation is used to authenticate privileged users of

cation is used to authenticate unprivileged users of

ication is used to authenticate users of data

ication uses either: something users have and something thing users have that is unlocked by something users

cation used for authenticating users of online services is

ication used for authenticating customers of online phishing-resistant.

\_

ication used for authenticating users of systems is

ication used for authenticating users of data ing-resistant.

cessful multi-factor authentication events are centrally

ted from unauthorised modification and deletion.

net-facing servers are analysed in a timely manner to events.

internet-facing servers are analysed in a timely ber security events.

kstations are analysed in a timely manner to detect s.

	_	Cyber security events are analysed in a timely manner to identify cyber security incidents.	Cyber security events a security incidents.
	_	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.	Cyber security incidents Officer, or one of their o discovered.
	_	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.	Cyber security incidents occur or are discovered
	_	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.	Following the identificatincity incident response plan i
Restrict administrative privileges	Requests for privileged access to systems, applications and data repositories are validated when first requested.	Requests for privileged access to systems, applications and data repositories are validated when first requested.	Requests for privileged are validated when first
provides	_	Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated.	Privileged access to syst after 12 months unless
	_	Privileged access to systems and applications is disabled after 45 days of inactivity.	Privileged access to syst inactivity.
	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.	Privileged users are assi solely for duties requiri
	_	_	Privileged access to sys only what is required fo
	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.	Privileged user accounts online services) are pre- services.
	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.	Privileged user account strictly limited to only w their duties.
	_	_	Secure Admin Worksta activities.
	Privileged users use separate privileged and unprivileged operating environments.	Privileged users use separate privileged and unprivileged operating environments.	Privileged users use sep environments.
	_	Privileged operating environments are not virtualised within unprivileged operating environments.	Privileged operating environments
	Unprivileged user accounts cannot logon to privileged operating environments.	Unprivileged user accounts cannot logon to privileged operating environments.	Unprivileged user accou environments.



#### s are analysed in a timely manner to identify cyber

nts are reported to the Chief Information Security ir delegates, as soon as possible after they occur or are

nts are reported to ASD as soon as possible after they ed.

ication of a cyber security incident, the cyber security an is enacted.

ed access to systems, applications and data repositories irst requested.

ystems, applications and data repositories is disabled ss revalidated.

ystems and applications is disabled after 45 days of

ssigned a dedicated privileged user account to be used iring privileged access.

systems, applications and data repositories is limited to d for users and services to undertake their duties.

nts (excluding those explicitly authorised to access prevented from accessing the internet, email and web

ints explicitly authorised to access online services are y what is required for users and services to undertake

#### stations are used in the performance of administrative

separate privileged and unprivileged operating

environments are not virtualised within unprivileged ents.

counts cannot logon to privileged operating

Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Privileged user account logon to unprivileged o
_	_	Just-in-time administra applications.
_	Administrative activities are conducted through jump servers.	Administrative activitie
_	Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.	Credentials for break g accounts are long, uniq
_	_	Memory integrity func
_	_	Local Security Authorit
_	_	Credential Guard funct
_	_	Remote Credential Gu
_	Privileged access events are centrally logged.	Privileged access event
_	Privileged user account and security group management events are centrally logged.	Privileged user account logged.
_	Event logs are protected from unauthorised modification and deletion.	Event logs are protecte
_	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.	Event logs from interne detect cyber security e
_	_	Event logs from non-in manner to detect cybe
_	_	Event logs from works cyber security events.
_	Cyber security events are analysed in a timely manner to identify cyber security incidents.	Cyber security events a security incidents.
_	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.	Cyber security incident Officer, or one of their discovered.
_	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.	Cyber security incident occur or are discovered
_	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.	Following the identifica incident response plan



unts (excluding local administrator accounts) cannot doperating environments.

tration is used for administering systems and

ties are conducted through jump servers.

glass accounts, local administrator accounts and service nique, unpredictable and managed.

nctionality is enabled.

rity protection functionality is enabled.

nctionality is enabled.

Guard functionality is enabled.

ents are centrally logged.

unt and security group management events are centrally

cted from unauthorised modification and deletion.

rnet-facing servers are analysed in a timely manner to y events.

-internet-facing servers are analysed in a timely /ber security events.

rkstations are analysed in a timely manner to detect ts.

s are analysed in a timely manner to identify cyber

ents are reported to the Chief Information Security eir delegates, as soon as possible after they occur or are

ents are reported to ASD as soon as possible after they red.

fication of a cyber security incident, the cyber security an is enacted.

Application control	Application control is implemented on workstations.	Application control is implemented on workstations.	Application control is i
	_	Application control is implemented on internet-facing servers.	Application control is i
	_	_	Application control is
	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.	Application control is a operating systems, we
	_	Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.	Application control is a temporary folders use clients.
	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.	Application control res scripts, installers, com applets to an organisa
	_	_	Application control re approved set.
	_	Microsoft's recommended application blocklist is implemented.	Microsoft's recommer
	_	_	Microsoft's vulnerable
	_	Application control rulesets are validated on an annual or more frequent basis.	Application control rul basis.
	_	Allowed and blocked application control events are centrally logged.	Allowed and blocked a
	_	Event logs are protected from unauthorised modification and deletion.	Event logs are protected
	_	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.	Event logs from intern detect cyber security e
	_	_	Event logs from non-in manner to detect cybe
	_	_	Event logs from works cyber security events.
	_	Cyber security events are analysed in a timely manner to identify cyber security incidents.	Cyber security events a security incidents.
	_	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.	Cyber security inciden Officer, or one of their discovered.
	_	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.	Cyber security incident occur or are discovere



is implemented on workstations.

is implemented on internet-facing servers.

#### is implemented on non-internet-facing servers.

is applied to user profiles and temporary folders used by web browsers and email clients.

is applied to all locations other than user profiles and used by operating systems, web browsers and email

restricts the execution of executables, software libraries, ompiled HTML, HTML applications and control panel isation-approved set.

restricts the execution of drivers to an organisation-

nended application blocklist is implemented.

ble driver blocklist is implemented.

rulesets are validated on an annual or more frequent

ed application control events are centrally logged.

ected from unauthorised modification and deletion.

ernet-facing servers are analysed in a timely manner to by events.

n-internet-facing servers are analysed in a timely yber security events.

rkstations are analysed in a timely manner to detect ts.

ts are analysed in a timely manner to identify cyber

ents are reported to the Chief Information Security eir delegates, as soon as possible after they occur or are

lents are reported to ASD as soon as possible after they ered.

	_	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.	Following the identification incident response plan
Restrict Microsoft Office macros	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	Microsoft Office macro demonstrated busines
	_	_	Only Microsoft Office environment, a Truste publisher are allowed
	_	_	Microsoft Office macro code before being digi
	_	_	Only privileged users are free of malicious c Locations.
	_	_	Microsoft Office macro be enabled via the Me
	_	_	Microsoft Office macro signatures cannot be e
	_	_	Microsoft Office's list more frequent basis.
	Microsoft Office macros in files originating from the internet are blocked.	Microsoft Office macros in files originating from the internet are blocked.	Microsoft Office macro
	Microsoft Office macro antivirus scanning is enabled.	Microsoft Office macro antivirus scanning is enabled.	Microsoft Office macro
	_	Microsoft Office macros are blocked from making Win32 API calls.	Microsoft Office macro
	Microsoft Office macro security settings cannot be changed by users.	Microsoft Office macro security settings cannot be changed by users.	Microsoft Office macro
User application hardening	Internet Explorer 11 is disabled or removed.	Internet Explorer 11 is disabled or removed.	Internet Explorer 11 is
hardening	Web browsers do not process Java from the internet.	Web browsers do not process Java from the internet.	Web browsers do not
	Web browsers do not process web advertisements from the internet.	Web browsers do not process web advertisements from the internet.	Web browsers do not
	_	Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	Web browsers are hard the most restrictive gu
	Web browser security settings cannot be changed by users.	Web browser security settings cannot be changed by users.	Web browser security
	_	Microsoft Office is blocked from creating child processes.	Microsoft Office is bloc
	_	Microsoft Office is blocked from creating executable content.	Microsoft Office is bloc



fication of a cyber security incident, the cyber security lan is enacted.

cros are disabled for users that do not have a less requirement.

ce macros running from within a sandboxed sted Location or that are digitally signed by a trusted ed to execute.

cros are checked to ensure they are free of malicious ligitally signed or placed within Trusted Locations.

rs responsible for checking that Microsoft Office macros s code can write to and modify content within Trusted

cros digitally signed by an untrusted publisher cannot Message Bar or Backstage View.

acros digitally signed by signatures other than V3 be enabled via the Message Bar or Backstage View.

st of trusted publishers is validated on an annual or

cros in files originating from the internet are blocked.

cro antivirus scanning is enabled.

cros are blocked from making Win32 API calls.

cro security settings cannot be changed by users.

is disabled or removed.

ot process Java from the internet.

ot process web advertisements from the internet.

ardened using ASD and vendor hardening guidance, with guidance taking precedence when conflicts occur.

ty settings cannot be changed by users.

locked from creating child processes.

locked from creating executable content.

_	Microsoft Office is blocked from injecting code into other processes.	Microsoft Office is bloc
_	Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.	Microsoft Office is conf Embedding packages.
_	Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	Office productivity suit guidance, with the mos conflicts occur.
_	Office productivity suite security settings cannot be changed by users.	Office productivity suit
_	PDF software is blocked from creating child processes.	PDF software is blocked
_	PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	PDF software is harden the most restrictive gui
_	PDF software security settings cannot be changed by users.	PDF software security s
_	_	.NET Framework 3.5 (in
_	_	Windows PowerShell 2
_	_	PowerShell is configur
_	PowerShell module logging, script block logging and transcription events are centrally logged.	PowerShell module log centrally logged.
	Command line process creation events are centrally logged.	Command line process
_	Event logs are protected from unauthorised modification and deletion.	Event logs are protecte
_	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.	Event logs from interne detect cyber security e
_	_	Event logs from non-in manner to detect cybe
_	_	Event logs from works cyber security events.
_	Cyber security events are analysed in a timely manner to identify cyber security incidents.	Cyber security events a security incidents.
_	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.	Cyber security incident Officer, or one of their discovered.



ocked from injecting code into other processes.

nfigured to prevent activation of Object Linking and

uites are hardened using ASD and vendor hardening nost restrictive guidance taking precedence when

uite security settings cannot be changed by users.

ked from creating child processes.

ened using ASD and vendor hardening guidance, with guidance taking precedence when conflicts occur.

y settings cannot be changed by users.

(includes .NET 2.0 and 3.0) is disabled or removed.

I 2.0 is disabled or removed.

ured to use Constrained Language Mode.

ogging, script block logging and transcription events are

ss creation events are centrally logged.

ted from unauthorised modification and deletion.

net-facing servers are analysed in a timely manner to events.

internet-facing servers are analysed in a timely ber security events.

kstations are analysed in a timely manner to detect s.

s are analysed in a timely manner to identify cyber

nts are reported to the Chief Information Security ir delegates, as soon as possible after they occur or are

	_	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.	Cyber security inciden occur or are discovere
	_	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.	Following the identific incident response plar
accordance with business criticality and l Backups of data, applications and setting restoration to a common point in time. Backups of data, applications and setting resilient manner. Restoration of data, applications and set point in time is tested as part of disaster Unprivileged user accounts cannot acces accounts.	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.	Backups of data, applie accordance with busin
	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.	Backups of data, applic restoration to a comm
	Backups of data, applications and settings are retained in a secure and resilient manner.	Backups of data, applications and settings are retained in a secure and resilient manner.	Backups of data, applic resilient manner.
	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.	Restoration of data, a point in time is tested
	Unprivileged user accounts cannot access backups belonging to other user accounts.	Unprivileged user accounts cannot access backups belonging to other user accounts.	Unprivileged user acco accounts.
	_	_	Unprivileged user acc
	_	Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts.	Privileged user accoun access backups belong
	_	_	Privileged user accour access their own back
	Unprivileged user accounts are prevented from modifying and deleting backups.	Unprivileged user accounts are prevented from modifying and deleting backups.	Unprivileged user acco backups.
	_	Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.	Privileged user accour prevented from modif
	_	_	Backup administrator



ents are reported to ASD as soon as possible after they red.

fication of a cyber security incident, the cyber security lan is enacted.

plications and settings are performed and retained in siness criticality and business continuity requirements.

plications and settings are synchronised to enable nmon point in time.

olications and settings are retained in a secure and

applications and settings from backups to a common ed as part of disaster recovery exercises.

ccounts cannot access backups belonging to other user

#### ccounts cannot access their own backups.

unts (excluding backup administrator accounts) cannot nging to other user accounts.

ounts (excluding backup administrator accounts) cannot ackups.

ccounts are prevented from modifying and deleting

unts (excluding backup administrator accounts) are difying and deleting backups.

or accounts are prevented from modifying and deleting ir retention period.

#### Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

#### Copyright

© Commonwealth of Australia 2023.

With the exception of the Coat of Arms, the Australian Signals Directorate logo and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

#### Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/government/commonwealth-coat-arms).

### For more information, or to report a cyber security incident, contact us:

### cyber.gov.au | 1300 CYBER1 (1300 292 371)



**Australian Government** 

**Australian Signals Directorate**