Australian Government
Attorney-General's Department

Protective Security Policy Framework

10 Safeguarding information from cyber threats

A. Purpose

1. This policy describes how entities can mitigate common and emerging cyber threats. Cyber threats faced by the Australian Government commonly include:

   a. external adversaries who steal data

   b. ransomware that denies access to data, and external adversaries who destroy data and prevent systems from functioning

   c. malicious insiders who steal data

   d. malicious insiders who destroy data and prevent systems from functioning.

2. The most common cyber threat facing entities is external adversaries who attempt to steal data. Often these adversaries want access to systems and information through email and web pages. It is critical that entities safeguard the information held on systems that can receive emails or browse internet content.

3. The Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) provides expert guidance to help entities mitigate cyber threats. While no single mitigation strategy is guaranteed to prevent a cyber security incident, the ACSC estimates many cyber threats could be mitigated by whitelisting applications, patching applications and operating systems, and restricting administrative privileges. These four mandatory strategies form part of the Essential Eight mitigation strategies. The Essential Eight represents the best advice on the measures entity can implement to mitigate cyber threats. Considered the baseline for cyber resilience, entities are strongly recommended to implement the Essential Eight mitigation strategies.

B. Requirements

B.1 Core requirement

Each entity must mitigate common and emerging cyber threats by:

a. implementing the following Australian Signals Directorate (ASD) Strategies to Mitigate Cyber Security Incidents:

i. application whitelisting

ii. patching applications

iii. restricting administrative privileges, and

iv. patching operating systems;

b. considering which of the remaining Strategies to Mitigate Cyber Security Incidents you need to implement to protect your entity.

B.2 Supporting requirements

4. Supporting requirements help to safeguard information from cyber threats when engaging with members of the public online.

Supporting requirements for safeguarding information from cyber threats

#	Supporting requirements
Requirement 1. Transacting online with the public	Entities **must** not expose the public to unnecessary cyber security risks when they transact online with government.

C. Guidance

5. When implementing a mitigation strategy, first implement it for workstations of high-risk users and for internet-connected systems before implementing more broadly.

C.1 Achieving PSPF maturity with ASD mitigation strategies

6. To achieve a PSPF maturity rating of **Managing** for each of the four Strategies to Mitigate Cyber Security Incidents, implement the maturity level three requirements as set out in the ACSC's Essential Eight Maturity Model.

7. The Essential Eight to ISM document provides a mapping between the maturity level three of the Essential Eight Maturity Model and the security controls in the Australian Government Information Security Manual. This mapping represents the minimum security controls required to meet the intent of the Essential Eight.

C.1.1 Application whitelisting

8. Malicious code (malware) often aims to exploit security vulnerabilities in existing applications and does not need to be installed on the workstation to be successful. Application whitelisting is effective in addressing instances of malicious code.

9. Application whitelisting ensures that only authorised applications (eg programs, software libraries, scripts and installers) can be executed. As such, application whitelisting prevents malicious software and unapproved programs from running. Through application whitelisting, an entity can protect its systems by:

   a. identifying authorised applications

   b. developing rules to ensure only authorised applications can execute

   c. maintaining whitelisting rules using a change-management program.

10. It is important that users and system administrators cannot temporarily or permanently disable, bypass or be exempt from application whitelisting mechanisms (except when conducting authorised administrative activities). This maintains the integrity of application whitelisting as a security treatment.

11. For further guidance on application whitelisting, see ACSC:

   a. Implementing Application Whitelisting

   b. Australian Government Information Security Manual.

C.1.2 Patching vulnerabilities in applications and operating systems

12. A patch is a piece of software designed to fix problems or update an application or operating system. This includes fixing security vulnerabilities and other program deficiencies as well as improving the usability or performance of the software.

13. Applying patches to operating systems, applications, drivers, ICT equipment and mobile devices is a critical activity for systems security:

   a. Patching applications helps to prevent the delivery and execution of malicious code (malware).

   b. Patching operating systems helps to limit the extent of cyber security incidents. For example, applying fixes to known security flaws means systems are protected from compromise. If the operating system is compromised, any action or information handled by that computer is at risk.

14. Patches for security vulnerabilities come in many forms. These include:

   a. fixes that can be applied to pre-existing application versions

   b. fixes incorporated into new applications or drivers that require replacing pre-existing versions

c. fixes that require overwriting of the firmware on ICT equipment.

15. Patches for high assurance ICT equipment (ICT equipment that has been approved for the protection of information classified SECRET or above) is assessed by the ACSC, and where required the ACSC will issue advice on the timeframe in which the patch is to be deployed or amend the Australian Government Information Security Manual.

16. For guidance on patching applications and systems, see ACSC:

    a. Assessing security vulnerabilities and applying patches – provides guidance on conducting a risk assessment to assess the severity of security vulnerabilities and examples of risk level outcomes (extreme risk, high risk, moderate risk and low risk vulnerabilities)

    b. Australian Government Information Security Manual.

17. The Attorney-General's Department recommends that entities :

    a. monitor relevant sources for information about new security vulnerabilities and associated patches for operating systems and applications. Patching drives and firmware for ICT equipment is also encouraged

    b. implement a centralised and managed approach to patch operating systems and applications (where possible)

    c. confirm that patches have been installed, applied successfully and remain in place.

18. Managing application patches can be significantly more challenging than operating system patching. The Attorney-General's Department recommends that entities use the latest release of key business applications as newer applications have better security functionality built it. Applications include:

    a. office productivity suites (eg Microsoft Office)

    b. PDF readers (eg Adobe Reader)

    c. web browsers (eg Microsoft Internet Explorer, Mozilla Firefox or Google Chrome)

    d. common web browser plugins (eg Adobe Flash)

    e. email clients (eg Microsoft outlook)

    f. software platforms (eg Oracle Java Platform and Microsoft .NET Framework).

C.1.2.1 Unsupported systems and when patches not available

19. Patches may not be available for older versions of operating systems, especially those no longer supported by vendors. Using unsupported systems exposes entities to security vulnerabilities. New versions of operating systems, applications and hardware often introduce improvements in security functionality over previous versions. This can make it difficult for an adversary to exploit security vulnerabilities they discover.

20. If there are no patches available from vendors for a security vulnerability, temporary workarounds may provide an effective protection. These workarounds may be published in conjunction with, or soon after, security vulnerability announcements. Temporary workarounds may include disabling the vulnerable functionality within the operating system, application or device or restricting or blocking access to the vulnerable service using firewalls or other access controls. The decision to implement a temporary workaround is risk-based. For guidance on how to manage a security vulnerability when patches are not available, see the system patching guidance in the Australian Government Information Security Manual.

21. When a patch is not available for a security vulnerability, it is recommended that entities reduce access to the vulnerability through alternative means by:

    a. disabling the functionality associated with the vulnerability

    b. asking the vendor for an alternative method of managing the vulnerability

    c. moving to a different product with a responsive vendor

    d. engaging a software developer to resolve the vulnerability.

22. If a patch is not available for an application or system that may expose government to high risk, contact ACSC for advice.

C.1.3 Restricting administrative privileges

23. User accounts with administrative privileges are an attractive target for adversaries because they have a high level of access to the entity's systems. Minimising administrative privileges makes it difficult for an adversary to spread or hide their existence.

24. Privileged accounts that cannot access emails or open attachments, cannot browse the internet or obtain files via internet services such as instant messaging or social media, minimises opportunities for these accounts to be compromised.

25. The PSPF policy: Access to information provides guidance on managing access to information systems. These include unique user identification, user authentication and authorisation practices. The Australian Government Information Security Manual provides technical guidance on using multi-factor authentication to assure a privileged account user's identity. Implementing the identified security controls will lower the risk of user accounts being compromised.

26. For further guidance on administrative privileges, see ACSC:

    a. Restricting administrative privileges

    b. Australian Government Information Security Manual.

C.2 The Essential Eight and other strategies to mitigate cyber security incidents

27. The Attorney-General's Department strongly recommends entities implement the ACSC Essential Eight strategies to mitigate cyber threats. These strategies incorporate the four mitigation strategies mandated by this policy (see section B) as well as four additional strategies that effectively mitigate common and emerging cyber threats. The additional four are:

    a. configuring Microsoft Office macro settings

    b. user application hardening

    c. multi-factor authentication

    d. daily backups.

28. Entities are encouraged to implement the remaining Strategies to Mitigate Cyber Security Incidents, where relevant to their operational and risk environment. A list of the ACSC strategies is at **Annex A**.

C.3 Cyber security responsibilities when transacting online with the public

29. Demand for online government services continues to grow, as does the scale, sophistication and perpetration of cybercrime and activities by either malicious or benign actors.

30. **Table 1** provides examples of potential threats to the public when transacting online with government.

Table 1 Potential threat sources when transacting online with Australian Government entities

Potential threat sources when transacting online with Australian Government entities
An attacker masquerades as a legitimate entity website to compromise a public user's internet-connected device, steal their identity, or scam them into providing personal details (such as credit card information).
An entity website is compromised and used to host malicious software which subsequently compromises an internet-connected device used by the public when they access the website.
An entity website is compromised and used to redirect the public to another malicious website that subsequently compromises their internet-connected device.
A compromised entity website could result in public username or password details being stolen, and an attacker masquerading as the user to claim government or other financial benefits.
The compromised account details of public users could lead to the compromise of other websites, as public users may use the same details for multiple government online accounts.
The compromise of an internet-connected device used by the public could result in: a. their addition to a botnet to participate in illegal activities b. theft of details for fraud or identity theft purposes c. blackmail of the user (where attackers encrypt hard drives and demand money for a decryption key) d. corruption of the internet-connected device and loss of user information.

31. The Attorney-General's Department recommends entities evaluate the threat scenarios identified in **Table 1** and adopt applicable security actions for online services as outlined in **Table 2**. These activities will avoid exposing the public to cyber security risks when they transact online with government.

Table 2 Suggested actions to reduce the risk of harm to the public when transacting online with Australian Government entities

Suggested actions to reduce the risk of harm to the public when transacting online with Australian Government entities
Where online transaction accounts are in use, ensure: a. users accept account terms and conditions prior to establishing an account as well as when terms and conditions change b. there is a warning that explains (simply): i. the specific risks associated with use of the online service ii. who may, or may not, use the service and under what circumstances iii. provide details of alternative channels for service or support. c. a link to an entity's privacy policy page is provided for further information to public users on the conditions of acceptance d. transaction processes that put the user at risk of unnecessary harm are not implemented.
When public users elect to download non-public information from an entity website, ensure: a. an appropriate pre-download warning be in place, identifying the potential risk that they are 'about to download information across an unsecured connection' b. warning options 'proceed', 'cancel' or '?' are provided c. links to additional information on associated risks is provided.
Ensure that Australian Government websites: a. contain statements including a 'security notice' and a 'disclaimer notice' (use www.australia.gov.au website as a template for these notices, in consultation with the entity's legal area. For example, advising the public to report suspicious or unauthorised activity related to an online transaction to the responsible entity).
Patches for online services (including maintaining information-only web pages) and web servers be actioned as a priority by the entity's IT support. Delays in patching may create cyber security vulnerabilities for public users: a. online transactions that transfer personal details to government require a secure connection (only collect information needed for the delivery of a service) b. for entities using social networking services to interact with the public, ensure they: **i. carefully evaluate privacy and security implications when collecting/retaining personal information as part of a service** ii. monitor social networks for malicious hyperlinks embedded in posts where not directly moderated by the entity before publishing.
Where appropriate and reasonable, entities may offer or impose: a. higher level security credentials (eg one-time passwords, digital certificates or tokens) or policy, to help users select a secure password b. restrictions or warnings about browser versions known to have security weaknesses, are out of date and/or unsupported c. a display of the previous login details at user login (entities implementing a high value or high risk transaction may consider notifying the user of access on their account with details of the Internet Protocol (IP) address) d. a message of what personal information an entity will never require users to disclose over email (eg that they would not require users to provide sensitive personal information such as login credentials). Entities may provide advice or links to cyber security and cyber safety information e. an alert to users when they are redirected to an external website.
Indications of a security compromise can be detected by: a. analysing patterns of online user interactions for unusual activity b. fingerprinting user access to detect anomalous access vectors c. performing a code audit of web application used on the entity's website to detect security vulnerabilities.

D. Find out more

32. Other legislation and policies include:

a. the Australian Government Information Security Manual

b. Strategies to Mitigate Cyber Security Incidents

c. the Australian Cyber Security Centre (ACSC)supporting publications and advice.

D.1 Change log

Table 3 Amendments in this policy

Version	Date	Section	Amendment
v2018.1	Sep 2018	Throughout	Not applicable. This is the first issue of this policy
V2018.2	Oct 2019	Throughout	Amendments of core and supporting requirements and guidance to recalibrate alignment with ACSC’s technical advice.

Annex A. ACSC strategies to mitigate cyber incidents[1]

33. The Australian Signals Directorate (ASD) has developed prioritised strategies to help mitigate cyber threats, including advice on the suggested implementation order depending on the threats that most concern your entity. For further guidance see ACSC publications: Strategies to Mitigate Cyber Security Incidents and Strategies to Mitigate Cyber Security Incidents Mitigation Details.

Annex A Table 1 Strategies to mitigate cyber incidents – Mitigation strategies to prevent malware delivery and execution

Relative security effectiveness rating	Mitigation strategy
Essential (mandatory)	**Application whitelisting** of approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (eg Windows Script Host, PowerShell and HTA) and installers.
Essential (mandatory)	**Patch applications** eg Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with extreme risk vulnerabilities within 48 hours. Use the latest version of applications.
Essential (strongly recommended)	**Configure Microsoft Office macro settings** to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
Essential (strongly recommended)	**User application hardening**. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (eg OLE), web browsers and PDF viewers.
Excellent	**Automated dynamic analysis of email and web content run in a sandbox**, blocked if suspicious behaviour is identified (eg network traffic, new or modified files, or other system configuration changes).
Excellent	**Email content filtering**. Whitelist allowed attachment types (including in archives and nested archives). Analyse and sanitise hyperlinks, PDF and Microsoft Office attachments. Quarantine Microsoft Office macros.
Excellent	**Web content filtering**. Whitelist allowed types of web content and websites with good reputation ratings. Block access to malicious domains and IP addresses, ads, anonymity networks and free domains.
Excellent	**Deny corporate computers direct internet connectivity**. Use a gateway firewall to require use of a split DNS server, an email server and an authenticated web proxy server for outbound web connections.
Excellent	**Operating system generic exploit mitigation** eg Data Execution Prevention (DEP), Address Space Layout Randomisation (ASLR) and Enhanced Mitigation Experience Toolkit (EMET).
Very good	**Server application hardening** especially internet accessible web applications (sanitise input and use TLS not SSL) and databases, as well as applications that access important (sensitive or high availability) data.
Very good	**Operating system hardening** (including for network devices) based on a Standard Operating Environment, disabling unneeded functionality (eg RDP, AutoRun, LanMan, SMB/NetBIOS, LLMNR and WPAD).
Very good	**Antivirus software using heuristics and reputation ratings** to check a file's prevalence and digital signature prior to execution. Use antivirus software from different vendors for gateways versus computers.
Very good	**Control removable storage media and connected devices**. Block unapproved CD, DVD, USB storage media. Block connectivity with unapproved smartphones, tablets and Bluetooth, Wi-Fi, 3G, 4G devices.
Very good	**Block spoofed emails**. Use Sender Policy Framework (SPF) or Sender ID to check incoming emails. Use 'hard fail' SPF TXT and DMARC DNS records to mitigate emails that spoof the entity's domain.
Good	**User education**. Avoid phishing emails (eg with links to login to fake websites), weak passphrases, passphrase reuse, as well as unapproved: removable storage media, connected devices and cloud services.
Limited	**Antivirus software with up-to-date signatures** to identify malware, from a vendor that rapidly adds signatures for new malware. Use antivirus software from different vendors for gateways versus computers.
Limited	**TLS encryption between email servers** to help prevent legitimate emails being intercepted and subsequently leveraged for social engineering. Perform content scanning after email traffic is decrypted.

[1] As these tables are based on best advice from ASD, they will periodically be updated to reflect any changes in ASD guidance.

Annex A Table 2 Strategies to Mitigate Cyber Incidents – Mitigation strategies to limit the extent of cyber security incidents

Relative security effectiveness rating	Mitigation strategy
Essential (mandatory)	**Restrict administrative privileges** to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.
Essential (mandatory)	**Patch operating systems.** Patch/mitigate computers (including network devices) with extreme risk vulnerabilities within 48 hours. Use the latest operating system version. Do not use unsupported versions.
Essential (strongly recommended)	**Multi-factor authentication** including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive or high availability) data repository.
Excellent	**Disable local administrator accounts** or assign passphrases that are random and unique for each computer's local administrator account to prevent propagation using shared local administrator credentials.
Excellent	**Network segmentation.** Deny network traffic between computers unless required. Constrain devices with low assurance (eg BYOD and IoT). Restrict access to network drives and data repositories based on user duties.
Excellent	**Protect authentication credentials.** Remove CPassword values (MS14-025). Configure WDigest (KB2871997). Use Credential Guard. Change default passphrases. Require long complex passphrases.
Very good	**Non-persistent virtualised sandboxed environment**. Deny access to important (sensitive or high availability) data, for risky activities (eg web browsing, and viewing untrusted Microsoft Office and PDF files).
Very good	**Software-based application firewall, blocking incoming network traffic.** Block traffic that is malicious or unauthorised, and deny network traffic by default (eg unneeded or unauthorised RDP and SMB/NetBIOS traffic).
Very good	**Software-based application firewall, blocking outgoing network traffic** Block traffic that is not generated by approved or trusted programs, and deny network traffic by default.
Very good	**Outbound web and email data loss prevention.** Block unapproved cloud computing services. Log recipient, size and frequency of outbound emails. Block and log emails with sensitive words or data patterns.

Annex A Table 3 Strategies to Mitigate Cyber Incidents – Mitigation strategies to detect cyber security incidents and respond

Relative security effectiveness rating	Mitigation strategy
Excellent	**Continuous incident detection and response** with automated immediate analysis of centralised time-synchronised logs of permitted and denied: computer events, authentication, file access and network activity.
Very good	**Host-based intrusion detection and prevention system** to identify anomalous behaviour during program execution (eg process injection, keystroke logging, driver loading and persistence).
Very good	**Endpoint detection and response software** on all computers to centrally log system behaviour and facilitate incident response. Microsoft's free SysMon tool is an entry-level option.
Very good	**Hunt to discover incidents** based on knowledge of adversary tradecraft. Leverage threat intelligence consisting of analysed threat data with context enabling mitigating action, not just indicators of compromise.
Limited	**Network-based intrusion detection and prevention system** using signatures and heuristics to identify anomalous traffic both internally and crossing network perimeter boundaries.
Limited	**Capture network traffic** to and from corporate computers storing important data or considered as critical assets, and network traffic traversing the network perimeter, to perform incident detection and analysis.

Annex A Table 4 Strategies to Mitigate Cyber Incidents – Mitigation strategies to recover data and system availability

Relative security effectiveness rating	Mitigation strategy
Essential (strongly recommended)	**Daily backups** of important new or changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.
Very good	**Business continuity and disaster recovery plans** which are tested, documented and printed in hardcopy with a softcopy stored offline. Focus on the highest priority systems and data to recover.
Very good	**System recovery capabilities** eg virtualisation with snapshot backups, remotely installing operating systems and applications on computers, approved enterprise mobility, and onsite vendor support contracts.

Annex A Table 5 Strategies to Mitigate Cyber Incidents – Mitigation strategy specific to preventing malicious insiders

Relative security effectiveness rating	Mitigation strategy
Very good	**Personnel management** eg ongoing vetting especially for users with privileged access, immediately disable all accounts of departing users, and remind users of their security obligations and penalties.