GOVERNMENT OF
WESTERN AUSTRALIA

Western Australian Government Cyber Security Policy

2026

Contents

Introduction 4

Purpose 5

Alignment 6

Scope 9

Roles and responsibilities 10

Accountable Authority 10

Government Chief Information Officer (GCIO) 10

Cyber Security Unit (CSU), led by the Chief Information Security Officer (CISO) 11

1. Govern 12

1.1 Accountable Authority 12

1.2 Cyber Security Executive 12

1.3 Cyber Security Operations 13

1.4 Cyber Security Governance 13

1.5 Annual Implementation Reporting 14

1.6 OAG Management Letters 14

2. Identify 15

2.1 Cyber Security Context 15

2.2 Cyber Security Risk Management 16

3. Protect 17

3.1 The Essential Controls 17

3.2 Cyber Security Training 21

3.3 Enterprise Mobility 21

3.4 Secure Procurement and Supply Chain Risk Management 22

3.5 Data Offshoring 23

3.6 Secure Data Removal and Device Disposal 23

3.7 Vulnerability Management Program 24

3.8 Identity and Access Management 24

3.9 Physical Security of Assets 24

3.10 Personnel Security 25
3.11 Encryption 25
3.12 Post-Quantum Cryptographic (PQC) Standards 26
3.13 Secure Development of Applications and Software 26
3.14 Artificial Intelligence Security 26
3.15 Security of Operational Technology (OT) and Industrial Control Systems (ICS) 28
3.16 Security of Internet of Things (IoT) Devices 29
3.17 Cyber Security Insurance 29
3.18 Whole-of-Government Cyber Security Advice and Direction 29

4. Detect 30
4.1 Continuous Monitoring 30
4.2 Adverse Event Analysis 31

5. Respond 32
5.1 Incident Reporting 32
5.2 Cyber Security Incident Management and Response Plan 32
5.3 Incident Response Playbooks 33
5.4 Cyber Security Exercises and Testing 33
5.5 Government Ransomware Position 33

6. Recover 34
6.1 Capability to Restore Services and Information 34
6.2 Response Lessons Learned 34

Annual Implementation Reporting 35

Exemptions 36

Review 36

Additional Resources 37
DGov Guidance Documents 37

Further information 43

Introduction

The WA Government Cyber Security Policy (this Policy) specifies the measures WA Government entities are required to undertake to manage their cyber security risks.

Cyber security is a term that refers to the measures used to protect digital information, information systems and assets from cyber threats and ensure their confidentiality, integrity and availability.

While cyber security risks can never be eliminated, a comprehensive and systematic approach to cyber security assists the State Government in reducing the level of cyber security risk to its operations and information.

WA Government entities rely on technology to manage valuable information and infrastructure, provide public services and ensure business continuity. However, while the cyber sphere is a critical enabler of public service, it also acts as a vector through which malicious actors can cause harm. Due to technological advancement, increased connectivity and geopolitical volatility, cyber threats are increasing in frequency, scale and sophistication. Cyber-criminals and hostile state actors are continually looking for vulnerabilities in electronic systems and networks and adopting new technologies including Artificial Intelligence (AI) which are enabling them to execute faster large-scale attacks.[1]

Information loss and service disruption can result in financial loss, reputational harm and loss of trust from citizens in using Government digital services. The Policy is designed to mitigate these threats by outlining a structured process to prevent, respond to and recover from cyber security incidents. Many incidents reported each year within the WA Government and across Australia could have been prevented or mitigated by implementing good cyber security practices.

1 Australian Signals Directorate (ASD) Annual Cyber Threat Report 2024-2025

Purpose

The purpose of this Policy is to outline mandatory measures that WA Government entities are required to undertake to manage their cyber security risks. Specifically, the Policy:

- Prescribes the cyber security measures required to govern cyber security activities, identify risks, protect from, detect and respond to threats, recover from cyber security incidents and restore business operations
- Prescribes the establishment and maintenance of key cyber security controls at specific application levels [2]
- Provides a roadmap for WA government to implement Zero Trust principles and Post Quantum Cryptography capability [3]
- Promotes best practice for managing risks of procurement, Operational Technology and Artificial Intelligence
- Identifies the procedure for reporting incidents to the Office of Digital Government.

2 The key controls comprise ACSC Essential Eight controls at Maturity Level 2 and five additional controls from ACSC Strategies for Mitigating Incidents, prioritised by DGov for WA threat landscape.

3 Zero Trust is a security model that assumes no implicit trust and verifies every point of access to government owned information and systems.

Alignment

The Policy mandate is supported by the Cyber Security Measures for WA Government Entities – Premier's Circular 2025/13 and is intended to supersede the current WA Government Cyber Security Policy 2024.

WA Government entities captured under the Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act) can use this Policy as an equivalent framework for the purpose of reporting on their cyber and information security hazards to the Department of Home Affairs (DHA) as per section 8 (5) under Security of Critical Infrastructure Risk Management Program Rules (CIRMP) (LIN23/006).[4]
The Policy is strategically aligned with:

- The Digital Strategy for the Western Australian Government, which guides secure digital transformation across Western Australia
- WA Government Cyber Security Incident Coordination Framework (WA CSICF), which sets out a structured process for cyber security incident management and response in WA Government
- Limited Use Obligations under the *Cyber Security Act 2024* (Cth)
- WA Information Classification Policy
- Protective Security Policy Framework (PSPF) Directions
- Enhanced Critical Infrastructure Risk Management Program (CIRMP)
- "The big four" 2025 Australian Signals Directorate recommendations[5]
- *Privacy and Responsible Information Sharing Act 2024 (WA).*

4 The agreement to consider the Policy an equivalent framework was confirmed by the Critical Infrastructure Security Centre, Department of Home Affairs (DHA) in 2024. This Policy is proactively aligned with the enhanced CIRMP requirements.

5 The "big four" recommendations are best-practice logging, replacing legacy IT, effectively managing third-party risk and preparing for post-quantum cryptography. ASD 2024-25 Cyber Security Threat Report pages 40-42.

Legislation and guidance relevant to this Policy includes, but is not limited to:

- *Emergency Management Act 2005 (WA)*
- *Cyber Security Act 2024 (Cth)*
- *Government Trading Enterprises Act 2023 (WA)*
- *Data Availability and Transparency Act 2022 (Cth)*
- *Public Sector Management Act 1994 (WA)*
- *Security of Critical Infrastructure Act 2018 (Cth)*
- *State Records Act 2000 (WA)*
- *Privacy Act 1988 (Cth)*
- *Section 56. Financial Management Act 2006* (WA) (Establishment of the Office of GCIO).

This Policy supersedes 2024 WA Government Cyber Security Policy.

The requirements of this Policy are aligned with the information security advice from the Australian Cyber Security Centre (ACSC) and the US National Institute for Standards and Technology (NIST) Cyber Security Framework.

2026 WA Cyber Security Policy

1 Govern

Establish essential governance and foundations of cyber security management.

2 Identify

Identify elements of your entity's cyber security environment and manage its cyber security risks.

3 Protect

Protect your entity's critical services and information holdings.

4 Detect

Detect and diagnose a cyber security incident.

5 Respond

Respond to an identified cyber security incident.

6 Recover

Recover from the impact of a cyber security incident and restore capability, services and information.

Scope

Implementation of the Policy is mandatory for entities included in the Policy scope:

- WA Public Sector, as defined in the *Public Sector Management Act 1994 (WA)*
- Entities listed in the Schedule 1 of the *Public Sector Management Act 1994 (WA)*
- Senior Executive Service (SES) entities listed in the Schedule 2 of the *Public Sector Management Act 1994 (WA)*.

The scope excludes Local Government entities, however they are encouraged to comply with the provisions of the Policy.

Roles and responsibilities

Accountable Authority

The Director General (DG), Chief Executive Officer (CEO) or Chief Officer of each entity is accountable for the entity's cyber security risk management, including:

- The entity's cyber security risk assessment
- Implementation of cyber security prevention measures for the entity, and
- Responding to cyber security incidents affecting the entity.

Government Chief Information Officer (GCIO)

The GCIO is responsible for:

- Strategic direction for cyber security, digital transformation and data policy in WA government
- Provision of whole-of-government policy leadership, advice and direction on digital transformation, cyber security and incident prevention and management
- Acting for the Department of the Premier and Cabinet as the Hazard Management Agency for the Cybersecurity Incident Hazard, including the exercise of powers granted in Sections 50, 53 and 55(1) of the Emergency Management Act 2005 (Cth).

Cyber Security Unit (CSU), led by the Chief Information Security Officer (CISO)

The Cyber Security Unit, Office of Digital Government, the Department of the Premier and Cabinet is responsible for developing an integrated approach to information security for Western Australian Government, including:

- WA Cyber Security Policy, the main jurisdictional cyber security framework, in alignment with national and WA privacy legislation, national cyber security legislation, national and international cyber security standards and the WA threat context
- Annual Implementation Reporting process against the Policy, which helps CSU build a broad understanding of cyber risk and resilience across the sector and guide support where it is most needed
- Leadership of capability uplift across WA government, supporting entities included in the scope of this Policy to establish and improve their cyber security measures
- Leadership of WA Cyber Security Operations Centre (WA SOC) a centralised government-wide 24/7 service for threat detection and incident response and Vulnerability Scanning service
- Strategic communications and threat intelligence, improving the visibility of cyber security threats, vulnerabilities and controls across the WA Government sector
- Coordinating inter-agency operational responses to cyber security incidents
- Leadership of incident response engagement with the ACSC and interjurisdictional counterparts in line with Cyber Incident Management Arrangements for Australian Governments (CIMA)
- Leadership of whole-of-government expert groups that bring together ICT leaders and risk managers to facilitate knowledge sharing and development of tailored security solutions and best practices
- Leadership of targeted programs of work to address systemic issues that are identified across the sector
- Leadership and membership of national and jurisdictional expert bodies, strategic collaboration and information sharing.

1. Govern

Establish essential governance and foundations of cyber security management.

1.1 Accountable Authority

The Accountable Authority (DG, CEO or chief officer) of an entity is accountable for the entity's risk management, including cyber security risk management and implementation of this Policy.

The Accountable Authority:

a. Remains accountable for their entity's cyber security risks even when their entity's IT environment is managed by another entity or managed service provider
b. Allocates executive responsibility for cyber security to the Cyber Security Executive or serves as Cyber Security Executive by default
c. Considers the implications of their risk management decisions on WA Government
d. Shares threat and risk intelligence with the Office of Digital Government (DGov) in support of whole-of-government cyber security
e. Ensures the entity has sufficient resources to implement this Policy and ensure its continued implementation
f. Approves the Annual Implementation Report (AIR) before it is submitted to DGov.

1.2 Cyber Security Executive

The Cyber Security Executive has executive responsibility for the cyber security of an entity and must:

a. Have executive authority to implement this Policy
b. Possess or oversee the cyber security qualifications, skills and resources required to implement this Policy and ensure its continued implementation
c. Report to the Accountable Authority on the implementation of this Policy

d. Understand the implications of their entity's cyber security risk management decisions on other WA entities
e. Share information on risks with DGov where appropriate
f. Notify the Cyber Security Unit of DGov on cyber.policy@dpc.wa.gov.au within 5 days if the entity's Cyber Security Executive has changed.

1.3 Cyber Security Operations

Each entity must have cyber security capability (human resources) of sufficient size and competency to ensure the continued implementation of this Policy.

1.4 Cyber Security Governance

Each entity must establish cyber security governance and document its overall approach to implementing the requirements of the Policy, either through an existing governance committee or by establishing a dedicated cyber security governance committee. Governance arrangements must cover:

a. Development and maintenance of cyber security workplans including roadmaps (staged plans) to manage the implementation of all requirements of the Policy, detailing resources, deadlines and oversight arrangements
b. Implementation and executive reporting related to essential controls outlined in clauses 3.1 to 3.13
c. The entity's strategic and operational cyber security risk and vulnerability assessment of Information Technology (IT), Internet of Things (IoT) and Operational Technology (OT) risks and the potential impact on the entity's operations
d. Disaster recovery plans and capabilities for IT, OT and IoT technologies
e. Incident reporting, response and disaster recovery documents, processes and capabilities, including ensuring that they are fully understood and tested
f. A review of all entity security policies and procedures every 2 years, with executive oversight
g. Oversight of enterprise mobility
h. Oversight of device and data lifecycle management
i. Annual Implementation Reporting process (AIR)
j. Resolution of Office of the Auditor General (OAG) findings.

1.5 Annual Implementation Reporting

Each entity must provide its WA Government Cyber Security Policy AIR, approved by its Accountable Authority, to DGov by the deadline published for the relevant year.

1.6 OAG Management Letters

Entities must provide a copy of their OAG management letter containing any findings with relevance to cyber security or information systems, and their response to OAG findings, to DGov (cyber.policy@dpc.wa.gov.au) within seven days of responding to the OAG.

2. Identify

Develop organisational understanding to manage cyber security risks.

2.1 Cyber Security Context

Each entity must understand its cyber security context (people, processes, technology, information, procurement and application development) as a basis for sound cyber security decision-making. To achieve this understanding, entities must:

a. Achieve a reconciled enterprise view (and identify any critical interdependencies of) all tangible and intangible assets, including but not limited to:
   i. Hardware
   ii. Software
   iii. Applications
   iv. Enterprise mobility arrangements
   v. Data assets, including those the entity relies on but does not own.

   The reconciled enterprise view should be achieved using automated discovery methods where possible.

b. Understand any vulnerabilities and risks in its cyber security context (IT, OT and IoT)

c. Use the DGov Information Security Risk Self-Assessment Table to determine the substantive information risk tier appropriate to their data holdings

d. Manage Limited Use Obligations with appropriate WA Information Classification Policy labeling (Official: Sensitive Legal (Limited Use)) to facilitate threat intelligence sharing within WA Government

e. Implement information classification and labeling processes based on the WA Information Classification Policy. Automated methods should be used to achieve this where possible[6]

6 While Schedule 1 entities are not currently included in the scope of the WA Information Classification Policy, compliance with the mandates of the WA Cyber Security Policy is expected including where they rely on information classification, including clause 2.1 (Cyber Security Risk Context), subclauses c (Risk Assessment Table) and d (Limited Use Obligations).

f. Implement data loss prevention (DLP) strategies based on static attributes and classification labels. To achieve this, automated methods should be established and used where possible
   i. Technical controls to detect and prevent unauthorised data exfiltration (e.g. DLP solutions)
   ii. Monitor for anomalous data transfers, including to removable media, cloud
   iii. Apply DLP policies to protect sensitive information in line with the WA Information Classification Policy and DGov Risk Self-Assessment Table
g. Be able to access data within the period defined by the entity's Record Keeping Plan and the State Records Act 2000 (WA) and ensure that data is not kept for longer than necessary
h. Review arrangements giving individuals access to entity information and systems and OT systems (whether staff, consultants, contractors or service providers) every two years.

2.2 Cyber Security Risk Management

Each entity must establish a Cyber Security Risk Management program to manage cyber security risks to the entity's information and operations (including its mission, image and reputation).

The Cyber Security Risk Management Program must be documented with reference to this Policy.

The Cyber Security Risks Management Program should take account of:

a. The entity information confidentiality and integrity requirements
b. Risks arising from the entity's cyber security context
c. Risks arising from all individuals accessing the entity's systems, including staff, consultants, contractors and service providers
d. Any other business continuity risks.

Risk should be reassessed when any of the following occur:

e. Two years have elapsed since last risk assessment
f. New systems or services are implemented
g. The security posture or the threat level changes; or
h. There are major changes to the entity's operating environment.

3. Protect

Protect critical services and information holdings.

Each entity must implement all the controls outlined in Policy Domain 3 (Protect) by December 2028.

3.1 The Essential Controls[7]

The entity's decision on how to prioritise the implementation of this clause will be determined by the entity's cyber security context and risk assessment.

Where primary controls cannot be implemented, compensating/mitigating controls should be implemented to achieve the same or similar security objective and any residual risks documented with executive sign-off.

3.1.1 Patch Applications

a. Patches must be applied within 14 days of release, or 48 hours if a critical vulnerability/exploit exists
b. Undertake weekly (or more frequent) scanning for missing patches on all systems including OT and IoT
c. High-risk applications (browser, Microsoft Office, PDF) must be patched at least fortnightly
d. Legacy systems and unsupported application versions must be documented and transition plans developed by the end of 2027
e. Patch deployment should be automated where possible.

3.1.2 Patch Operating Systems (OS)

a. Internet-facing or important systems must be updated within 48 hours. All other updates must be completed on a maximum 2-week cycle
b. New OS fixes must be verified to ensure functionality
c. Legacy OS must be documented and transition plans developed by the end of 2027

7 The Essential Controls clause comprises thirteen key controls. Eight are aligned with Essential Eight with specific applications described at Maturity Level 2, and five are aligned with additional five controls from the list of 37 ACSC Strategies for Mitigating Cyber Security Incidents prioritized by DGov based on WA threat landscape, commonly known as the "further five".

d. OS on all machines must have the latest security patch level
e. Auto-updates should be utilised where possible
f. Entities should test and deploy patches in a timely manner, including outside normal schedules if warranted by risk.

3.1.3 Multi-factor Authentication (MFA)

a. MFA is required for all user accounts accessing agency systems processing, storing or communicating sensitive or official data (enterprise-wide MFA)
b. No login is possible to critical systems (such as operational technology systems or data repositories) without MFA, even on the internal network
c. Entities must implement phishing-resistant MFA, or the strongest form of MFA supported by their systems
d. Legacy authentication protocols that cannot enforce MFA must be disabled
e. Adaptive MFA is encouraged for high-risk actions
f. All MFA events are centrally logged and abnormal patterns trigger alerts

3.1.4 Restrict Administrative Privileges

a. Access to administrator functions requires a written justification and formal approval.
b. All privileged accounts are re-validated once a year, with a quarterly manager re-approval, or more often if required. Accounts should expire automatically if not re-approved
c. Admin accounts are technically prevented (prevented by systems, not only by policy) from accessing internet or email
d. Entity staff performing admin functions must use dedicated secure admin workstations or jump-servers
e. Just-in-time elevation should be implemented where feasible and standing admin rights minimised. Staff performing admin functions must use non-privileged accounts by default, with their access elevated only when needed
f. All administrative actions are centrally logged and actively monitored.

3.1.5 Application Control (Allowlisting)

a. Allowlisting is extended to all entity endpoints, including internet-facing servers
b. All unapproved executables, scripts, installers, libraries, etc. are disallowed
c. Microsoft recommended block rules are enabled (e.g. script interpreters, LOLBins)
d. Rules are centrally managed and reviewed at least annually or whenever new threats are identified

e. Non-administrative users cannot bypass or alter allowlisting settings
f. All executions (allowed/blocked) are logged centrally
g. Threat protections are embedded in application workflows to defend against targeted and application-specific threats.

3.1.6 Restrict Office Macros

a. Macros run only in highly controlled circumstances. Unsolicited macros are universally blocked
b. Macros are disabled by default for all users and only explicit exceptions are allowed
c. Even for allowed users, only macros that are trusted (e.g. in Trusted Locations or with a trusted digital signature) can execute. All other macros are blocked without any scope for user override
d. Microsoft Office is configured so that macros cannot call Win32 APIs or spawn child processes (enforced lockdown)
e. All macro execution (allowed or blocked) is centrally logged and monitored.

3.1.7 User Application Hardening

a. Entities must maximise hardening of all user software. All unsupported components (such as Flash, IE11, etc.) should be fully removed or disabled system-wide
b. Browsers are locked down to allow only necessary features. Allow lists are enabled for browser extensions or block all but approved sites for active content
c. Office applications are configured to disable legacy features (e.g., old file format support if not needed, OLE object prompts) and prevent Office from launching external executables
d. PDF reader software is:
    i. Blocked from creating child processes
    ii. Hardened using ASD and vendor guidance, with the most restrictive guidance taking precedence where advice conflicts
    iii. Configured so that security settings cannot be changed by users.
e. Any other software that provides macro-like functions or scripting functionality is:
    i. Blocked from creating child processes
    ii. Hardened using vendor guidance
    iii. Configured so that security settings cannot be changed by users.
f. Any setting that can reduce risk is enabled, using latest CIS benchmarks/ACSC guidelines. These settings are reviewed and updated regularly as new threats emerge. Standard users are unable to modify settings.

3.1.8 Regular Backups

a. Daily or more frequent backups are enabled in line with entity business continuity needs, including multiple snapshots per day for mission-critical data
b. Backups must meet defined Recovery Point Objective and Recovery Time Objective from the entity Business Continuity Plan/ Disaster Recovery Plan
c. Backups must be stored in ways that are immutable and isolated, for example on offline media or cloud storage with write-once controls to preserve integrity
d. Access is strictly limited: Administrative staff do not have the ability to easily access and purge backups. Separate credentials or MFA should be used for backup deletion
e. Recovery should be tested regularly, not just annually but through scheduled drills in which ransomware recovery should be simulated to ensure that backups are viable
f. Multiple generations of backups should be kept, ensuring that one copy is always off-network (out of reach of cyberattack)
g. Backups should be encrypted for confidentiality, and integrity verified in accordance with the entity Business Continuity Plan.

3.1.9 Server Application Hardening

a. Server Application Hardening configurations are implemented
b. Specific attention is paid to securing the entity's Domain Controllers.

3.1.10 Block Spoofed Emails

a. Authenticated Email and Anti-spoofing Controls (Block Spoofed Emails controls) are implemented.

3.1.11 Secure Network Architecture and Design

a. Network segmentation and micro-segmentation are implemented
b. Isolation mechanisms and micro-perimeters restrict lateral movement of threat actors and secure service-specific connections, achieving micro-segregation
c. A protective domain naming system (DNS) is implemented
d. Network documentation is developed, implemented and maintained.

3.1.12 Continuous Incident Detection and Response

a. The entity has the capability to perform continuous incident detection and response (The specific requirements have been detailed in the Policy Domains 4, Detect, and 5, Respond).

3.1.13 Personnel Management

a. Personnel Management strategies are in place to minimise malicious insider risk
b. All staff, consultants and contractors with access to government-owned information and systems must undergo an appropriate background check upon onboarding. Acceptable checks include:
    i. AusCheck (mandatory for critical workers in critical infrastructure entities captured under the SOCI Act 2018)
    ii. Australian Government Security Vetting Agency (mandatory for financial institutions such as GESB)
    iii. Police clearance
    iv. NCCHC (Nationally Coordinated Criminal History Check)
    v. Any other clearance provider considered appropriate by the entity
c. Conducts and document targeted reviews of privileged and generic account access
d. Develop contractor, casual and third-party access management protocols aligned with Identity and Access Management principles.

3.1.14 Any additional controls

Based on the entity's cyber security risk assessment, each entity must decide whether it requires the implementation of any additional controls that may include:

a. Any additional controls from the ASD Strategies to mitigate Cyber Security Incidents
b. Application of Modern Defensible Architecture
c. Consider appropriate security controls for non-Microsoft platforms.

3.2 Cyber Security Training

Each entity must ensure that users accessing their systems undertake:

a. Cyber security awareness training on an annual basis
b. Additional tailored cyber security training for staff in specialist positions, such as cyber security specialists, executives, finance/payroll staff or staff with access to personal and sensitive information.

3.3 Enterprise Mobility

Each entity must ensure that entity information accessed by corporate-issued and BYO devices is secure at all times.

a. The entity governs device and asset lifecycles via entity-wide policies, automated where possible. Non-compliant devices are identified, isolated, monitored and reviewed

b. Network capabilities are tuned to meet availability demands
c. The entity undertakes threat modelling for device applications to identify and manage information security risks
d. Wherever possible, entity devices and virtual assets are continuously monitored, with automated inventory and anomaly detection to flag unauthorised access
e. Wherever possible, mission-critical applications are securely accessible over public networks to authorised users with verified credentials via a secure VPN controlled by the entity.

3.4 Secure Procurement and Supply Chain Risk Management

Each entity must assess and manage cyber security risk as a part of their procurement process for any goods or services that require suppliers or vendors to access the entity's data or systems.

These requirements apply to any new procurements, or where existing contract extension options allow for renegotiation or variations of contract requirements.

In managing procurement risks, an entity should assess the supplier's/vendor's:

a. Information security maturity, including relevant security certifications/assurances. For Tier 1 Risk procurements, preference should be given to suppliers with current certification from an ACSC Infosec Registered Assessors Program (IRAP) qualified assessor, or equivalent similar industry certification
b. Ability to enable the procuring entity to implement its WA Cyber Security Policy obligations, including reporting cyber security incidents to DGov within 6 hours of incident being suspected or confirmed
c. Personnel security controls for accessing entity data, including subcontractors, service providers and consultants
d. Artificial Intelligence security
e. Software security practices for software that is procured or developed in-house
f. Adequate insurance arrangements including, but not limited to:
    i. Public liability insurance
    ii. Product liability insurance (where procurement includes products)
    iii. Professional indemnity insurance and
    iv. Cyber liability insurance.

Entities should also ensure:

g. Entity information remains the property of the entity for the duration of the contract and will be securely removed, disposed of, or transferred back to the entity upon termination of the contract, termination of a managed service, novation, or assignment to a third party
h. An adequate shared responsibility model exists between the supplier and the entity
i. Foreign ownership control and influence (FOCI) risks have been assessed and addressed
j. Key performance indicators relevant to the goods or services being procured are developed for performance management purposes
k. Remedies are available in the event of default or failure to meet procurement requirements.

Additional frameworks, including the ACSC Procurement Guidelines, ACSC Supply Chain Risk Management and ACSC Guidelines for Software Development are available to assist entities in managing procurement risks.

3.5 Data Offshoring

Entities must not offshore information classified as Tier 1 Risk.

Each entity must perform a risk assessment and establish governance of their information offshoring arrangements, with reference to the DGov Information Security Risk Self-Assessment Table and the Policy Implementation Guideline 3.5 (Data Offshoring Governance with WA Government Offshoring Position). [8]

3.6 Secure Data Removal and Device Disposal

Each entity must establish, document and maintain secure data and device disposal governance to ensure that government information is irrecoverable.

8 Western Australian Information Classification Policy is in alignment with WA Cyber Security Policy and Offshoring Governance guidance.

3.7 Vulnerability Management Program

Each entity must develop and implement a Vulnerability Management Program to address identified vulnerabilities and risks, including establishing:

a. Daily automated vulnerability scanning of its ICT environment including OT and IoT capabilities where possible
b. Other processes to identify vulnerabilities where automation is not possible
c. A process for vulnerability disclosure and reporting (internal and external)
d. Remediation of all vulnerabilities identified
e. A documented risk-based approach to manage vulnerabilities that cannot be remediated.

3.8 Identity and Access Management

Each entity must implement and maintain appropriate management, monitoring and review of user accounts, including customer and system accounts, to reduce the risk of unauthorised access, including:

a. Appropriate management of user lifecycle that supports Personnel Management (ACSC Strategies)
b. Following the principle of least privilege when providing access
c. A password filtering solution is implemented for all user accounts.

3.9 Physical Security of Assets

Each entity must ensure that physical access to their information technology and operational technology assets is managed to prevent unauthorised use and physical damage.

In areas which host core technology infrastructure, entities should implement controls which include, but are not limited to:

a. Identify the nature of the site the critical asset is located on, including ownership and tenancy, and how such arrangements could the availability or security of the asset
b. Potential risks posed by nearby attractive targets and other critical infrastructure assets
c. Fences and security barriers
d. Automated fire suppression system
e. Temperature and humidity controls
f. Electronic access control

g. Appropriate surveillance and out of hours controls such as alarms, secure doors, sensors and CCTV monitoring
h. Regular testing of arrangements, to ensure they are effective and appropriate to detect, deter, respond to and recover from a breach of physical security.

3.10 Personnel Security

Entities must manage personnel risks to information and OT security by practicing role-relevant and appropriate vetting processes for staff, consultants and contractors with access to government information systems and OT.

Entities should ensure that all personnel with access to entity systems, information and OT:

a. Demonstrate a suitable standard of integrity and honesty required to access and use WA Government data, systems and OT
b. Meet personnel security requirements for access to entity's data
c. Demonstrate that personnel (including contractors, casual workers and third parties) are vetted in reference to the risk-assessment of the information, systems and OT they would be accessing at all stages of engagement, including:
    i. Pre-engagement (before they gain access)
    ii. Engagement (monitoring whilst accessing)
    iii. Separation (after temporary or permanent loss of access)
d. The entity must actively review, validate and update their personnel security policies and procedures every two years, and embed these security requirements into human resources and local work management practices, as well as Cyber Security Governance.

3.11 Encryption

Entities must ensure encryption of entity data at rest and in transit at level AES 128, or higher where required.

a. Encryption keys are protected. Secrets are not hard-coded and are rotated on a regular basis
b. The entity manages issuance and rotation of keys and certificates
c. All internal and external traffic protocols are encrypted.

3.12 Post-Quantum Cryptographic (PQC) Standards

Each entity must consider and document an approach to transitioning to Post Quantum Cryptography (PQC) standards by December 2027.

3.13 Secure Development of Applications and Software

Each entity must monitor the security of in-house application and software development, which should attract the same process as risk assessment as procurement of bespoke software, following a process that ensures security requirements are identified, implemented and verified.

a. Segregate development, security, and operations teams. Restrict unauthorised changes to production environments
b. Ensure security controls are applied consistently across all environments, including testing, development and production
c. Sensitive production data is sanitised (deidentified, scrambled, obfuscated) when used in non-production environments
d. Integrate application security testing, including regular dynamic testing, into the development and deployment process
e. Train developers on secure software development processes and common application security risks.

Additional information on secure development of applications and software can be found in the ACSC Guidelines for software development.

3.14 Artificial Intelligence Security

Entities must manage the security risks of Artificial Intelligence.

3.14.1 Publicly available AI Systems

Entities must not input Tier 1 or Tier 2 Risk information [9] or security classified information into consumer or publicly available AI systems. Only publicly available, non-sensitive, non-proprietary information or information formally approved for public release may be used with such systems.

9 As defined by the DGov Information Security Risk Self-Assessment Table.

3.14.2 Enterprise or Custom AI Systems

Where agencies deploy enterprise-grade or custom-built AI models, they must ensure that they are cyber-secure:

a. Ensure that WA government inputs into AI (including prompts and datasets used for model training) are under the exclusive control of the entity
b. Implement applicable protective security controls outlined in Policy Domain 3 (Protect)
c. Enforce data retention and deletion policies including ensuring that the supplier deletes the model if the entity cancels their service
d. Ensure foreign ownership and data sovereignty (offshoring) risks of AI systems have been assessed and addressed. Tier 1 Risk information is not offshored.

3.14.3 Quality control and accountability

Agencies must ensure:

a. Inputs are validated to prevent data poisoning or prompt injection attacks
b. Outputs are reviewed for hallucinations or malicious content before use
c. AI models are monitored for model drift and adversarial manipulation
d. Human oversight of AI-generated outputs and AI-assisted decision making to ensure that decisions made by AI are transparent, explainable and contestable
e. Human oversight and governance of security measures applied to AI systems
f. Staff are trained on AI-specific cyber threats and mitigation strategies.

3.15 Security of Operational Technology (OT) and Industrial Control Systems (ICS)

Entities using OT and Industrial Control Systems (ICS) must manage security risks in their environments, including implementing the following controls:

a. OT operators should assess OT security against the WA Cyber Security Policy and apply all controls that are appropriate to their environments
b. Legacy OT must be documented and transition plans developed by the end of 2027
c. Entities using OT should implement Network Segmentation, ensuring the highest practical level of segregation of your entity's critical systems from all other networks, including implementing relevant standards and zoning models to isolate OT assets
d. Establish oversight of patch management and firmware updates
e. Implement compensating controls where possible, to overcome patching limitations
f. Implement protocol-specific protections (e.g. Modbus, DNP3 and OPC-UA)
g. Harden out-of-the-box configurations (passwords are changed and unnecessary services disabled)
h. Harden configurations of other network hosts that interact with OT
i. Ensure critical systems are operationally independent from IT systems, such that they can be sustained during an IT outage
j. Maintaining an inventory of critical assets that are important to the delivery of the function of the asset
k. Maintain and review access logs for communication paths between IT and OT networks
l. Understand and mitigate OT risks associated with AI
m. Assess OT procurement against requirements outlined in clause 3.4 and apply controls as appropriate.

3.16 Security of Internet of Things (IoT) Devices

Entities must manage security risks of IoT whether already in their networks or being procured by:

a. Assessing IoT procurement against requirements outlined in clause 3.4 and applying controls as appropriate
b. Implementing IoT relevant controls from clauses 3.1 (Essential Controls) and 3.15 (Security of Operational Technology and Industrial Control Systems).

3.17 Cyber Security Insurance

Each entity must collaborate with the Insurance Commission of Western Australia (ICWA) (or make other appropriate insurance arrangements such as self-insurance), including:

a. Cyber insurance for losses incurred by the entity as a result of a cyber security incident
b. Cyber Liability insurance.

3.18 Whole-of-Government Cyber Security Advice and Direction

Each entity must:

a. Comply with whole-of-government advice direction and strongly consider advice on cyber security or any related matters issued by the GCIO, or write to DGov (cyber.policy@dpc.wa.gov.au) to request an exemption from the direction
b. Consider the cyber threat intelligence and advice provided by DGov and take action as required
c. Implement whole-of-government advice and DGov government guidance on Limited Use Obligations under the Cyber Security Act 2024 (Cth).

4. Detect

Detect and triage a cyber security incident.

4.1 Continuous Monitoring

Each entity must continuously monitor, analyse and triage cyber security events and initiate action on suspected or confirmed incidents, specifically:

a. Establish and maintain a Security Information and Event Management System (SIEM) solution with a continuous incident detection and response system for its assets and networks, aligned to DGov's WA Security Operations Centre (WASOC) SIEM Guidance baseline for data sources and detections

b. Ensure sufficient and appropriate logs are collected to minimise visibility gaps

c. Ensure the collection of logs into the SIEM is timely

d. Ensure the integrity of logs is protected from unauthorised access

e. Retain firewall, networking, DNS and verbose data source logs for a minimum of six months

f. Retain Endpoint Detection, Identity and Access Management (IAM), Email Exchange and Office logs for a minimum of 12 months

g. Where possible, automate your entity's response to threat intelligence information received.

4.2 Adverse Event Analysis

Each entity must ensure that the likelihood and potential impact of an adverse event[10] affecting their entity is well understood, by taking the following steps:

a. Facilitating the transfer of cyber security incident information from the entity SIEM to WASOC
   i. The entity's SIEM must connect to WASOC through direct integration
   ii. If direct integration is not possible, the entity must work with DGov to find an alternative arrangement to provide DGov with similar visibility over their networks and systems.
b. Identifying adverse events through characteristics such as attacks and compromises, excessive resource utilisation, spikes in service use, behaviour pattern changes, billing spikes
c. Triaging events, categorising them and actioning the entity incident response playbook within four hours of a suspected or confirmed incident
d. Reviewing adverse events at least every 24 hours within normal operational periods, as a part of the entity's standard operating procedures
e. Understanding the potential impact of adverse events on the entity and the WA government
f. Sharing any threat intelligence with DGov within six hours of acquiring it via the reporting portal https://irp.dpc.wa.gov.au. (In addition, you can also phone 1800 922 923 (1800 WA CYBER) and/or email cybersecurity@dpc.wa.gov.au

10 An adverse event is an occurrence that indicates unauthorized access, a breach, a system failure or unexpected state which could threaten the confidentiality, integrity or availability of information systems. Events can be caused by malicious actors or unintentional errors such as misconfigurations.

5. Respond

Respond to an identified cyber security incident.

5.1 Incident Reporting

Each entity must report any suspected or confirmed cyber security incidents to DGov within 6 hours of suspicion/ confirmation via the reporting portal https://irp.dpc.wa.gov.au. (In addition, you can also phone 1800 922 923 (1800 WA CYBER) and/or email cybersecurity@dpc.wa.gov.au

For suspected incidents, DGov will assist with triaging to confirm or classify the incident.

Confirmed incidents are to be reported to ACSC within 12 hours of detection on Report | Cyber.gov.au.

For confirmed incidents, the reports must include the following information:

a. Type of incident
b. Indicators of compromise, if known
c. Tactics, Techniques and Procedures (according to MITRE ATT&CK matrices)
d. Impact to agency and whether an Incident Response Plan/ playbooks have been activated
e. Any other relevant information provided as it becomes known.

Any information provided to DGov regarding incident management will be treated in the strictest confidence.

5.2 Cyber Security Incident Management and Response Plan

Each entity must develop and exercise a cyber security incident management and response plan, which:

a. Is printed out and stored in a secure, but well-known and accessible location and readily available to be executed in the event of a cyber security incident
b. Includes the requirement for the entity to triage incidents and follow the relevant playbook within 4 hours of a suspected or confirmed incident
c. Includes the requirement to report confirmed or suspected cyber security incidents to DGov within 6 hours of detection/suspicion, and to ACSC through ReportCyber within 12 hours of confirmation.

d. If the incident is reported verbally to either DGov or to ACSC within 6 hours the incident, it must also be reported in writing within 48 hours of the verbal report via the reporting portal https://irp.dpc.wa.gov.au. (In addition, you can also phone 1800 922 923 (1800 WA CYBER) and/or email cybersecurity@dpc.wa.gov.au
e. Documents alignment with the WACSICF
f. Incorporates MITRE ATT&CK for ICS into incident response planning for Entities relying on OT.

5.3 Incident Response Playbooks

In preparation for a cyber security incident, agencies must develop and maintain incident response playbooks for the main types of cyber security incidents (Phishing, Data Breach (Theft), Malware, Ransomware, Denial of Service) based on their entity environment and the WA threat landscape.

5.4 Cyber Security Exercises and Testing

Each entity must perform annual cyber security incident response exercises and testing.

5.5 Government Ransomware Position

The Western Australian Government does not support the payment of ransom.

Any ransom demands related to cyber incidents should be reported immediately via the reporting portal https://irp.dpc.wa.gov.au. (In addition, you can also phone 1800 922 923 (1800 WA CYBER) and/or email cybersecurity@dpc.wa.gov.au)

In the event of a ransomware attack, DGov will assist in determining next steps including involving the WA Police Force. All entities must report ransom requests to DGov immediately.

6. Recover

Recover from the impact of a cyber security incident and restore capability, services and information.

6.1 Capability to Restore Services and Information

Each entity must have the capability to recover and restore their services and information in the event of a disruption caused by a cyber security incident, within the timeframes defined by the entity's Business Continuity Plan (BCP), Disaster Recovery Plan (DRP) and Cyber Security Incident Response Plan (CIRP).

a. Entities must maintain Disaster Recovery Plans and procedures for their critical ("crown jewels") systems and information

b. Entities must test Disaster Recovery Plans annually, with results reported to DGov through the Annual Implementation Report

c. Ensure recovery capability aligns with BCP/DRP/CIRP timeframes.

6.2 Response Lessons Learned

Following a significant cyber security incident or cyber crisis and once response is complete, each entity must review response lessons learned and create a Post Incident Review (PIR) report. The PIR must be shared with DGov within 20 working days from the date the entity's cyber incident response is completed.

Where appropriate, its findings should inform a review of the entity's Business Continuity and Disaster Recovery Plan as well as future programs of work documented within the entity's cyber security governance.

Annual Implementation Reporting

Entities must respond to AIR requests issued by DGov and provide its AIR to DGov. AIRs must be completed using the format prescribed by DGov. The Report must be approved by the agency's Accountable Authority.

DGov will collate and analyse the AIRs provided by entities and provide the Cabinet with a deidentified and aggregated report based on the information received. AIRs are due during the fourth quarter of each calendar year.

This Policy acknowledges that some entities captured by the SOCI Act have pre-existing cyber security control requirements and reporting obligations as a part of their Critical Infrastructure Risk Management Programs (CIRMP). WA Government entities captured under the SOCI Act can use this Policy as an equivalent framework for the purpose of reporting on their cyber and information security hazard to the DHA as per section 8 (5) under Security of Critical Infrastructure Risk Management Program Rules (LIN23/006). This Policy also responds to enhanced CIRMP requirements (2025).

Entities that utilise different cyber security frameworks such as Australian Energy Sector Cyber Security Framework (AESCSF) can submit their self-assessment under those along with assessment against the remaining clauses of the Policy not covered by the chosen Framework, which will be considered in lieu of AIRs to reduce reporting duplication.

Exemptions

Where a requirement of this Policy or of GCIO issued whole-of-government advice and direction is inappropriate for an entity's business model, the entity may apply for an exemption.

Exemption applications will be considered by the Chief Information Security Officer on a case-by-case basis. Policy exemptions will be granted if deemed justified by the entity's circumstances.

To request an exemption, the entity's Cyber Security Executive should contact DGov (Cyber.Policy@dpc.wa.gov.au) and provide a justification for the proposed exemption request approved by the entity's Accountable Authority.

Entity exemption applications should include:

- the purpose of the exemption, and
- a detailed account of measures which the entity has taken to mitigate security risks associated with operating under an exemption.

In addition to assessment by CISO, requests for exemption from Policy clause 3.5 (Offshoring Governance) [i.e. requests to offshore government information rated Tier 1 Risk on the DGOV Information Security Self-Assessment Table will require the Minister for Science and Innovation to be notified.

Review

This Policy is reviewed and updated every two years. It may be reviewed earlier by decision of the Cabinet, the Premier or the Minister for Science and Innovation.

The most recent Policy review was conducted in late 2025 and 2026. The Draft 2026 Policy was developed in consultation with all entities included in the Scope of the Policy. The next Policy review is scheduled for Q3 2028.

Additional Resources

Supporting guidance and material is available to assist entities with the implementation of this Policy.

DGov Guidance Documents

DGov is in the process of preparing guidance for each clause of the Policy. Some documents have been published on the WA Cyber Security Policy Webpage. Others can be shared in draft. For enquiries, please contact us on cyber.policy@dpc.wa.gov.au.

Clause title	Clause	Resource
General Cyber Security Frameworks		
General Guidance for cyber security		ISO 27001 SOC2 FedRAMP NIST CSF ACSC ISM CIS Security Controls
Non-Domain Clauses		
Alignment		Cyber Security Measures for WA Government Entities – Premier's Circular 2025/13 WA Information Classification Policy Protective Security Policy Framework (PSPF) Directions Proposed enhanced Critical Infrastructure Risk Management Program (CIRMP) US National Institute for Standards and Technology (NIST) Cyber Security Framework
Domain 1: Govern		
Cyber Security Governance	1.4	Australian Prudential Regulation Authority Standard 234 – Information Security Cyber Security Governance Principles | Version 2
Domain 2: Identify		
Cyber Security Risk Management	2.1 & 2.2	DGov Information Security Risk Self-Assessment Table NCSC Cyber Security Risk Management Framework NIST Risk Management Framework | CSRC NIST Risk Management framework Special Publication 800-30 Revision 1 Guide for conducting risk assessments Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023 Australian Prudential Regulation Authority (APRA) Standard 230 - Operational Risk

Clause title	Clause	Resource
Domain 3: Protect		
The Essential Controls	All sub-clauses	Essential Eight Maturity model Strategies to mitigate cyber security incidents NIST SP 800-207 Zero Trust Architecture ACSC Gateway security guidance package: Gateway technology guides Memorandum 22-09 – Moving the US Government Toward Zero Trust Cybersecurity Principles
The Essential Controls (Multi-Factor Authentication)	3.1.3	NIST SP 800-63B-4 Digital Identity Guidelines: Authentication and Authenticator Management
The Essential Controls (User Application Hardening)	3.1.7	CIS Benchmarks List ACSC Guidelines for System Hardening Microsoft Security Baselines Blog Security Configuration Guide for Acrobat Chrome Browser Enterprise Security Configuration Guide
The Essential Controls (Server Application Hardening)	3.1.9	ACSC Guidelines for Networking
The Essential Controls (Block Spoofed Emails)	3.1.10	CISA Binding Operational Directive 18-01
The Essential Controls (Secure Network Architecture and Design)	3.1.11	ACSC Gateway security guidance package: Gateway technology guides ACSC Guidelines for Networking
The Essential Controls (Any Additional Controls)	3.1.14	ASD Strategies to mitigate Cyber Security Incidents Modern Defensible Architecture NCSC Mac OS Device security guidance NIST Automated Secure Configuration Guidance from the macOS Security Compliance Project
Enterprise Mobility	3.3	ACSC guidelines for Enterprise Mobility

Clause title	Clause	Resource
Secure Procurement and Supply Chain Risk	3.4	ACSC Guidelines for procurement and outsourcing ACSC Managing cyber supply chains DGov Information Security Risk Self-Assessment Table ACSC Infosec Registered Assessors Program (IRAP)
Secure Procurement and Supply Chain Risk & Data Offshoring & Secure Data Removal and Device Disposal	3.4, 3.5, 3.6	Australian Prudential Regulation Authority Standard 235 – Data Management
Secure Data Removal and Device Disposal	3.6	NIST SP 800-88 Rev. 2 Guidelines for Media Sanitization ACSC How to dispose of your device securely
Identity and Access Management	3.8	CISA Trusted Information Guidance Documents Microsoft – FIDO Passkeys: Password less Authentication
Personnel Security	3.10(b)	DGov Information Security Risk Self-Assessment Table
Encryption	3.11	NIST Key Management Guidelines ACSC Cryptographic fundamentals OMB M-15-13 M-19-26 M-22-09 DHS Binding Operational Directive 18-01 NIST SP 800-207 HTTPS Interception Weakens TLS Security | CISA
Post-Quantum Cryptographic Standards	3.12	ACSC Guidelines for Cryptography controls: • ISM-2073 • ISM-1917 • ISM-1990 • ISM-1996

Clause title	Clause	Resource
Secure Development of Applications and Software	3.13	ACSC Guidelines for software development
Artificial Intelligence Security	3.14.2(d)	DGov Information Security Risk Self-Assessment Table
Security of Internet-of-Things Devices (IoT)	3.15	Please refer to DGov Risk Assessment Template for IoT which can be requested on cyber.policy@dpc.wa.gov.au
Security of Operational Technology and Industrial Control Systems	3.16(a)	NIST 800 82 Rev 3 CISA ICS best practises IEC/ISA 62443 MITRE ATT&CK for ICS
	3.16(c)	NIST 800 82 Rev 3 CISA OT Segmentation Guide ISA/IEC 62443 ISO/IEC 80001-1 ISO/IEC 27019
	3.16(f)	Modbus Specifications and Implementation Guides Overview of DNP3 Protocol OPC Unified Architecture
Whole-of-Government Cyber Security Advice and Direction	3.18(c)	Cyber Security Advisory Notice – Limited Use Provisions in the Cyber Security Legislative Package 2024 (Cth)

Clause title	Clause	Resource
Domain 4: Detect		
Continuous Monitoring	4.1(a)	WASOC SIEM Guidance Cyber Security and Record Keeping Best practices for event logging and threat detection WA Cyber Security Policy Clauses and SRC Standards Table
Adverse Event Analysis	4.2	WA Security Operations Centre - IRP
Domain 5: Respond		
Incident Reporting & Cyber Security Incident Management & Incident Response Playbooks	5.1, 5.2, 5.3	ACSC: Cybersecurity incident response planning: Practitioner guidance CISA Cybersecurity Incident & Vulnerability Response Playbooks
Incident Reporting & Cyber Security Incident Management	5.1, 5.2	MITRE ATT&CK Data Sources Atlassian - How to create an incident response playbook
Cyber Security Exercises and Testing	5.4	NIST SP 1800-26 Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events
Domain 6: Recover		
Capability to Restore Services and Information & Response Lessons Learned	6.1 & 6.2	Governing Through a Cyber Crisis - Cyber Incident Response and Recovery for Australian Directors
Annual Implementation Reporting		
Annual Implementation Reporting	N/A	Consultation on enhancements to the CIRMP Rules

Further information

For further information about this Policy, visit DGov website
Office of Digital Government (www.wa.gov.au) or email cyber.policy@dpc.wa.gov.au.

Western Australian Government Cyber Security Policy