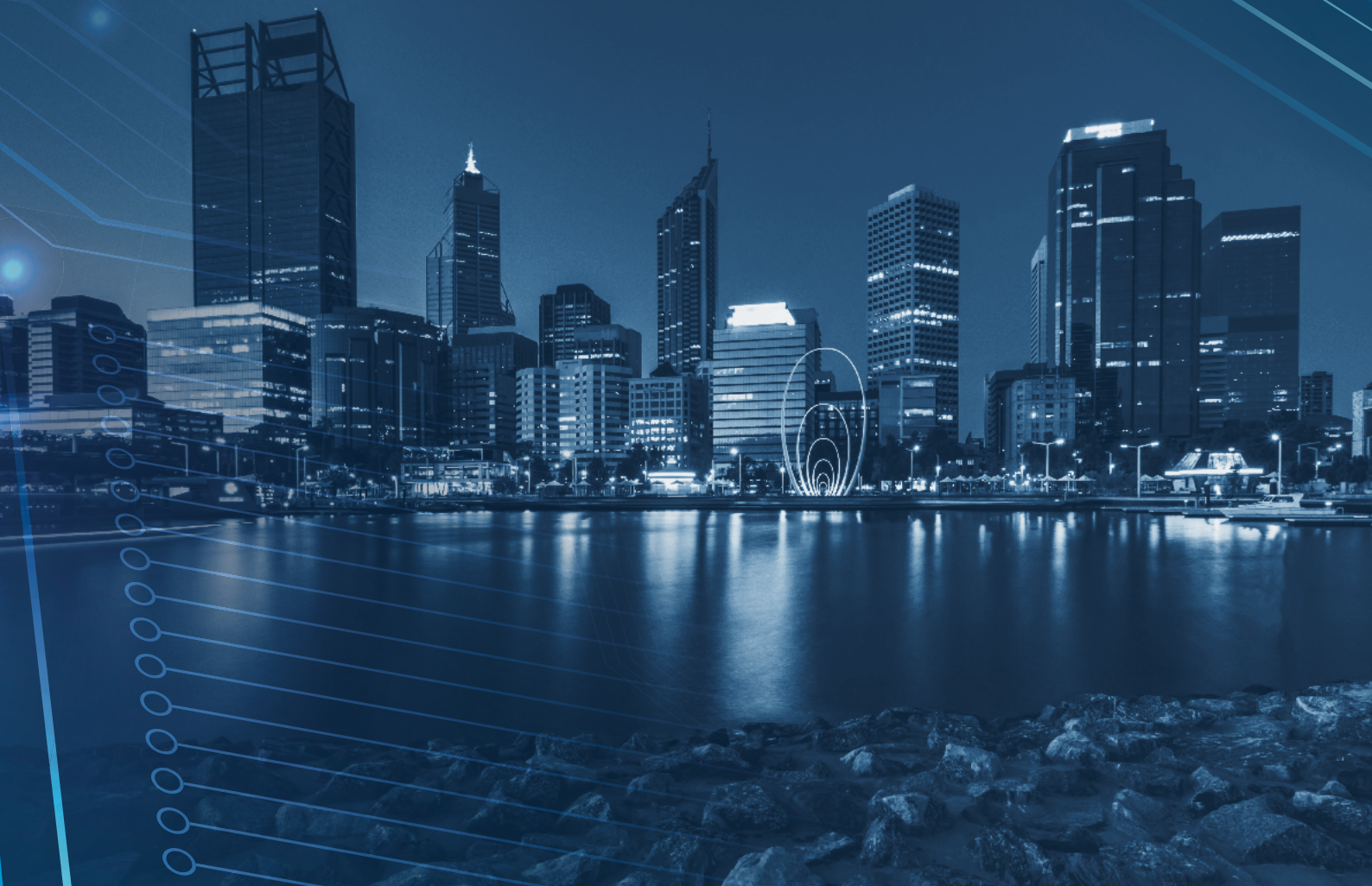
GOVERNMENT OF
WESTERN AUSTRALIA

Western Australian Government Cyber Security Policy

2024



Contents

Introduction

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

Cyber security 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 cannot be eliminated, a comprehensive and systematic approach to cyber security will assist the State Government in reducing the level of cyber security risk to its operations and information.

Western Australian Government entities rely on secure technology to manage valuable information and infrastructure, provide public services and ensure business continuity.

As Australians integrate more technology into their lives and businesses, the number of possible weak points or vectors for malicious cyber actors to exploit — known as the attack surface — grows.[1]

The consequences of losing information and disruption to services include financial loss, reputational harm and citizens' loss of trust in using the Government's expanding digital services.

Many incidents reported each year within the WA Government and in Australia could have been avoided or mitigated by implementing good cyber security practices.

[1] Australian Signals Directorate (ASD) Cyber Threat Report 2022-2023, p 11.

Purpose

The purpose of this Policy is to prescribe the baseline for cyber security capabilities and practices for the WA Government. Specifically, the Policy:

Alignment

Prescribes the establishment and maintenance of key cyber security controls in **alignment** with the advice from the Australian Cyber Security Centre (ACSC) and the United States National Institute of Standards and Technology (NIST).

Prevention

Prescribes the establishment and maintenance of cyber security practices required to **prevent** cyber security incidents, respond to them and restore business operations.

Reporting

Identifies the procedure for **reporting** to DGov.

Seeking Exemption

Identifies the procedure for **seeking exemption** from any aspect of this Policy.

Development

Outlines the required approach to entities' cyber security **capability development.**

Best Practice

Promotes **best practice** in cyber security procurement .

Context

This Policy is strategically aligned with:

- WA Whole of Government Cyber Security Incident Coordination Framework (WA WoG CSICF), which sets out a structured process for cyber security incident management and response in WA Government
- Other WA Government information security frameworks and initiatives.

Entities captured under the Security of Critical Infrastructure Act 2018 (Cwlth) can now use this Policy as one of the recognised SOCI reporting frameworks.

Legislation and guidance relevant to this Policy include, but are not limited to:

- Section 56 of the Financial Management and Accountability Act 1997 (Establishment of the Office of GCIO)[2]
- Public Sector Management Act 1994
- State Records Act 2000
- Government Trading Enterprises Act 2023
- Privacy Act 1988 (Cth)
- Security of Critical Infrastructure Act 2018 (Cth)
- Data Availability and Transparency Act 2022 (Cth)
- WA Information Classification Policy
- WA Data Offshoring Position.

This Policy supersedes WA Government Cyber Security Policy (2021).

The requirements of this Policy are aligned with the advice from the Australian Cyber Security Centre (ACSC) and the Cyber Security Framework developed by the United States NIST 2.0.[3]

2 Now repealed and replaced by *Public Governance, Performance and Accountability Act 2013* (Cth).

3 Draft NIST Cybersecurity Framework 2.0 Core: https://www.nist.gov/cyberframework/framework.

2024 WA Government 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

The Policy applies to:

- WA Public Service as defined in the Public Sector Management Act 1994
- Schedule 1 agencies as defined in the Public Sector Management Act 1994, specifically:
  - the WA Police Force
  - Health Service Providers (as defined in the Health Services Act 2016)
  - WA Technical and Further Education (TAFE) colleges
  - Gold Corporation and Goldcorp Australia
  - Racing and Wagering Western Australia
  - Western Australian Land Authority
  - Department of the Staff of Parliament
  - WA Universities (Curtin University, Edith Cowan University, Murdoch University, The University of Notre Dame, The University of Western Australia)
  - all WA Government Trading Enterprises (GTEs), regardless of whether included in the Scope of the GTE Act 2023 and regardless of whether included in the scope of the Security of Critical Infrastructure Act 2018 (Cwlth).
- Schedule 2 Senior Executive Service (SES) entities as defined in the Public Sector Management Act 1994.
- Local Government and other WA Public Service entities not specified in the Scope are also encouraged to comply with the provisions of this Policy.

Roles and responsibilities

The Accountable Authority

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

- the entity's cyber security risk management
- implementation of cyber security prevention measures for the entity, and
- responding to cyber security incidents affecting the entity.

The Cyber Security Unit

Office of Digital Government, Department of the Premier and Cabinet (DGov) is responsible for:

- supporting the entities included in the scope of this Policy to establish and improve their cyber security measures
- improving the visibility of cyber security threats, vulnerabilities and controls across the WA Government sector
- coordinating inter-agency operational responses to cyber security incidents
- leading cyber security engagement with the ACSC and interjurisdictional counterparts in line with Cyber Incident Management Arrangements for Australian Governments (CIMA)
- setting a baseline standard for cyber security risk management in Government procurement practices
- providing cyber security advice to entities included in the scope of this Policy.

The Government Chief Information Officer (GCIO)

Is responsible for:

- oversight of DGov
- strengthening cyber security and digital transformation
- provision of whole-of-government policy leadership, advice and direction on digital transformation, cyber security and incident prevention and management.

1. Govern

Establish essential governance and foundations of cyber security management.

1.1 Accountable Authority

The Accountable Authority (DG, CEO or chief employee) of an entity is accountable for the entity's risk management, including cyber security risk management. The Accountable Authority must:

a. Manage the entity's cyber security risks.
b. Allocate executive responsibility for cyber security.
c. Consider the implications of their entity's cyber security risk management decisions on other WA entities and share information on risks with DGov where appropriate.
d. Allocate adequate resources to implement this policy and ensure the continuity of its implementation.

1.2 Cyber Security Executive

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

a. Have executive authority to implement this Policy.
b. Have or allocate adequate skills and resources to implement this Policy and ensure the continuity of its implementation.
c. Report to the Accountable Authority on the implementation of this Policy.
d. Notify the Cyber Security Unit of the Office of Digital Government (cyber.policy@dpc.wa.gov.au) within 5 days if the Cyber Security executive for their agency has changed.

1.3 Cyber Security Operations

Each entity must ensure sufficient technical cyber security capability (HR) is available to implement this Policy and ensure the continuity of its implementation.

1.4 Cyber Security Governance

Each entity must establish governance of cyber security for their entity, which has considered:

a. alignment of cyber security to the entity's purpose and business strategies
b. visibility of cyber security risks
c. the current state of the entity's cyber security maturity and its cyber security objectives
d. adequate oversight and management over third-party arrangements
e. sufficient and appropriate plans to manage the implementation of the policy
f. planning for business continuity, response and recovery following a significant cyber security incident
g. obtaining assurance over the implementation of cyber security controls in the entity, including ACSC controls.[4]

For more information, please see:

- Security governance | Protective Security Policy Framework

1.5 Data Offshoring Governance

Each entity must define and understand its risks associated with data offshoring, with reference to:

a. the WA Government Data Offshoring Position and Guidance
b. Public Cloud Risk Assessment Guidance
c. Western Australian Information Classification Policy.

For more information, please see:

- Western Australian Government Offshoring Position and Guidance
- Public Cloud Risk Assessment
- Western Australian Information Classification Policy

4 The Australian Signals Directorate's ACSC leads the Australian Government's efforts on cyber security. It brings together capabilities to improve the cyber resilience of the Australian community and help make Australia the most secure place to connect online.

1.6 Secure Device Disposal Governance

Each entity must maintain oversight of the secure disposal of devices, computers or media that hold digital information.

For more information, please see:

- How to dispose of your device securely | Cyber.gov.au

1.7 Vulnerability Management

Each entity must implement governance of vulnerability management to identify and remediate cyber vulnerabilities in a timely manner.

1.8 Vulnerability Disclosure Program

Each entity must implement a vulnerability disclosure program.

For more information, please refer to:

- WA Vulnerability Disclosure Policy
- ACSC – Vulnerability Disclosure Programs Explained

1.9 Whole-of-Government Cyber Security Advice and Direction

Each entity must:

a. Comply with whole-of-government advice and direction on cyber security or any related matter issued by the GCIO or apply for an exemption.

b. Consider cyber threat intelligence and advice provided by DGov.

2. Identify

Develop organisational understanding to manage cyber security risks.

2.1 Cyber Security Context

To understand its cyber security context as a basis for sound cyber security decision-making, each entity must maintain an inventory of their ICT environment, including:

a. devices, servers and other ICT equipment
b. application systems and servers
c. critical databases and information assets
d. any relevant personnel and third-party providers
e. any social media applications used within the entity
f. system dependencies and related risks
g. its known future cyber security needs
h. any relevant legal and regulatory requirements.

2.2 Cyber Security Risk Management

The purpose of the Risk Management process is to guide the entity's assessment, understanding and management of cyber security risk to its staff, operations (including its mission, functions, image and reputation) and organisational assets, including digital information.

The initial risk assessment should be conducted with reference to this clause, or, additionally where required, to a more detailed recognised risk management framework applicable to cyber security, and take account of:

a. the entity's broader risk framework
b. the entity's cyber security context
c. any known vulnerabilities and threats
d. critical information managed by the entity
e. any responsibilities shared with third-party service providers of managed services
f. any procurement and supply chain risks.

Risk should be re-assessed whenever new systems or services are implemented, the risk posture or the threat level changes, or when there are major changes to entities' operating environments.

For more information, please see:

- Cyber security risk management framework – NCSC.GOV.UK
- NIST Risk Management Framework | CSRC
- NIST Risk Management framework Special Publication 800-30 Revision 1 Guide for conducting risk assessments
- International Standard ISO 31000
- Risk Management

3. Protect

Protect critical services and information holdings.

3.1 Australian Cyber Security Centre (ACSC) Controls

3.1.1 The "Essential Eight"

Each entity must:

a. Implement the set of technical controls comprising the ACSC's Essential Eight controls to Maturity Level One as defined by ACSC in November 2022 as the minimum baseline maturity level and continue to Maturity Level Two where appropriate.

b. Based on its cyber security risk assessment, the entity should decide whether the entity requires a level of maturity higher than Level One for any of the Essential Eight controls to manage its cyber security risks.

For more information, please refer to:

- ACSC – The Essential Eight
- ACSC – Essential Eight Maturity Model

3.1.2 The "Further Five"

In addition to the "Essential Eight", each entity must implement the "Further Five" mitigation strategies,[5] unless your entity's cyber security risk assessment determined that they were not required.

The Further five include:

1. server application hardening
2. block spoofed emails
3. network segmentation
4. continuous incident detection and response
5. personnel management.

For more information, please refer to:

- ACSC – Strategies to Mitigate Cyber Security Incidents

5 The term "Further Five" is refers to a set of risk mitigation strategies from ACSC's Strategies to Mitigate Cyber Security Incidents, prioritised by DGov based on new information on WA-specific threat context.

3.1.3 Additional controls

Based on the entity's cyber security risk assessment, each entity must decide whether it requires the implementation of the following to manage its cyber security risks:

a. any remaining ACSC controls
b. any additional controls, including any operational technology systems.

For more information, please refer to:

- ACSC – Strategies to Mitigate Cyber Security Incidents

3.2 Cyber Security Training

Each entity must ensure that its personnel 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 Cyber Secure Enterprise Mobility including Overseas Travel

Each entity must develop the capability to monitor and manage corporate-issued and BYO mobile devices[6] and harden applications residing on them from threats, including during overseas business travel.

Entities should consider advice from the Department of the Premier and Cabinet's Office of State Security and Emergency Management (OSSEM) on the level of security recommended for travel to specific countries.

For more information, please refer to:

- ACSC guidelines for Enterprise Mobility
- DGov Overseas Travel Guidelines

(please contact cyber.policy@dpc.wa.gov.au to request)

6 The term Bring-Your-Own (BYO) device refers to personally owned devices used for both private and business purposes.

3.4 Information Secure Procurement

Each entity must consider information security risks when procuring any goods or services involving access to digital information.

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

3.4.1 Procurement risk management

Each entity must consider information security risks as a part of their procurement and contract risk assessment. This consideration must be informed by ACSC Procurement Guidelines, ACSC Supply Chain Risk Management, ACSC Guidelines for Software Development.

Prior to procurement, each entity must:

a. Perform a risk assessment taking into consideration how the procurement may impact confidentiality, integrity and availability of the entity's operations, as well as the sensitivity of the information in the scope of the proposed procurement.
b. Conduct due diligence on any suppliers' information security maturity, including, where appropriate, whether the supplier has been independently assessed or certified against information security industry standards.[7]
c. Assess any supply chain risks which may impact the security of the entity's information.
d. Consider software security in software procurement or when undertaking software development and integration by the entity.
e. For high-risk procurements involving managed service providers and/or cloud service providers, give preference to supplier offerings which have undergone an independent assessment by a qualified assessor under the ACSC Infosec Registered Assessors Program (IRAP) or similar industry certification.
f. Understand the shared responsibility model between the supplier and the entity under which services are being contracted and managed.[8]
g. Ensure the supplier and their subcontractors have adequate insurance arrangements commensurate with the potential risks, including but not limited to General Liability, Professional Indemnity, Product Liability and Cyber Risk.
h. Consider the WA Data Offshoring Position.

7 Such as Information Security Registered Assessors Program (IRAP) and relevant ISO 27000 series certification or System and Organisation Controls (SOC) 2 certification.

8 Software-as-a-service (SaaS), platform-as-a-service (PaaS), infrastructure-as-a-service (IaaS), self-managed or another model.

For more information, please see:

- DGov Procurement and Supply Chain Risk Management Guidelines for WA Government
- ACSC Guidelines – procurement and outsourcing
- ACSC Cyber Supply Chain Risk Management
- ACSC Cloud Computing Security for Tenants
- ACSC Guidelines for Software Development
- WA Data Offshoring Position
- Information security registered assessor program (IRAP)
- RiskCover insurance

3.4.2 Contract clauses promoting information security

Each entity must include information security clauses for procurements involving government information.

In drafting the relevant clauses, the entity should consider DGov Procurement and Supply Chain Guidelines, ACSC Procurement Guidelines, ACSC Supply Chain Risk Management, ACSC Guidelines for Software Development and DGov Procurement Guidelines.

The clauses should include requirements for:

a. Service providers to report any cyber security incidents to the entity within 24 hours of detection.[9]
b. Suppliers maintain relevant information security certifications for the duration of the contract.
c. Entity information is adequately secured for the duration of the contract.
d. Secure disposal, or transfer back to the entity, of entity information at the termination of the contract.
e. Penalties or early termination of the contract in the event of failure to meet information security requirements.
f. Any other pertinent clauses as prescribed in the ACSC Guidelines for Procurement and Outsourcing – Contractual security requirements for service providers.

For more information, please refer to:

- DGov Procurement and Supply Chain Risk Management Guidelines for WA Government
- ACSC Guidelines – procurement and outsourcing
- ACSC Cyber Supply Chain Risk Management

9 NIST Computer Security Resource Center Glossary defines cyber security incident as "an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies."

- ACSC Cloud Computing Security for Tenants
- ACSC Guidelines for Software Development
- WA Data Offshoring Position
- Information security registered assessors program (IRAP)
- RiskCover insurance
- Information and Communications Technology Services CUAICTS2021 (www.wa.gov.au)

3.5 Physical Security of Assets

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

3.6 Identity and Access Management

Each entity must implement appropriate management, monitoring and review of its user, customer and system accounts to prevent 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
d. alignment to WA Government Authentication Guidelines
e. use of a protective domain naming system
f. improvement of networking controls.

For more information on identity and access management, please refer to:

- DGov Authentication Guidelines
- Microsoft Passwordless Authentication
- ACSC Strategies to Mitigate Cyber Security Incidents
- ACSC Gateway Security Guidance Package: Gateway Technology Guides
- ACSC Guidelines for Networking

3.7 Cyber Security Insurance

Each entity must consider cyber security insurance. The insurance should include:

a. first-party coverage, for losses incurred by the entity as a result of a cyber security incident
b. third-party coverage, for liability claims against the entity incurred as a result of a cyber security incident.

4. Detect

Detect and diagnose a cyber security incident.

4.1 Adverse Event Analysis

Each entity must ensure that the likelihood and potential impact of an adverse cyber security event[10] is well understood, specifically:

a. Ensure that adverse events are analysed to find and characterise possible attacks and compromises, and potential cyber security incidents are escalated for triage.
b. Review adverse events at least every 24 hours within normal operational periods as a part of its standard operating procedures and report any potential cyber security incidents.
c. Understand the potential impact of adverse events.
d. Share any threat intelligence with DGov within 24 hours of acquiring it, to practice good citizenship and promote broader cyber security in WA Government.

4.2 Continuous Monitoring

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

a. Establish a Security Information and Event Management System (SIEM) solution with a continuous incident detection and response system for its assets and networks.
b. Align to DGov's Mitre Attack Data Sources baseline for data sources and detections.
c. Facilitate the transfer of cyber security incident information from the entity SIEM to DGov's Security Operations Centre (SOC), preferably through direct integration with a fall back to delegated access as needed.

For more information on continuous monitoring, please refer to:

- Continuous incident detection and response in ACSC Strategies to Mitigate Cyber Security Incidents
- DGov's MITRE ATT&CK Data Sources

10 Activity with a potential negative impact on cyber security of an entity.

5. Respond

Respond to an identified cyber security incident.

5.1 Cyber Security Incident Management and Response Plan

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

a. is readily available to be executed in the event of a cyber security incident
b. requires the entity to triage incidents and develop an appropriate response within 4 hours
c. includes a process for reporting any confirmed cyber security incident to DGov within 24 hours of detection
d. includes a process for reporting relevant cyber security incidents to ACSC through ReportCyber within 24 hours of detection
e. aligns to the WA CSICF and the ACSC Cyber Security Incident Response Plan Guidance and Template.

For more information, please refer to:

- ACSC Cyber Incident Response Plan Guidance & Template
- US Cyber Security Infrastructure Security Agency (CISA) Cyber security Incident and Vulnerability Response Playbooks

5.2 Cyber Security Exercises and Testing

Each entity must perform annual cyber security incident response testing.

5.3 Ransomware Position

The Western Australian Government does not support the payment of ransoms. The Security and Emergency Committee of Cabinet (SECC) is the only WA Government body that can approve a ransom payment.

Any ransom demands related to cyber incidents should be referred to the Cyber Security Unit, Office of Digital Government and the WA Police Force.

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 restore their services and information within the timeframes as defined by the entity's Business Continuity Plan or Incident Management Plans.

6.2 Response Lessons Learned

Following a significant cyber security incident or cyber crisis (as defined in the WA WoG CSICF), and once response is complete, each entity must review response lessons learned and create a Post Incident Review (PIR) report, and where appropriate include its findings in the entity's Business Continuity and Recovery Plan.

The PIR must be shared with the Office of Digital Government within 20 working days from the date the cyber incident was detected.

Exemptions

If unable to comply with any of the requirements of this policy, GCIO issued advice or directions, an entity may seek an exemption by contacting DGov and providing a justification for the proposed exemption.

Exemption applications will be considered by the Chief Information Security Officer on a case-by-case basis.

Exemptions will be granted only if deemed justified by the agency's circumstances. The entity's exemption application should include:

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

Reporting

Entities must respond to Annual Implementation Report (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. The request for AIRs will be issued during the fourth quarter of each calendar year.

Entities captured by the SOCI Act 2018 should nominate WA Cyber Security Policy as a recognised cyber security framework under the SOCI Act. In this case, AIRs can be used to report to the Commonwealth Government as well as DGov, eliminating reporting duplication.

This Policy acknowledges that entities captured by the SOCI Act 2018 may wish to keep pre-existing cyber security control frameworks reporting obligations. These will be considered in lieu of AIRs to reduce reporting duplication.

Review

This Policy will be reviewed and updated every two years or as required. It may be reviewed earlier by decision of the Cabinet, the Premier, or the Minister for Innovation and the Digital Economy.

Additional Resources

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

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