GOVERNMENT OF
WESTERN AUSTRALIA

Western Australian Government Cyber Security Policy

Overview

2024

Introduction

The 2024 Government of Western Australia's Cyber Security Policy (the Policy) specifies the measures WA Government entities are required to undertake to prevent a cyber security incident, respond to an incident and restore business operations. The Policy prescribes a minimum baseline of cyber security controls for entities to implement with additional controls to be selected by each agency using a risk management approach that appropriately reflects its cyber security profile.

Entities captured under the Security of Critical Infrastructure Act 2018 (Cwlth) can use this Policy as an equivalent framework for the purpose of reporting on their cyber and information security hazard to the Department of Home Affairs as per section 8(5) under Security of Critical Infrastructure Risk Management Program Rules (LIN23/006).

For more information, please contact cyber.policy@dpc.wa.gov.au

Supersedes

This Policy replaces the 2021 WA Government Cyber Security Policy.

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 Sector entities not specified in the Scope are also encouraged to comply with the provisions of this Policy.

Requirements and Exemptions

High level policy requirements are outlined in the diagram on the next page, with additional detail available in the full Policy document.

An agency may seek an exemption for select requirements of this Policy. Exemptions will be made on a case-by-case basis, with entities required to demonstrate they have sufficient compensating controls in place to mitigate the specific threats the Policy requirement/s are designed to address.

Entities in the scope of the Policy are required to submit an Annual Implementation Report (AIR) within the time-period identified by the Office of Digital Government (DGov), between December and March each year. AIRs detail an entity's progress in the implementing of the Policy. The AIR must be approved by the agency's Accountable Authority.

Policy Timetable

Requirement Due Date	Requirement Description
Q2 2024	Cabinet Approves the 2024 Policy
December 2024	Security and Emergency Committee of Cabinet endorsed deadline to implement the Australian Cyber Security Centre's (ACSC) Essential Eight controls to Maturity Level One as defined by ACSC in November 2022.
TBA	Entities submit their AIR against the 2024 Policy requirements.
Q2 2025 (onwards)	Policy Review Period

1 Govern

Establish essential governance and foundations of cyber security management.

- Accountable Authority
- Cyber Security Executive
- Cyber Security Operations
- Cyber Security Governance
- Data Offshoring Governance
- Secure Device Disposal Governance
- Vulnerability Management
- Vulnerability Disclosure Program
- Whole-of-Government cyber security advice and direction

2 Identify

Develop organizational understanding to manage cyber security risks.

- Cyber Security Context
- Cyber Security Risk Management

3 Protect

Protect critical services and information holdings.

- ACSC Security Controls
- Cyber Security Training
- Cyber Secure Enterprise Mobility including Overseas Travel
- Information Secure Procurement
- Physical Security of Assets
- Identity and Access Management
- Cyber Security Insurance

4 Detect

Detect and diagnose a cyber security incident.

- Adverse Event Analysis
- Continuous Monitoring

5 Respond

Respond to an identified cyber security incident.

- Cyber Security Incident Management and Response Plan
- Cyber Security Exercises and Training
- Ransomware Position

6 Recover

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

- Response Lessons Learned