GOVERNMENT OF
WESTERN AUSTRALIA

Department of **the Premier and Cabinet**
Office of Digital Government

WA Government Cyber Security Policy

Policy Overview

2021

Introduction

The Government of Western Australia's Cyber Security Policy specifies the measures WA Government agencies are required to undertake to manage their cyber security risks. This Policy prescribes a minimum baseline of cyber security controls for agencies to implement with additional controls to be selected by each agency using a risk management approach that appropriately reflects its cyber risk profile.

Supersedes

The Policy replaces the:

- WA Government's Digital Security Policy (2016)
- Public Sector Commissioner Circular 2010-05: Computer information and internet security, and
- The Security and Emergency Committee of Cabinet (SECC) Top 5 Controls

Scope

The proposed Policy is intended to apply to the:

- WA Public Sector (as defined in the Public Sector Management Act 1994)
- WA Police Force
- Health Service Providers (as defined in the Heath Services Act 2016)
- TAFE colleges

Other WA Government organisations (for example, Government Trading Entities) are also encouraged to comply with the provisions of the Policy.

Requirements and Exemptions

High level policy requirements and 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 only be approved if justified by the agency's circumstances. Each decision will be made on a case-by-case basis.

Reporting

Agencies must develop an Annual Implementation Report and provide it to the Office of Digital Government once approved by the agency's accountable authority. Baseline reporting will be due in early 2022, with full reporting undertaken later in the year. See below for a proposed timeline.

- Role of the Accountable Authority in leading cyber security
- **Appointment of a Security Executive**

- Understand organisational Cyber Security Context
- **Assess cyber risk**
- Plan to manage cyber risk

- **Integrate Cyber Security into Business Continuity Planning**
- Ensure adequate cyber security Insurance coverage to manage impact.
- Review and share lessons learnt from incident recovery.

Implement controls to manage risk:

- **Essential 8 Controls**
- **Strategies to Mitigate Cyber Intrusions**
- Vulnerability Management
- Secure Software Development
- Security Awareness
- Secure overseas travel
- **Supply Chain Security**
- Physical security of relevant assets
- Safe and secure disposal of digital assets

- Plan for how to respond to cyber incidents.
- Regularly test and exercise response plans.
- **Report incidents to the Office of Digital Government.**
- Review and share lessons learnt from incident response.

- Maintain event logs for critical systems
- Implement Intrusion Detection
- Process log data through a Security Information and Event Monitoring system.
- **Integrate with the Office of Digital Government SIEM.**

Policy Timeline