



# Premier's Circular

Number:	2022/03
Issue Date:	26/08/2024
Review Date:	30/06/2025

## TITLE

### CYBER SECURITY MEASURES FOR WA GOVERNMENT ENTITIES

## POLICY

The strengthening of cyber security in WA Government is a key priority of the *Digital Strategy for the Western Australian Government 2021-2025 / 2026-2030*.

This Circular applies to:

- WA Public Sector as defined in the *Public Sector Management Act 1994* (WA).
- Schedule 1 entities as defined in the *Public Sector Management Act 1994* (WA), specifically:
  - The WA Police Force
  - 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* (Cth)
- Schedule 2 Senior Executive Service (SES) entities as defined in the *Public Sector Management Act 1994* (WA).
- Health Service and Health Service Providers (as defined in the *Health Services Act 2016* (WA)).

- Local Government and other entities not specified in the Scope are also encouraged to comply with the provisions of the Policy.
1. Implementation of the 2024 *Western Australian Government Cyber Security Policy* (the Policy)
    - The Policy sets standards and measures to manage cyber security risks.
    - Entities must:
      - Implement the Policy,
      - Connect to the Office of Digital Government (DGOV) Security Operations Centre, and
      - Report annually on the implementation of the Policy to DGOV.
  2. Compliance with *Western Australian Whole-of-Government Cyber Security Incident Coordination Framework* (Framework)
    - The Framework sets coordination measures for cyber incident response.
    - Entities must:
      - Incorporate the Framework into their cyber incident response planning, and
      - Report cyber incidents to the WA Government Cyber Security Incident Reporting Portal.
  3. Provision of Office of the Auditor General's (OAG) audit findings to DGOV
    - The OAG audits how entities manage confidentiality and integrity of information systems.
    - Entities must provide a copy of their management letters and their response to OAG findings to DGOV within 7 days of responding to the OAG.

## **BACKGROUND**

Government is dependent on reliable and secure digital systems to provide public services and protect valuable information.

Compliance with 2024 Western Australian Government Cyber Security Policy and Western Australian Whole-of-Government Cyber Security Incident Coordination Framework protects the integrity of WA Government information systems reduces cyber security risk and improves cyber security resilience of WA Government entities.

Roger Cook MLA  
**PREMIER**

For enquiries contact:	6551 3925 Chief Information Security Officer Department of the Premier and Cabinet
Other relevant Circulars:	N/A
Circular/s replaced by this Circular:	N/A