Government of **Western Australia**
Office of the **Government Chief Information Officer**

Whole-of-Government
Digital Security Policy

Document Control

The Western Australian Whole of Government
Digital Security Policy: Version 2 – 13 June 2017

Produced and published by: Office of the Government Chief Information Officer

Acknowledgements: The Policy was developed in collaboration with Western Australian public sector agencies.

Contact: Office of the Government Chief Information Officer

2 Havelock Street

WEST PERTH WA 6005

Telephone: (08) 6551 3901

Email: policy@gcio.wa.gov.au

Document version history

Date	Author	Version	Revision Notes
May 2016	Office of the GCIO	1	First Release
June 2017	Office of the GCIO	2	Second Release

1. Purpose

The purpose of the Western Australian whole -of-government Digital Security Policy (the Policy) is to provide direction for Western Australian public sector agencies in adequately managing their digital security risks.

2. Scope

The scope of the Policy is the management of digital information security risks.

Digital information security goes hand-in-hand with broader information security and agencies must consider broader aspects such as personnel and physical security in their compliance activities.

3. Objectives

The Digital Security Policy has the objective of enabling agencies to better ensure the confidentiality, integrity and availability of their digital information. This objective will be achieved by agencies:

- integrating digital security governance within their overall corporate risk management practices;
- identifying their digital security risk exposure;
- incorporating appropriate controls that will enable them to treat those risks; and
- taking a managed, systematic approach.

4. Definition of Terms

Defined terms are as per *ISO 27000: Information Technology – Security techniques – Information Security Management Systems – Overview and vocabulary*.

Additional references used are defined as below:

Digital Security
Digital security ensures the confidentiality, availability and integrity of digitally stored information. Digital security involves the application and management of appropriate controls by considering a wide range of threats, with the aim of ensuring sustained business success and continuity, and minimizing consequences of digital information security incidents.

Information Security Management System (ISMS)
A systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives.

An ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets.

5. The Risk Management Context

Digital security is primarily a risk management activity. Western Australian government agencies have risk management obligations (see *Section 6: Relevant Policy Obligations*), and generally have governance arrangements to enable them to meet these obligations.

Agencies can only make informed decisions regarding risk once they are aware of them. A risk-based decision making approach to digital security, within the oversight of the peak corporate risk management body, enables agencies to ensure that digital security is appropriately planned, implemented and resourced within business needs and risk appetite.

6. Policy Requirements

The requirements of the Digital Security Policy are as follows:

Policy Requirement One: Implement an Information Security Management System

Agencies must implement a system for managing their information security risks.

This ISMS must have the characteristics detailed in Policy Requirements two, three and four.

Agencies must ensure their ISMS is aligned with their broader risk management approach.

Policy Requirement Two: Governance and Accountability

Agencies must establish governance that details decision rights, roles, and accountability for managing digital information security risks.

Digital security must be linked to an agency's risk and ICT governance frameworks to ensure a consistent approach to risk and the highest level of executive support.

Policy Requirement Three: Assess and Treat Security Risks

Agencies must have a process that ensures assessment and appropriate treatment of digital security risks.

Agencies must ensure they are aware of the relevant risks they face. Appropriate steps must be taken to provide protection and assurance that digital security risks are being efficiently and effectively managed within the agency risk appetite.

Policy Requirement Four: Continuous Improvement

Agencies must ensure that digital security arrangements include formal mechanisms for continuous improvement.

Digital security arrangements must be routinely monitored, reviewed and tested.

Agencies must ensure that their risk management approach, and their digital security skills and capabilities, remain commensurate with a dynamic digital security threat environment.

7. Relevant Policy Obligations

The following list of Policy obligations is non-exhaustive, and exclusive of any legislative obligations.

Agencies are required to comply with this Policy as per *Premier's Circular 2016/03: Mandatory Implementation of Whole of Government Information and Communications Technology (ICT) Strategy and Associated Policies*.

> *All Western Australian state government agencies are expected to apply the principles and requirements contained within the strategy and policies into all current and future projects as well as normal operational procedures and practices.*

Public Sector Commissioner's Circular 2010-05: Computer Information and Information Security requires *agencies to ensure that they have policies and procedures in place to manage:*

- *General controls of computer systems;*
- *The protection of personal and sensitive information;*
- *Network threats that aid in the spread of viruses and malicious software; and*
- *Laptops and Portable Storage Devices.*

The Public Sector Commission and the Department of Treasury also mandate the following generalised risk management obligations for the public sector.

Public Sector Commissioner's Circular: 2015-03 Risk Management and Business Continuity Planning stipulates that:

> *All public sector bodies should manage the risks associated with the activities performed by their organisation. This involves prudently conducting risk assessment processes to identify the risks facing organisations, being able to demonstrate the management of risks and having continuity plans to ensure they can respond to and recover from any business disruption.*
>
> *Public sector bodies should ensure policies and continuity plans are maintained to ensure they are up to date with the activities performed by their organisation.*

Treasurer's Instruction 825: Risk management and Security stipulates that the

> *Accountable authority shall ensure that:*
>
> *i. there are procedures in place for the periodic assessment, identification, and treatment of risks inherent in the operations of the agency; and*
>
> *ii. suitable risk management policies and practices are developed.*

The Policy seeks to provide a digital security specific supplement to these existing policy obligations.

8. Implementation

Implementation of the Policy will be a progressive and evolving process. It is not expected that agencies will immediately assume a fully mature implementation. Rather, agencies should assess their current capability and maturity, and where shortfalls are identified, develop a roadmap for achieving the requisite level of capability.

9. Reporting

Self-assessment of compliance with this Policy will be included within agencies' annual reporting requirements to the Office of the GCIO.

Agencies may also be assessed as part of the Auditor General's annual Systems Audit Report.

10. Supporting Material

Additional supporting material includes a Supplementary Guide, and practical tools and templates to assist in implementation. These are available from the whole of government website, wa.gov.au