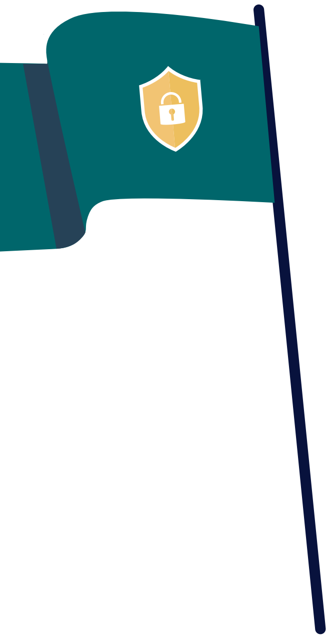
Government of **Western Australia**
Department of **the Premier and Cabinet**
Office of Digital Government

WA Government Cyber Security Policy



Produced and published by
Department of the Premier and Cabinet
Office of Digital Government

Published October 2021

Principal address:
Dumas House
2 Havelock Street
West Perth WA 6005

Postal address:
Locked Bag 3001
West Perth WA 6872

Telephone: (08) 6552 5000
Fax: (08) 6552 5001
Email: dgov-administrator@dpc.wa.gov.au

Acknowledgement of Country

The Government of Western Australia acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures; and to Elders past, present and emerging.

Contents

Version	Date	Who
1.0 Release	December 2021	Office of the Digital Government

Introduction

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

Cyber security refers to the measures used to protect the confidentiality, integrity, and availability of systems, assets, and information from cyber threats.[1] While cyber security risks cannot be completely 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.

The objective of this Policy is to improve the implementation of good fundamental cyber security practices in WA Government entities. Improving agencies' cyber resilience will make it much harder for adversaries to compromise government systems and will support more effective and efficient responses when they do.

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. Nothing in this Policy prevents an agency from moving to a higher level of cyber security maturity than the minimum requirements specified.

This Policy:

- outlines the strategic context for agencies' cyber security efforts;
- clarifies roles and responsibilities;
- mandates requirements for agencies;
- authorises an exemptions process for the requirements; and
- identifies reporting and review provisions.

This Policy complements agencies' other risk management obligations under:

- *Treasurer's Instruction 825: Risk Management and Security*; and
- *Public Sector Commissioner's Circular 2015-03: Risk management and business continuity planning*.

This Policy replaces the:

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

[1] Definition of cyber security adapted from Australian Signals Directorate definition of cyber security: "Measures used to protect the confidentiality, integrity and availability of systems and information." Available from: cyber.gov.au/ism/cyber-security-terminology

Scope

The proposed Policy is intended to apply to the WA Public Sector (as defined in the *Public Sector Management Act 1994)*, the WA Police Force, the Health Service Providers (as defined in the *Health Services Act 2016*), and the TAFEs. Other WA Government organisations are also encouraged to comply with the provisions of this Policy.

Context

The WA Government, like other governments and organisations worldwide, is dependent on reliable and secure digital systems and infrastructure to conduct its business and provide public services. The systems supporting these assets and services collectively hold a large amount of sensitive information and/or are critical for the effective delivery of Government services.

While the cyber realm is a critical enabler of Government business and service provision, it also acts as a vector through which malicious actors can cause harm. Cyber security threats are increasing in frequency, scale, and sophistication,[1] and adversaries are constantly looking for vulnerabilities and weaknesses in systems and networks.[2]

Advice from the Australian Government is that Australian governments and critical infrastructure providers continue to be targeted by highly sophisticated nation states and state-sponsored actors. These actors seek to obtain sensitive information and may seek to achieve disruptive or destructive effects.[3]

Cybercriminals, including transnational cybercrime syndicates, also target Australian organisations for financial gain.[4] Ransomware has become one of the most significant threats given the potential impact on business operations.[5]

The potential consequences of malicious cyber activity against the WA Government are significant. They include:

- information compromise (including loss of personal and other sensitive information);
- disruption to government infrastructure and services, and their associated impacts;
- interference with government systems;
- financial loss; and
- loss of public confidence in Government.

Many of the incidents, however, that are reported each year within the WA Government could have been avoided or substantially mitigated by good cyber security practices.

[1] Australian Cyber Security Centre, 2020, *ACSC Annual Cyber Threat Report: July 2020 to June 2021*, p 8.
[2] Ibid, p 37.
[3] Ibid, p 23.
[4] Australia's *Cyber Security Strategy 2020*, pp 12.
[5] *ACSC Annual Cyber Threat Report: July 2020 to June 2021*, p 9.

Roles and Responsibilities

Agencies own the cyber security risks for their organisation. They are responsible for:

1. assessing cyber security risks;
2. implementing their own cyber security measures; and
3. controlling their own responses to cyber security incidents.

The Office of Digital Government, Department of the Premier and Cabinet is responsible for:

1. coordinating and supporting improvements to cyber security resilience across the Government Sector;
2. improving visibility of cyber security threats, vulnerabilities and controls across the Government Sector;
3. coordinating inter-agency operational responses to cyber security incidents;
4. leading the State's inter-jurisdictional cyber security engagement; and
5. providing cyber security advice to Government.

ATTACK
Document hacking alert
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
0011010110100100 xx1la1 AAPP01
10 : 37 NSA
10 : 12 NSA
11 : 01 NSA
12 : 44 NSA
13 : 32 NSA
10 : 37 NSA
10 : 12 NSA
11 : 01 NSA
12 : 44 NSA
13 : 32 NSA
10 : 37 NSA
10 : 12 NSA
11 : 01 NSA
12 : 44 NSA
13 : 32 NSA
10 : 37 NSA
Shut down

Requirements

The requirements of this Policy are aligned with a modified version of the functional areas of the *Cyber Security Framework* developed by the United States National Institute of Standards and Technology (NIST). The six functional areas used in this Policy are: Lead, Identify, Protect, Detect, Respond and Recover.[1]

LEAD IDENTIFY PROTECT DETECT RESPOND RECOVER

Cyber Security Policy Requirements

1. Lead	
Purpose is to articulate who is accountable and manages the cyber risks of an organisation.	
1.1	**Accountable Authority**
	The chief executive officer/chief employee of an organisation is its accountable authority for cyber security. The accountable authority must: a. determine the organisation's tolerance for cyber security risks; b. ensure the organisation's cybersecurity risks are appropriately managed; c. consider the implications their cyber security risk management decisions have for other organisations (including non-government organisations) and share information on risks where appropriate; and d. appoint or assign an executive member of the organisation with the responsibilities or to the role of Cyber Security Executive.
1.2	**Security Executive**
	The Security Executive function: a. is responsible for managing the organisation's implementation of this Policy's requirements; b. must have the authority, skills and resources to manage implementation of this Policy's requirements; and c. is to report to the Accountable Authority on the implementation of this Policy's requirements.

[1] The NIST Cyber Security Framework has five categories/functions – Identify, Protect, Detect, Respond and Recover.

Cyber Security Policy Requirements

2. Identify	
Purpose is to develop an organisation's understanding to enable it to more effectively and efficiently manage its cyber security risks.	
2.1	**Cyber Security Context**
	Each organisation must establish its cyber security context to inform its cyber security decision-making. Organisations must: a. inventory the physical devices and systems within the organisation; b. inventory the software platforms and applications within the organisation; c. catalogue the external information systems used by the organisation; d. identify critical functions and system dependencies for the delivery of the organisation's services; e. understand the organisation's legal and regulatory requirements regarding cyber security (including privacy obligations); and f. identify suppliers and third-party partners of information systems, components and services.
2.2	**Risk Assessment**
	Each organisation must conduct a cyber security risk assessment at least once per annum. • The purpose of this assessment is to develop and maintain the organisation's understanding of cyber security risk to its operations (including its mission, functions, image and reputation), organisational assets (including information) and individuals. • This risk assessment is to be conducted in accordance with one or more recognised risk management standards or frameworks applicable to cyber security.

Cyber Security Policy Requirements

2. Identify	
2.2	• The risk assessment must take account of: o its cyber security context (Requirement 2.1); o cyber threats (this includes annual national cyber threat reports developed by the Australian Cyber Security Centre and the *Annual WA Government Cyber Threat Assessment Report* developed by the Office of Digital Government); o the cyber vulnerabilities of the organisation's assets; o the criticality of the services the organisation provides; o the sensitivity of the organisation's information holdings; o how the organisation's assets are used; o cyber-related supply chain risks; and o potential impacts/consequences of cyber security incidents.
2.3	**Risk Management** Each organisation must develop a cyber security risk management strategy that is approved by the accountable authority. The strategy must: a. identify the organisation's cyber security priorities, constraints, risk tolerances, and assumptions (to support operational risk decisions); and b. establish cyber security risk management processes.

Cyber Security Policy Requirements

3. Protect	
Purpose is to develop and implement appropriate safeguards to ensure delivery of critical services and protect information.	
3.1	**Essential Eight Controls**
	Each organisation must implement a baseline set of technical controls comprising the Australian Cyber Security Centre's (ACSC's) Essential Eight controls and password filtering. a. The Essential 8 controls must be implemented to Maturity Level One. b. Password filtering must be implemented for all user accounts.
3.2	**Additional Controls**
	Each organisation must decide, based on its cyber security risk profile (Requirements 2.2 and 2.3): a. if a higher level of maturity for any or all of the Essential Eight controls will be implemented; b. which of the other controls in the ACSC's Strategies to Mitigate Cyber Security Incidents will be implemented; and c. what, if any, additional controls will be implemented for the organisation's systems (including any operational technology systems); to effectively manage the organisation's cyber security risks.
3.3	**Vulnerability Management**
	Each organisation must develop and implement a cyber security vulnerability management process, which includes vulnerability disclosure, to identify and remediate cyber vulnerabilities in a timely manner.
3.4	**Secure Software Development**
	Each organisation must consider security in its software development, implementation and maintenance processes for traditional, mobile and web applications.
3.5	**Cyber Awareness & Training**
	Each organisation must ensure that the organisation's staff undertake basic cyber security awareness training on an annual basis with training for executives, finance/payroll staff, and other staff in sensitive positions being prioritised.

Cyber Security Policy Requirements

3. Protect

3.6 Overseas Travel

Each organisation must implement appropriate cyber security measures on the mobile devices of their staff travelling overseas that are used for business purposes. This includes:

a. both corporate-issued devices and bring-your-own-devices (used for business purposes); and

b. organisations consulting and considering advice from the Department of the Premier and Cabinet's Office of State Security and Emergency Coordination on the level of security recommended for travel to specific countries.

3.7 Secure Procurement Practices

Each organisation must incorporate cyber security requirements in its procurement practices for all digital goods including internet-of-things devices and services. This includes:

a. standard cyber security clauses in all new and extended IT contracts that, among other things, require third-party service providers to report cyber security incidents to the organisation;

b. new whole-of-government contracts applying the requirements of this Policy;

c. developing and implementing a cyber supply chain risk management approach that is informed by the ACSC's Cyber Supply Chain Guidance prior to undertaking the procurement process;

d. undertaking adequate due diligence on suppliers' IT controls, processes and standards to address cyber related risks at the time of contract formation and management; and

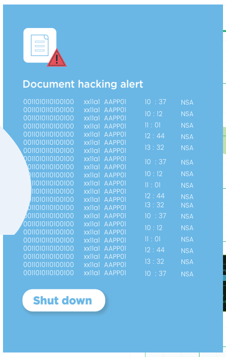
e. the assessment of cyber risks in any contract risk assessments.

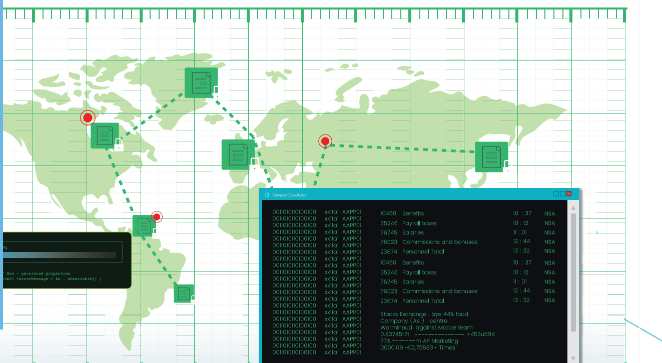
Agencies must develop a policy position regarding the offshoring of systems and data, in line with:

a. The WA Government Data Offshoring Position;

b. Western Australian Information Classification Policy; and

c. Any other regulations or Acts that apply to their data or operations.





Cyber Security Policy Requirements

3. Protect	
3.8	**Physical Security**
	Each organisation must ensure that physical access to relevant assets is managed and protected from unauthorised access and accidental damage.
3.9	**Secure Media Disposal**
	Each organisation must ensure that digital assets are disposed of in a way that appropriately safeguards the information held on these assets.

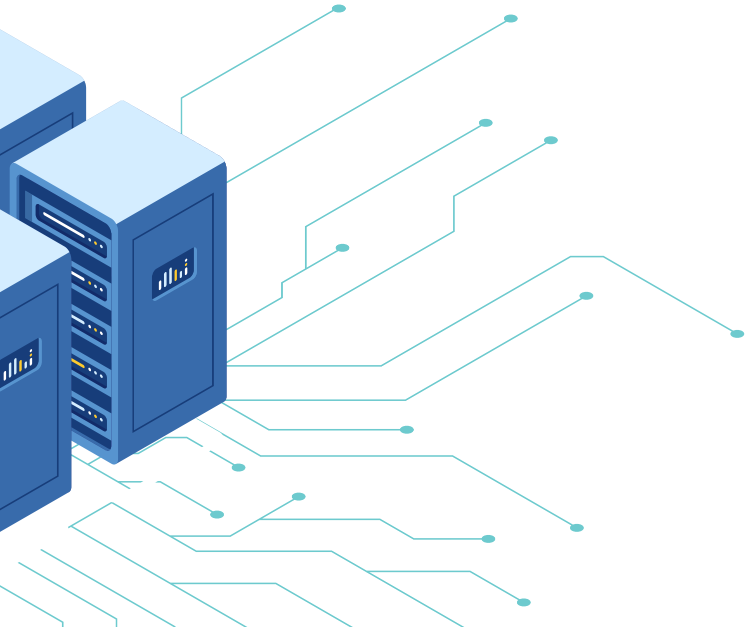
4. Detect	
Purpose is to develop and implement appropriate activities to identify the occurrence of a cyber security incident.	
4.1	**Event Logging**
	Each organisation must maintain event logs of critical systems.
4.2	**Intrusion Detection**
	Each organisation must implement intrusion detection mechanisms.
4.3	**Establishing SIEM**
	Each organisation must implement and manage a Security Information and Event Management system (SIEM) for its own networks.
4.4	**Connecting SIEM**
	Each organisation must connect its SIEM to the WA Government SIEM managed by the Office of Digital Government.
4.5	**Monitor & Analyse**
	Each organisation must have processes in place to monitor and analyse security events, and initiate action on suspected cyber security incidents.

Cyber Security Policy Requirements

5. Respond	
Purpose is to develop and implement appropriate response activities regarding a detected cyber security incident.	
5.1	**WA WoG Cyber Security Incident Coordination Framework**
	Each organisation must comply with its responsibilities in the Western Australian Whole-of-Government Cyber Security Incident Coordination Framework. These responsibilities include: • developing and exercising cyber security incident management/ response plans; • reporting cyber security incidents to the Office of Digital Government and the WA Police Force; and • supporting incident coordination arrangements.
5.2	**Ransomware Position**
	If the incident involves ransom-based crimes the affected organisation must notify the WA Police Force, Office of Digital Government, Riskcover and the State Solicitors Office for consultation and advice. The Government's general position is that ransom is not to be paid. Only Cabinet or the Security and Emergency Committee of Cabinet can approve a ransom payment.
5.3	**Response Lessons Learnt**
	Each organisation must review response lessons learnt following a significant cyber incident or cyber crisis (as defined in the Western Australian Whole-of-Government Cyber Security Incident Coordination Framework). a. The lessons learnt must be shared with the Office of Digital Government.

Cyber Security Policy Requirements

6. Recover	
Purpose is to develop and implement appropriate arrangements to restore any capabilities, services or information that are impacted by a cyber security incident.	
6.1	**Cyber aspects of Business Continuity Planning**
	Each organisation must incorporate recovery from cyber security incidents into its Business Continuity and Recovery Plan.
6.2	**Business Continuity Plan Testing**
	Each organisation must annually exercise/test the cyber security component of its Business Continuity and Recovery Plan.
6.3	**Cyber Insurance**
	Each organisation must have cyber insurance. This insurance must include: a. first-party coverage for losses/expenses incurred by the organisation due to a cyber security incident; and b. third-party coverage for liability claims against the organisation due to a cyber security incident.
6.4	**Recovery Lessons Learnt**
	Each organisation must review recovery lessons learnt following a significant cyber incident or cyber crisis (as defined in the *Western Australian Whole-of-Government Cyber Security Incident Coordination Framework*). a. The lessons learnt must be shared with the Office of Digital Government.



Exemptions

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.

Decisions about exemptions will be made by the Chief Information Security Officer, Office of Digital Government. Organisations seeking an exemption must contact the Office for advice and provide a justification for the recommended exemption before any decision is made.

Reporting

Each agency must develop an Annual Implementation Report on its implementation of this Policy. The Report must be approved by the agency's Accountable Authority.

Each agency must provide its Report to the Office of Digital Government. The Office will collate and analyse agencies' Reports and provide the Cabinet with a report on the Public Sector's implementation.

Annual Implementation Reports are due during the fourth quarter of each calendar year. Full reporting will commence in 2022. Baseline Reporting, consisting of only Requirements 3.1 and 3.2, will take place during Q1 of 2022.

Review

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

Supporting material

The Office of Digital Government will develop and provide supporting material (including templates) to agencies to assist their implementation of this Policy's requirements.

Further information

For further information about this Policy, visit the Office of Digital Government's website or email cybersecurity@dpc.wa.gov.au.