



Department of the Premier and Cabinet
Office of Digital Government

CYBER SECURITY EXECUTIVE

Guideline to support implementation of Western
Australian Government Cyber Security Policy clause 1.2
(Cyber Security Executive)





Produced and published by

Office of Digital Government
Department of the Premier and Cabinet
Published **January 2025**

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: Cyber.Policy@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.

Approval

Name / Title	Date
Peter Bouhlas Chief Information Security Officer	24 July 2024

Contact Officers

Name	Email	Phone
Danijela Kambaskovic-Schwartz	Danijela.Kambaskovic-Schwartz@dpc.wa.gov.au	+61 8 6552 6020
Sandra Franz	Sandra.Franz@dpc.wa.gov.au	+61 8 6551 3971



Contents

1. The relevant WA Government Cyber Security Policy clause	3
2. Overview	3
3. Cyber Security Executive Guidance.....	4
Organisational structure and communications.....	4
Cyber Security Strategic Planning and Governance	5
Cyber Security Risk Management	6
ICT Assets and Cyber Security Operations	7
Information Security	7
Personnel Security	8
Threat Detection.....	8
Incident Response.....	9
Whole-of-Government Advice	10
Annual Implementation Reporting.....	10
Requests for Information	10
Personnel Training	10
Capability Profile	11
Training Courses	11
Additional Resources	13



1. The relevant WA Government Cyber Security Policy clause

Domain 1, **Govern**

1.2 Cyber Security Executive

The Cyber Security Executive has the executive responsibility for cyber security of a WA Government entity. The person occupying the role must:

- have executive authority to implement the Policy;
- have or allocate adequate expert skills and resources to implement the Policy and ensure the continuity of its implementation; and
- report to the Accountable Authority on the implementation of the Policy.

Entities are required to notify the Cyber Security Unit of the Office of Digital Government (DGov) (cyber.policy@dpc.wa.gov.au) within 5 days if the Cyber Security Executive for their entity has changed.

2. Overview

The Western Australian Government Cyber Security Policy (the Policy) requires WA government entities to appoint a Cyber Security Executive.

The Cyber Security Executive:

- Possesses or delegates cyber security knowledge and expertise necessary to undertake a continuous program of development at the forefront of the entity's cyber security strategy
- Develops and maintains cyber security strategic plans and governance.
- Oversees the work of the entity's cyber security management and operations staff and the entity's implementation of WA Cyber Security Policy
- Provides expert support and reports on cyber security matters to the Accountable Authority of a WA Government entity (the Director General or CEO), who is accountable for the entity's risk management including cyber security risk management
- Leads their entity's liaison on cyber security matters with DGov and the Western Australian Whole-of-Government Security Operations Centre (WASOC), the relevant Whole-of-Government governance bodies (Business and Technology

Advisory Council – BATAC, Directors General ICT Council) and communities of practice (example DGov’s Cyber Security Working Group (CSWG) etc).

For more details on the capabilities required from a cyber security executive, please refer to [Executive Cybersecurity Leadership \[NICE Framework Work Role\] | NICCS \(cisa.gov\)](#)

3. Cyber Security Executive Guidance

Organisational Structure and Communications

Traditionally, cyber security activities have been confined to Information Technology teams, reporting through a Chief Information Officer (CIO) or equivalent. In addition to leading cyber security operations of an entity, the Cyber Security Executive role has a broader strategic focus in developing and maintaining cyber security governance as well as developing and maintaining an information security culture.

A Cyber Security Executive supports the Accountable Authority by providing strategic oversight of the work of cyber security operations staff (Figure 1).

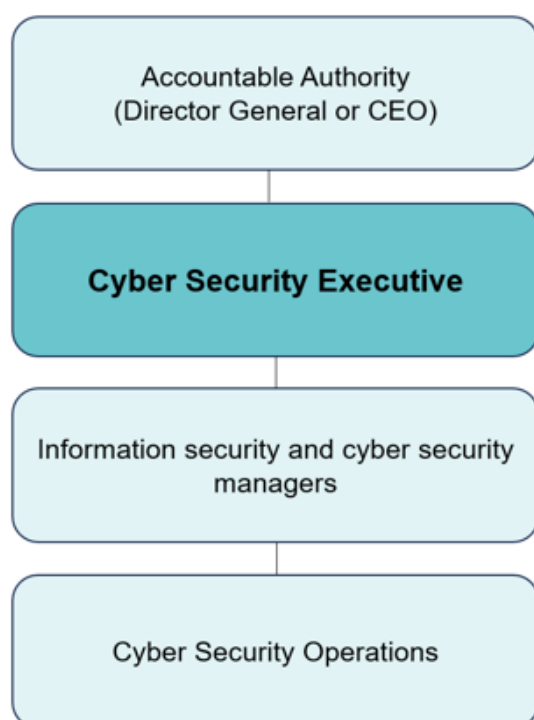




Figure 1. Position of a Cyber Security Executive within the organisational structure.

The Security Executive reports to the organisation’s Accountable Authority on cyber security matters. The reporting includes but is not limited to:

- 
- 
- The organisation's security risk profile within the broader threat context
 - Cyber security compliance with WA Government Cyber Security Policy
 - The status of key systems and any outstanding security risks or issues
 - Any planned cyber security uplift activities and relevant funding issues
 - The entity's ability to respond and recover from any cyber security incidents.

The Cyber Security Executive is a strategic executive manager who develops the entity's cyber security objectives across all lines of business within an entity as well as within the broader WA context. They oversee the entity's work across a number of strategic areas such as risk management, continuity and operations, incident response and management, communication and advocacy, and evaluation and reporting. They work closely with other entity executives, including risk, audit, and assurance functions (including Audit Committee), and liaise externally with their counterparts from other organisations, DGov, and may participate in forums like CSWG.

Cyber Security Strategic Planning and Governance

The Cyber Security Executive is responsible for establishing the entity's cyber security strategy and governance. This involves:



- Leading a structured process of developing the entity's cyber security strategy, policy and governance
- Developing and maintaining strategic plans that align cyber security priorities with the overall strategy of the entity
- Oversees the alignment of the entity's cyber security strategy, policy and governance to define and support the entity's cyber security and business continuity objectives (internal alignment)
- Oversees the alignment of the entity's cyber security strategy, policy and governance with WA Cyber Security Policy and other WA and Commonwealth legislation and guidance relevant to information security management (external alignment)
- Championing (effectively communicating the significance of) the information security governance to Accountable Authority, the executive team, the operation teams and all employees leading organisational and cultural change where required
- Overseeing the program of work to ensure continuous implementation of WA Government Cyber Security Policy.

- 
- 
- Leading the development of the entity cyber security risk management and cyber security governance for their entity using established information security frameworks
 - Leading the alignment of teams, business outputs and procurement processes to information security standards and processes
 - Leading the development, implementation and updating of the entity business continuity plan, incident response plan and disaster recovery plan
 - Leading the development, implementation and updating of the entity business continuity plan, incident response plan and disaster recovery plan.
 - In the event of a disaster, overseeing the implementation of the incident response and disaster recovery plans with the aim of improving business function resilience and ensuring the continued operation of critical business processes.

Cyber Security Risk Management

The Cyber Security Executive oversees information / cyber security risk management for their entity. This includes oversight of:

- The processes of identifying hazards / vulnerabilities and evaluating risk to entity's information security, operations and organisational assets, including:
 - Inventory of the entity's operations and organisational assets
 - Understanding of the broader risk landscape
 - Understanding of the cyber security risk context
 - Identifying any known cyber security vulnerabilities and threats
 - Understanding the confidentiality levels of the information managed by the entity
 - Understanding the entity's requirements in relation to availability and integrity of its information
 - Clarity on how the entity shares cyber security responsibilities with its suppliers
 - Reviews of the entity's supply chains and understanding risks to information security and operation disruption arising from the supply chains.

- 
- 
- Oversees the performance of a new risk assessment whenever new systems or services are implemented, the risk posture or the threat level changes, or when there are major changes to the entity's operating environments
 - Ensuring that the entity manages its supply chain risks, applying consistent vendor management processes across the entity, from discovery through to ongoing management.
 - Assists personnel to understand information security risks entering into contracts with suppliers and to assess and manage cyber supply chain risks.

ICT Assets and Cyber Security Operations



A Cyber Security Executive:

- Ensures oversight of the inventory of the entity's ICT environment, including critical databases and information assets
- Ensures that physical and digital access to information technology and cyber security assets is managed to prevent unauthorised use and physical damage
- Leading the development, implementation and updating of the entity's business continuity plan, including future ICT asset needs planning and budgeting for renewal
- Oversees the establishment of a Security Information and Event Management System (SIEM) solution with a continuous incident detection and response system for all the entity's assets
- Oversees continuous maintenance of the inventory, the security of assets and the SIEM.

Information Security

The Cyber Security Executive oversees information security management for their entity, including:

- The entity's implementation of the 2024 WA Government Cyber Security Policy
- Implementation of DGov's Information Security Risk Assessment Table
- The entity's implementation of relevant advice provided by Government Chief Information Officer, DGov, Australian Cyber Security Centre (ACSC) as required.

- 
- 
- Regular reviews and updating of their entity's information security and cyber security programs
 - Alignment of information security objectives with their organisation's strategic, operational, and budgetary processes.
 - Information secure procurement and supply chain management
 - Leading the development, implementation and updating of the entity incident response plan and disaster recovery plan
 - Leading the entity's cyber security incident exercising efforts

Personnel Security

The Cyber Security Executive oversees the process of screening and vetting of personnel and contractors working in cyber security in accordance with DGov's Information Security Risk Assessment Table and determines the level of vetting required for employees with privileged access to confidential information and sensitive systems.

The Cyber Security Executive is responsible for oversight of:



- an entity's personnel security activities aimed at mitigating the risk of unauthorised access to information at all stages of employment (pre-engagement, engagement, separation)
- the employees' use of social media in the context of WA government advice on the use of social media
- other activities as indicated by other whole-of-government or Commonwealth information security guidance on personnel risks.

The Cyber Security Executive oversees the process of recruiting adequately qualified cyber security operational staff to be employed at the entity.

Threat Detection

The Cyber Security Executive oversees threat detection activities and alignment with DGov's WASOC for their entity and is responsible for oversight of:

- Continuous monitoring, analysis and triage of security events and initiates action on suspected cyber security incidents

- 
- 
- Establishment and oversight of a SIEM solution with a continuous incident detection and response system for its assets and networks
 - Alignment to DGov's Mitre Attack Data Sources baseline for data sources and detections is required
 - Facilitating the onboarding of cyber security incident information from the entity's SIEM to DGov's SOC.

Incident Response

A Cyber Security Executive is responsible for oversight of the entity's response to cyber security incidents (cyber security events leading to compromise or a significant probability of compromise to their entity's business operations).

This includes ensuring that:

- Incidents are triaged and appropriately responded to within 4 hours
- Reporting any confirmed cyber security incident to DGov and through ReportCyber to the Australian Cyber Security Centre (ACSC) within 24 hours of detection
- Adherence of the entity to the Western Australian Cyber Security Incident Coordination Framework (WACSICF)
- The Cyber Security Incident Response Plan (CSIRP) for their entity is developed and regularly tested so that employees are aware of their roles and responsibilities in the event of an incident
- The entity is aware of the [ACSC Cyber Security Incident Response Plan \(CSIRP\) Guidance and Template](#) and utilising it as appropriate.
- In the event of a cyber security incident, the Cyber Security Executive leads the entity's incident response and participation in the coordination of the incident collaboratively with DGov and the Australian Cyber Security Centre.
- Cyber Security Executive reports any ransom demands to DGov Chief Information Security Officer (CISO). DGov will facilitate communication with the Australian Signals Directorate, Security and Emergency Committee of Cabinet (SECC) who is the only WA Government body that can approve a ransom payment.



Whole-of-Government Advice

The Cyber Security Executive oversees the entity's compliance with advice and direction of DGov's Government Chief Information Officer (GCIO) on cyber security related matters and considers cyber threat intelligence provided by DGov.

If unable to comply with DGov requirements or GCIO issued advice, the Cyber Security Executive oversees the entity's application for exemption to DGov.

Annual Implementation Reporting

The WA Government Cyber Security Policy (the Policy) requires entities to report annually on their progress in implementing the WA Cyber Security Policy. The entities' Annual Implementation Report (AIR) forms are kept in confidence and utilised by DGov to report to Cabinet and provide an understanding of the sector's cyber security maturity and develop programs of work to uplift cyber security in WA Government.

The Cyber Security Executive oversees the entity's Annual Implementation Reporting (AIR) process. Their signature certifies that AIR is:

- Completed using the template and by the deadline provided by DGov and
- Approved by the entity's Accountable Authority.

Requests for Information



The Cyber Security Executive oversees:

- Preparation of a timely response to requests for information issued by DGov
- Reporting of any threat intelligence to DGov
- Reporting of cyber security incidents to DGov's WASOC within 24 hours of detection.

Personnel Training

The Cyber Security Executive oversees the development and operation of their organisation's cyber security awareness training program. They should be able to foster positive security culture, where everyone understands importance of cyber security within the entity.

The Cyber Security Executive oversees the development and deployment of cyber security awareness training for all entity staff, as well as additional tailored cyber security training for staff in specialist positions, such as cyber security specialists,



executives, finance/payroll staff or staff with access to personal and sensitive information.

Capability Profile

While it is recognised that not all individuals will meet all requirements, the following criteria represent a list of desirable qualifications and experience for a person in a Cyber Security Executive role.



- It is recommended that a Cyber Security Executive be appointed at Tier 3 (Level 9) role. If you are considering appointing a cyber security executive at a lower tier, please discuss with DGov (cyber.policy@dpc.wa.gov.au)
- 10 to 15 years of experience in organisational and business strategy, IT strategic planning and risk management, classified or highly sensitive information and people development
- Previous experience in a Tier 4 (L8 or Director) role
- An undergraduate and a postgraduate degree or equivalent experience in a relevant field
- A proactive approach to understanding and addressing current and emerging cyber security threats
- Industry recognised training and certification or willingness to obtain them.

Please see the National Initiative for Cybersecurity Careers and Studies (NICCS) comprehensive overview of [Executive Cybersecurity Leadership](#) tasks, knowledges, skills and capability indicators.

Training Courses

The National Initiative for Cybersecurity Careers and Studies' (NICCS) [NICE Framework](#) for employers to develop their cybersecurity workforce is a recommended resource. Course topics should include but are not limited to:

- Executive core qualifications
- Managerial and operational workforce needs
- Conveying risk to stakeholders
- Technical
- Organisational behaviour and change

- 
- 
- Risk management training
 - Executive training
 - Information system security manager

Courses provided by the [SANS Institute](#) include:

- LDR419: Performing A Cybersecurity Risk Assessment
- LDR512: Security Leadership Essentials for Managers
- LDR514: Security Strategic Planning, Policy, and Leadership
- LDR521: Security Culture for Leaders
- LDR553: Cyber Incident Management

Microsoft offers [Chief Information Security Officer \(CISO\) Workshop Training](#) which contains a collection of security learnings, principles, and recommendations for modernizing security in an organisation is an additional resource.

The Australian Institute of Company Directors (AICD) and the Cyber Security Cooperative Research Centre (CSCRC) provide [Cyber Security Governance Principles](#) to assist Australian directors oversee and engage with management on cyber security risk. These principles are a helpful resource for Cyber Security Executives.

The International Organisation for Standardisation (ISO) provides Information Security certification. [ISO/IEC 270001](#) is a globally accepted standard for information security management systems (ISMS) and defines ISMS requirements. ISO/IEC 27001 provides guidance for establishing, implementing, maintaining, and continually improving an information security management system.

Australian universities offer Masters or Ph.D. level qualifications in the following areas:

- Cyber Security
- Computer science
- Computer information systems
- Business administration
- Information assurance
- Informatics

Assistance

If you require assistance developing an Executive Job Description Form (JDF) please contact cyber.policy@dpc.wa.gov.au.



Additional Resources

Additional resources for developing a Cyber Security Incident Operations can be found below:

- Australian Signals Directorate (ASD) - [Guidelines for Cyber Security Roles | Cyber.gov.au](#)
- [ACSC Cyber Security Incident Response Plan \(CSIRP\) Guidance and Template](#)
- ASD - [PROTECT - Cloud Computing Security for Executives \(January 2024\).pdf \(cyber.gov.au\)](#)
- Cyber Security Cooperative Research Centre - [Cyber Security Governance Principles - May 2024 \(aicd.com.au\)](#)
- Cybersecurity and Infrastructure Security Agency (CISA) - [Executives | Cybersecurity and Infrastructure Security Agency CISA](#)
- Department of Home Affairs - [Overview of Cyber Security Obligations for Corporate Leaders \(cisc.gov.au\)](#)
- DGov Cyber Security Executive JDF - cyber.policy@dpc.wa.gov.au.
- National Initiative for Cybersecurity Careers and Studies (NICCS) - [Executive Cybersecurity Leadership | NICCS \(cisa.gov\)](#)
- SANS Institute - [SANS Cybersecurity Leadership Training & Resources | SANS Institute](#)
- [Workforce Framework for Cybersecurity \(NICE Framework\) | NICCS \(cisa.gov\)](#) A cyber security capability framework developed by the US National Initiative for Cybersecurity Careers and Studies (NICCS), National Institute of Standards and Technology (NIST)
- [Executive Cybersecurity Leadership \[NICE Framework Work Role\] | NICCS \(cisa.gov\)](#)