Cyber Security Policy

Purpose of this policy

The Department of Planning and Environment (the department) is committed to delivering excellent service and satisfaction to its customers. Effective cyber security is critical to the department and the employees, customers and citizens of NSW. This policy defines the department's management intent, obligations, framework, objectives, exemptions, and roles and responsibilities for the management of assets in regard to cyber security. This policy aims to provide a consistent and integrated approach across the department, along with alignment to the department's Code of Ethics and Conduct, NSW Cyber Security Policy and NSW Cyber Security Strategy.

To whom this policy applies

This policy applies to all employees performing work for the department, including individuals seconded from other organisations, volunteers, contingent or labour hire workers, professional services contractors and consultants.

Policy statement

Management intent

- The department's management commit to implementing cyber security principles and practices to protect its crown jewels and other assets.
- The department and each separate agency adopting this policy, is responsible for the management of cyber security risks and controls pertaining to its crown jewels and other assets.
- An Information Security Management System (ISMS) based on ISO/IEC 27001:2013 standard must be implemented by the Office of the Chief Digital and Information Officer (CDIO) (or equivalent for agencies and entities with their own Information and Communications Technology (ICT)) providing a risk-based approach to the management of cyber security.
- A risk based approach will be used to determine the cyber security controls to be implemented following ISO/IEC 27001: 2013, the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the NSW Cyber Security Policy.
- An Information Security Steering Committee (ISSC) must be established to ensure governance of an ISMS, and management commitment to cyber security principles and practice.

Obligations

- The department recognises its obligations to protect the confidentiality, integrity and availability of the assets within its custody
- The department is obliged to monitor and report on the effectiveness and relevance of the ISMS to ensure continual improvement of the ISMS and its controls, as follows:
    - Report annually to Cyber Security NSW.

- Identified cyber security risks with a residual rating of high or extreme are reported to Cyber Security NSW.
- Crown jewels are identified and reported to Cyber Security NSW.
- Attest to cyber security in the department's annual report as outlined in section 4 of the NSW Cyber Security Policy.

Framework

- Cyber security is implemented according to the following governance approaches:
  - Certification - In scope assets as defined by the ISMS Scope document will be subject to an independent annual audit.
  - Compliance - All other information assets, including crown jewels not in certification scope must comply with the ISMS and be subject to an annual independent review or audit (unless an exemption is in place). These information assets must
  - be identified during the threat risk assessment and prioritised as being of sufficient risk to warrant an audit of the effectiveness of relevant ISMS controls.
  - Maturity assessment – An annual independent review or audit must be performed to assess the conformity of the ISO 27001:2013 standard, the effectiveness of the crown jewels assessment process, and the level of maturity against the mandatory requirements of the NSW Cyber Security Policy and Australian Cyber Security Centre (ACSC) Essential 8.
  - Awareness - Providing awareness and training directly relevant to the work of an employee and the cyber and information security risks they face in order to create cyber smart employees.
- The department conforms with the Australian Cyber Security Centre (ACSC) Essential Eight and or Information Security Manual (ISM) controls (marked as O: Official at a minimum) for all assets, unless an exemption is in place.
- Managed service providers and vendors will be certified/compliant to either ISO/IEC 27001:2013, SOC2 Type 2, IRAP, NIST SP 800-53 Rev 4, PCI DSS v3.2.1, NSW Cyber Security Policy or an equivalent standard.
- Managed service providers and vendors will conform/align with the department ISMS (or agency/entity specific ISMS) requirements, including but not limited to configuration, change and release, and risk management processes.
- A statement of applicability will be maintained for an ISMS to identify controls that are applicable to maintaining cyber security.

Objectives

- Identified crown jewels and other assets have a business impact assessment performed and appropriate business continuity and disaster recovery plans developed, tested and maintained.
- Identified assets must have a risk assessment performed by those responsible for the asset, and reviewed periodically, with identified threats mitigated as per the department's Risk Management Policy.
- Incident response plans and processes, including data breach are developed, tested and maintained.

- Assets are classified according to the NSW Government Information, Classification, Labelling and Handling Guidelines (ICLHG) and or the Australian Government, Protective Security Policy Framework (PSPF) to ensure appropriate controls are implemented.
- Where the department regularly shares data with other agencies or entities, the data is classified and Memorandums of Understanding (MOU) are in place.
- Approvals for data sharing are in place prior to sharing, especially when the data did not originate from the department.
- A cyber security training and awareness programme is available to all employees, contractors and where appropriate external parties, with specialised training provided to employees in scope of an ISMS.
- Non-department devices and or access from a non-department location are assessed for security risks, with controls implemented relative to the department's risk appetite, prior to physically and or logically connecting to the department.
- Specialist advice on cyber security matters will be available.
- Documentation that comprises an ISMS; this includes policies and procedures must be created, reviewed and maintained following a continual improvement process.
- Contact with external organisations is maintained to assist with the implementation of this policy; including NSW Chief Cyber Security Officer, Australian Cyber Security Centre, law enforcement authorities, regulatory bodies, professional organisations and other identified parties.

Exemptions

- All ICT policy exemptions are governed by the ISMS Exemptions Request Management Standard.
- For exemptions to controls specified in this policy and other ISMS documents, a business case, risk assessment and formal review process must be implemented.
- For exemptions relating to crown jewels, the cluster Chief Information Security Officer (CISO) or equivalent must be contacted, and if deemed valid the cluster CISO will contact Cyber Security NSW.
- All other exemption requests must be approved by the CDIO (or equivalent) or ISSC.
- All exemptions must be reviewed on a periodic basis, or annually at a minimum.

Failure to comply with this policy

Ethical and behavioural standards that employees are expected to demonstrate while working with the department are set out in the Code of Ethics and Conduct. If employees fail to meet those standards, corrective action may be taken in accordance the Code of Ethics and Conduct.

Individuals who are not government sector employees such as volunteers, contingent or labour hire workers, professional services contractors and consultants may have their services, contract or agreement terminated immediately, or legal action could be taken if they are found to have violated this policy.

Review timeframe

Digital Information Office will review this policy no later than 3 years from the date the document is approved. This policy may be reviewed earlier in response to post-implementation feedback, changes to legislation, or as necessary in accordance with the department's policy and procedures.

Related documents

A full list of legislative requirements or other related documents that may impact information security is maintained within the Information Security Management System (ISMS).

This policy should be read in conjunction with the following documents:

- NSW Cyber Security Policy
- Privacy Management Plan
- NSW Cyber Security Strategy
- ISMS Exemption Request Management Standard
- Code of Ethics and Conduct

Policy metadata

Table 1. Policy metadata

Category	Description
Status	Final
Date of approval	27.05.2021
Approver	Group Deputy Secretary
Group	Corporate Services
Division	Digital Information Office
Policy owner	Chief Digital and Information Officer
Document location	DPE Intranet
Next review date	April 2024
Associated procedure	N/A
Any additional applicability	Additional applicability will be considered in the future
Superseded document	N/A
Further information	cybersecurity@dpie.nsw.gov.au
Document Reference	POL21/10

Version control

Table 2. Version Control

Version	Date issued	Change
1	27.05.2021	New policy document
1.1	3.05.2022	Updated to reflect new branding and name change

Appendices

Appendix 1 – Definitions

Table 3 - Definitions

Term	Definition
Agency heads	Consistent with the Government Sector Employment Act 2013 (GSE Act), a Head of Agency is defined for the purpose of this policy framework as: • in the case of the Department of Planning and Environment –the Secretary of the department • in any other case – the Head of Agency listed in Part 2 or Part 3 of Schedule 1 of the GSE Act, such as Chief Executive, Commissioner or Chairperson. In practice, this represents the key person responsible for directing the affairs of the agency.
Asset	Operational systems or information that has value to the department.
Audit	Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.
Availability	Property of being accessible and usable upon demand by an authorised entity.
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Continual improvement	Recurring activity to enhance performance.
Control	Measure that is modifying risk.
Crown jewels	The most valuable or operationally vital systems or information in the department.
Industrial Automation and Control Systems (IACS)	Industrial Automation and Control Systems, also referred to as Industrial Control Systems (ICS), include “control systems used in manufacturing and processing plants and facilities, building environmental control systems, geographically dispersed operations such as utilities (and) pipelines…, and other industries and applications such as transportation networks, that use automated or remotely controlled or monitored assets.” (IEC/TS 62443-1-1 Ed 1.0)

Term	Definition
Integrity	Property of accuracy and completeness.
International Standards for security	• ISO/IEC 27001:2013, SOC2 Type 2, IRAP, NIST SP 800-53 Rev 4, PCI DSS v3.2.1 • Australian Cyber Security Centre, Australian Government Information Security Manual (ACSC ISM) • Australian Cyber Security Centre, Information Security Registered Assessors Program (IRAP) • Australian Government, Attorney-General's department, Protective Security Policy Framework (PSPF) • ISO/IEC 27000: 2016 – Information technology – Security techniques – Information security management systems – Overview and vocabulary • ISO/IEC 27001: 2013 – Information technology – Security techniques – Information security management systems – Requirements • ISO/IEC 27002: 2013 – Information technology – Security techniques – Code of practice for information security management • National Institute of Standards and Technology (NIST) - Framework for Improving Critical Infrastructure Cybersecurity • NSW Cyber Security Strategy • Payment Card Industry Data Security Standard (PCI DSS) • SOC 2 – SOC for Service Organisations: Trust Services Criteria, American Institute of CPA (SOC2)
ISMS	An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation's information security to achieve business objectives". (ISO/IEC 27000:2018)
Risk	Effect of uncertainty on objectives

Appendix 2 - Roles and responsibilities

Table 4: Roles and responsibilities

Role	Responsibility
All employees	• Cyber security of the department's assets is everyone's responsibility. • Are responsible for complying with this policy as per the Code of Ethics and Conduct. • Reporting potential or actual cyber security incidents to their supervisor, people leaders or the relevant Service Desk in a timely manner.
People leaders	• Are responsible for encouraging a culture of cyber security within the department. • Implementing and monitoring compliance to this policy within their area. • Providing sufficient resources to ensure compliance with the ISMS. • Helping employees understand the impact their actions have on cyber security.
Risk managers	• Assisting to ensure the risk framework is applied in assessing cyber security risks and with setting of risk appetite. • Assisting the agency CISO in analysing cyber security risks. • Meeting with cluster CISO to ensure cyber risk frameworks fit into the Enterprise Risk framework.
Internal auditors, Auditors and Professional Services Bodies	• Validating that the cyber security plan meets the agency's business goals and objectives and ensuring the plan supports the agency's cyber security strategy. • Regularly reviewing their agency's adherence to this policy and cyber security controls. • Providing assurance regarding the effectiveness of cybersecurity controls.
Information Management Officer	• Acting as a focal point within the department for all matters related to information management that are required to support cyber security. • Ensuring that cyber incidents that involve information damage or loss are escalated and reported to the appropriate information management response team within the department.
Chief Information Security Officer (or equivalent)	• Defining and implementing a cyber security plan for the protection of the agency's information and systems. • Developing a cyber security strategy, architecture, and risk management process and incorporate these into the agency's current risk framework and processes.

Role	Responsibility
	• Assessing and providing recommendations on any exemptions to agency or cluster information security policies and standards. • Attending agency or cluster risk committee meetings, when invited by the Audit and Risk Committee (ARC). • Implementing policies, procedures, practices and tools to ensure compliance with this policy. • Investigating, responding to and reporting on cyber security events. • Reporting cyber incidents to the appropriate agency governance forum and Cyber Security NSW based on severity definitions provided by Cyber Security NSW. • Representing their agency on whole-of-government collaboration, advisory or steering groups established by Cyber Security NSW or cluster CISO. • Establishing training and awareness programs to increase employees' cyber security capability. • Building cyber incident response capability that links to agency incident management and the whole of government cyber response plan. • Collaborating with privacy, audit, information management and risk officers to protect agency information and systems. • For cluster CISOs, supporting agencies in their cluster to implement and maintain an effective cyber security program including via effective collaboration and/or governance forums. • Managing the budget and funding for the cyber security program. • Managing and coordinating the response to cyber security incidents, changing threats, and vulnerabilities. • Developing and maintaining cyber security procedures and guidelines. • Providing guidance on cyber security risks introduced from business and operational change. • Managing the life cycle of cyber security platforms including design, deployment, ongoing operation, and decommissioning. • Ensuring appropriate management of the availability, capacity and performance of cyber security hardware and applications. • Providing input and support to regulatory compliance and assurance activities and managing any resultant remedial activity. • Developing a metrics and assurance framework to measure the effectiveness of controls. • Providing day-to-day management and oversight of operational delivery.

Role	Responsibility
Chief Digital and Information Officer (or equivalent)	• Working with CISOs and across their agency to implement this policy. • Implementing a cyber security plan that includes consideration of threats, risks and vulnerabilities that impact the protection of the agency's information and systems within the agency's cybersecurity risk tolerance. • Ensuring that all employees, including consultants, contractorsand outsourced service providers understand the cyber security requirements of their roles. • Clarifying the scope of CIO or COO responsibilities forcyber security relating to assets such as information, building management systems and IACS. • Assisting CISOs/CCSOs or equivalent position with their responsibilities. • Ensuring a secure-by-design approach for new initiativesand upgrades to existing systems, including legacy systems. • Ensuring all employees and providers understand their rolein building and maintaining secure systems.
Department Secretary / Agency Heads	• Appointing or assigning an appropriate senior executive bandofficer in the agency or across the cluster, with the authority to perform the duties outlined in this policy – this person should be dedicated to security at least at the cluster level. • Appointing or assigning a senior executive band officer with authority for Industrial Automation and Control Systems(IACS) cyber security for the agency or cluster (if applicable). • Ensuring all agencies in their cluster implement and maintainan effective cyber security program. • Supporting the agency's cyber security plan. • Ensuring their agency complies with the requirements of thispolicy and timely reporting on compliance with the policy. • Ensuring their agency develops, implements and maintainsan effective cyber security plan and/or information security plan. • Ensuring CISOs (or equivalent) and a senior executive band officer for IACS (if applicable) attend the agency's risk committeemeetings as advisors or committee members. • Determining their agency's risk appetite using the approved whole- of-government Internal Audit and Risk Management Policy. • Appropriately resourcing and supporting agency cybersecurity initiatives including training and awareness and continual improvement initiatives to support this policy. • Approving internal security policies as required.

Role	Responsibility
NSW Chief Cyber Security Officer (NSW CCSO)	• Creating and implementing the NSW Government Cyber Security Strategy. • Building a cyber-aware culture across NSW Government. • Receiving, collating and reporting on high cyber risks and monitoring cyber security incident reports across NSW Government. • Reporting on consolidated agency compliance and maturity. • Chairing the NSW Government Cyber Security Steering Group (CSSG). • Consulting with agencies and providing advice and assistance to the NSW Government on cyber security including improvements to policy, capability and capacity. • Recommending and recording exemptions to any part of the NSW Government Cyber Security Policy. • Representing NSW Government on cross-jurisdictional matters relevant to cyber security. • Assisting agencies to share information on security threats and cooperate on security threats and intelligence to enable management of government-wide cyber risk. • Creating and implementing the NSW Government cyber incident response arrangements. • Coordinating the NSW Government response to significant cyber incidents and cyber crises.
3rd party ICT providers	Where the department requires 3rd party vendors to comply with the NSW Cyber Security Policy, the department must ensure that vendors fulfil the following mandatory requirements from the NSW Cyber Security Policy to protect outsourced government systems: • Mandatory Requirement 1.5: The ICT provider has a process that is followed to notify the agency quickly of any suspected or actual security incidents and follows reasonable direction from the agency arising from incident investigations (noting this will vary based on risk profile and risk appetite) • Mandatory Requirement 2.1: The ICT provider ensures that their staff understand and implement the cyber security requirements of the contract • Mandatory Requirement 3.1: Any 'Crown Jewel' systems must be covered in the scope of an Information Security Management System (ISMS) or Cyber Security framework • Mandatory Requirement 3.4: Cyber Security requirements are built into the early stages of projects and the system development life cycle (SDLC) including agile projects • Mandatory Requirement 3.5: Ensure new ICT systems or enhancements include processes for audit trails and activity logging to assess the accuracy and integrity of data, including processes for internal fraud detection

Role	Responsibility
	This does not prevent other contractual obligations being imposed