System acquisition, development, and maintenance policy

Purpose of this policy

This policy describes the approach of the Department of Planning, Housing and Infrastructure (the department) to ensuring the security of a system over its entire life cycle to protect information and systems from unauthorised disclosure, theft, modification, or destruction. This policy is aligned to the Australian Cyber Security Centre Information Security Manual in order to provide a consistent approach to the security of systems' lifecycles.

To whom this policy applies

This policy applies to all employees who procure, develop, implement, or manage information systems for the department (including individuals seconded from other organisations, volunteers, contingent or labour-hire workers, professional services contractors, and consultants).

Policy statement

Security requirements of information systems

To ensure that security is an integral part of the system over its entire life cycle, the following controls must be implemented:

- The implementation of security controls for systems must follow a risk-based approach.
- All statutory and policy requirements or other limitations must be considered as part of the risk assessment.
- Care must be taken not to take or send records out of NSW in contravention of any legal responsibilities or business interests the department may have. Further information about the standards for record keeping can be located at: Storage of State records with service providers outside of NSW.
- Systems must be located within New South Wales, Australia unless the risks are identified, acceptable and well managed, and the records are managed in accordance with all the requirements under the State Records Act 1998.
- All systems must follow the department's change management process for change and release management throughout the lifecycle of the system.
- Systems must comply with the Cryptography Policy if cryptographic controls are required.

- Systems must comply with the Supplier Relationships Policy if supplier controls are required.
- Separate development, test and production environments must be implemented based on a risk Assessment.
- A code repository and version control must be implemented for all systems.
- All systems must be configured to send logs to a central repository for monitoring.
- All systems must have documentation that is maintained for currency.
  - a new low risk system or a system with a minor change must undergo a vulnerability scan, with any medium or above findings remediated prior to release
  - all other new systems or a system with major change must undergo a penetration test, with any medium or above findings remediated prior to release.

Security in decommissioning or migration

To ensure that security is considered in the final stages of a systems life, the following controls must be implemented

- Ensure records management requirements are complied with.
- Verify what contractual arrangements are in place.
- If the system is hosted externally, make arrangements for a return of data in a suitable format, via a secure mechanism.
- Ensure data hosted externally is disposed of in accordance with section 8.3.2 Disposal of media in the Cyber Security Assurance Standard.
- Ensure data returned is stored appropriately given the data classification requirements (see the NSW Government Information Classification, Labelling and Handling Guidelines).
- If the data is to be utilised in a different system, ensure the data is uploaded via a secure mechanism.

Test data

- Production data is not be used for testing in development environments unless the development environment has the same security controls.
- If personal information is used for testing, the data should have a privacy impact and risk assessment performed to determine whether it is acceptable to use as is, or whether the data must be anonymised.

Exemptions

- Exemptions to this policy must comply with the ISMS Exemption Request Management Standard.
- Exemptions must only be approved where it is technically, practically or financially infeasible to comply with this policy.
- Reviews of exemptions must be performed annually.

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 that may impact information security is maintained within the Information Security Management System (ISMS).

- Australian Cyber Security Centre Information Security Manual and Evaluated Products List
- Open Web Application Security Project (OWASP) Application Security Verification Standard
- Secure Coding Standards
- Top 10, Testing Guide and Development Guide
- NSW Government Information Classification, Labelling and Handling Guidelines

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

- Cyber Security Policy
- Access Control Policy

- Cryptography Policy
- 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	Deputy Secretary
Group	Corporate Services
Division	Digital Information Office
Policy owner	Chief Digital and Information Officer
Document location	DPHI intranet
Next review date	April 2026
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	POL21/14

Version control

Table 2. Version Control

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

Version	Date issued	Change
1.2	12.02.2024	Updated to reflect new branding and name change. Removed internal links.

Appendices

Appendix 1 – Definitions

Appendix 2 - Roles and responsibilities

Appendix 1 – Definitions

Table 3 - Definitions

Term	Definition
Availability	Property of being accessible and usable on demand by an authorised party.
Confidentiality	Property that information is not made available or disclosed to unauthorised individuals, entities, or processes.
Integrity	Property of accuracy and completeness.
Vulnerability	Weakness of an asset or control that can be exploited by one or more threats.

Appendix 2 - Roles and responsibilities

Table 4: Roles and responsibilities

Role	Responsibility
Chief Digital and Information Officer (CDIO)	• Approve exemptions to this policy.
Digital and Information Office (DIO)	• Must implement this policy. • Notify Chief Information Security Officer (or equivalent) of any changes.
Chief Information Security Officer (or equivalent)	• Must develop, maintain and improve this policy • Monitor and report on compliance to this policy (effectiveness measurements). • Review exemptions to this policy.