Cryptography Policy

Purpose of this policy

This policy describes the approach of the Department of Planning and Environment (the department) to securing sensitive information via approved algorithms and protocols for implementation based upon an identified need. It aims to provide a secure and consistent approach and is aligned to the Australian Cyber Security Centre Information Security Manual.

Cryptography provides the department with confidentiality, integrity, secure authentication and non-repudiation of information. Encryption of data at rest can reduce physical storage and handling requirements, whilst encryption in transit protects sensitive information being communicated over public networks.

To whom this policy applies

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

Policy statement

Risk-based approach

Cryptographic controls are implemented following a risk-based approach that considers the sensitivity of the information the cryptographic controls are planned to protect. The implementation of cryptographic controls does not alter the sensitivity of the encrypted information. Cryptography limits the ability of the information to be accessed by an attacker in the event that it is exposed.

Cryptographic key management practices are implemented following a risk-based approach that considers the sensitivity and criticality of the information; the cryptographic key protects.

Consideration must also be given to whether the key is for data in transit or at rest and the duration of the cryptographic key life.

Cryptographic key management

Key storage

Cryptographic keys are sensitive information and must be stored appropriately.

- Keys must be protected on both volatile and non-volatile memory.
- Keys must not be stored in plaintext.
- Keys should be stored in a hardware security module (HSM) or isolated cryptographic service/vault.
- If keys are stored in an offline database/device, the keys must be encrypted with a Key Encryption Key (KEK).

- Standard application code must never read or use cryptographic keys directly, key management libraries should be implemented.

Key security

- Key strength must be as per the current version of the Australian Cyber Security Centre (ACSC) Information Security Manual (ISM).
- Keys must be used for a single purpose only so as not to weaken the security provided.
- Keys must be generated by a cryptographic module (hardware preferred) with any random value required generated with the same module.
- The distribution of keys must be via a secure channel only.

Key backup

If an encryption key is lost, data encrypted with it must never be recovered, therefore keys must be securely backed up as follows:

- A backup of encryption keys needs to be encrypted to ensure their confidentiality.
- Escrow services can be used for the management of key backups.
- Digital signature keys must not be escrowed.

Key logging and monitoring

- All keys must be uniquely identifiable.
- All users with access to keys must be uniquely identifiable.
- A log of key usage should be maintained.
- A review of keys must be performed annually.
- A review of key access must be performed annually.
- A review of key usage must be performed annually.

Key compromise and recovery

- If keying material is compromised, the keying material must be revoked as soon as possible.
- A log of keys, usage and system contact must be maintained.
- The log of usage must contain at a minimum, date, time and account.
- Details on how to re-key must be recorded.
- Any system specific recovery procedures must be documented as required.

Cryptographic protocols

For a list of approved cryptographic protocols please refer to the current version of the ACSC ISM.

Cryptographic algorithms

For a list of approved cryptographic algorithms please refer to the current version of the ACSC ISM.

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

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

- Cyber Security Policy
- ISMS Exemption Request Management Standard
- NSW Cyber Security Policy
- NSW Cyber Security Strategy
- Code of Ethics and Conduct
- Open Web Application Security Project (OWASP) Key Management Cheat Sheet
- Australian Cyber Security Centre (ACSC)
- Information Security Manual (ISM)

Policy metadata

Table 1. Policy metadata

Category	Description
Status	Final
Date of approval	27.5.2021
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	
Any additional applicability	Additional applicability will be considered in the future
Superseded document	N/A
Further information	cybersecurity@dpie.nsw.gov.au
Document Reference	POL21/16

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

Appendices

Appendix 1 – Definitions

Table 3 - Definitions

Term	Definition
Cryptographic algorithm	An algorithm used to perform cryptographic functions such as encryption, integrity, authentication, digital signatures or key establishment.
Encryption	The process of encoding data / information in such a way that only authorised parties can access.
Escrow	An arrangement in which the keys needed to decrypt encrypted data are held in escrow so that in certain circumstances an authorised party can gain access to the keys for utilisation.

Appendix 2 - 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. • Must notify Chief Information Security Officer (or equivalent) of any changes.
Chief Information Security Officer (or equivalent)	• Must develop, maintain and improve this policy. • Must monitor and report on compliance to this policy (effectiveness measurements). • Must review exemptions to this policy.