# Supplier Relationships Policy

## Purpose of this policy

This policy describes the Department's approach to ensure the systems being developed, maintained or procured externally to the department are secure. This policy is based on best practice for supplier security to manage suppliers consistently throughout the agreement period.

## To whom this policy applies

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

## Policy statement

### Information security in supplier relationships

To ensure the confidentiality, integrity and availability of the department's assets that are accessible and/or managed by suppliers, the following controls must be implemented:

- A risk assessment must be performed prior to entering into any formal or informal agreement. The risk assessment must take into consideration the supplier's business and the country of origin of the goods or services to be supplied.
- The ownership of the department's data must be retained by the department.
- the sensitivity of the data must be assessed, and appropriate security controls implemented, as per the NSW Government Information Classification, Labelling and Handling Guidelines, and any other identified compliance requirements applicable to the goods or services being supplied.
- Agreements must comply with the department's procurement processes and associated requirements including:
  - information security requirements will be specified in the supplier contract, including any security risks with the supplier's subcontractors, memorandum of understanding or an equivalent agreement between parties
  - if no formal agreement is in place, the supplier must agree in writing to follow the applicable information security policies, procedures and processes, and if the supplier is

required to work from the department's premises, then each supplier must complete the applicable induction

— a formal agreement must also cover the supplier's security risks associated with their third parties.

### Supplier service delivery management

To ensure that an agreed level of security is maintained in line with agreements and supplier risk assessments (as described above), the following controls must be implemented

- Monitoring of the services provided by a supplier must be performed to ensure agreed service levels are met commensurate with risk.
- Periodic reporting of formal agreements must be performed by the team directly responsible for the service.
- If a gap in service or an issue arises with the service a supplier is providing, a resolution must be sort with the supplier.
- A change or termination of agreement with a supplier must be managed through a change management process to ensure that the criticality of the system is not compromised; and
- Suppliers that require access to the department's systems must comply with the department's Code of Ethics and Conduct, Acceptable Use Policy and the Access Control Policy.

### 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).

- Cyber Security Assurance Standard
- Vendor Information Security Requirements
- 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
- Acceptable Use Policy
- ISMS Exemption Request Management Standard
- Code of Ethics and Conduct
- NSW Cyber Security Policy
- NSW Cyber Security Strategy

# 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 | POL21/13 |

# 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. |
| Risk assessment | Overall process of risk identification, risk analysis and risk evaluation. |

# 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.<br>• Notify Chief Information Security Officer (or equivalent) of any changes. |
| Chief Information Security Officer (or equivalent) | • Must develop, maintain and improve this policy.<br>• Monitor and report on compliance to this policy (effectiveness measurements).<br>• Review exemptions to this policy. |