Policy and Procedure

Supplier Access and Security

Purpose

This policy and procedure aims to:

- Ensure protection of SWSPHN's data assets that are accessible and/or managed by suppliers; and maintain an agreed level of information security and service delivery in line with supplier agreements.
- Ensure the systems being developed, maintained, or procured externally to the organisation are secure.
- Describe how SWSPHN selects and evaluates suppliers and the purchasing process for the purpose of conforming to specified requirements for suppliers who can influence confidentiality, integrity and availability of sensitive information, through access to SWSPHN documents and records.

Policy

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

- Prior to entering into any formal or informal agreement, risks to information security must be considered and should also take into account the supplier's business and the country of origin of the goods or services to be supplied.
- SWSPHN preferences suppliers that have demonstrated a commitment to the security of their products and services, with a strong track record of transparency and maintaining the security of their own systems and supply chains. This includes suppliers with cyber assurance certification e.g. ISO 27001 or equivalent.
- The ownership of SWSPHN's data must be retained by SWSPHN.
- The sensitivity of the data must be assessed in line with the Australian Privacy Principle's definitions of personal and sensitive information, and appropriate security controls implemented, as per relevant privacy legislation and SWSPHN's information security policies and procedures, as well as any other identified compliance requirements applicable to the goods or services being supplied.
- Agreements must comply with SWSPHN's procurement and contract management processes and associated requirements including:
    - Relevant information security requirements must be established and specified in contracts with each supplier that may access, process, store, communicate or provide ICT infrastructure components for, the organisation's information.
    - 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 SWSPHN's premises, then each supplier must complete the applicable induction and training.
- SWSPHN requires suppliers to apply reasonable and appropriate safeguards and operations to protect information made available as part of the delivery of the contract against accidental and unlawful destruction, alteration, and unauthorised or improper disclosure or access. This includes relevant

information security policies and procedures, as well as initiatives to raise staff awareness around cyber security risks.

- SWSPHN requests disclosure by suppliers of any cyber security incidents and the strategies put in place in response to this. For non-commissioned service suppliers, this is to be done in writing as soon as practicable. For commissioned service suppliers this can be disclosed in the Annual Supplier Due Diligence Declaration or via the Incident Management Policy and Procedure.
- In the event of an incident, SWSPHN employees are to refer to the Cyber Security Incident Response Plan and the Information Classification and Handling Management Policy and immediately advise the Data Custodian and an Executive.
- Suppliers that require access to SWSPHN's systems must comply with SWSPHN's policies and procedures.

Exemptions to this policy must only be approved by the CEO where it is technically, practically, or financially infeasible to comply with this policy. Reviews of exemptions must be performed annually.

Applicability

All SWSPHN staff and service suppliers who can influence confidentiality, integrity and availability of sensitive information, through access to SWSPHN documents and records.

Procedure

1. New Suppliers

When assessing the need for a new supplier, Management must perform due diligence by evaluating suppliers using the criteria described below for non-commissioned suppliers or commissioning procedures and criteria for commissioned services. Refer to Commissioning Process SOPs for further detail. If the supplier satisfies the requirements, they are entered into Suppliers Register as Approved by the Owner (i.e. the SME responsible for managing and monitoring that supplier).

Note: Only suppliers with access to SWSPHN information are tracked in the List of Approved Suppliers and reviewed at Management Review. These suppliers are critical to the organisation and maintaining the confidentiality and integrity of SWSPHNs documents and records, and their performance is regularly evaluated to ensure they meet the requirements for our operations.

2. Evaluating New Suppliers

Management conducts an evaluation of new suppliers (using the **New Supplier Form** for non-commissioned suppliers and through the procurement and new contract process for commissioned services) by analysing:

- Reputation and relevant experience of the supplier
- Information security and data protection processes (consider ISO 27001 certification or equivalent)
- Quality control and complaints processes (consider ISO certification or equivalent)
- Adequate insurances (Public Liability, Professional Indemnity, Cyber Security, Workers Compensation)
- Service Level Agreements (SLA), Master Services Agreement (MSA) or Terms of Service (ToS) documents
- Risks

Executive approval is required for those non-commissioned suppliers who have access to SWSPHN information.

Evaluation Matrix**

Criteria	1 = Not Meeting Expectations	2 = Below Expectations	3 = Meets Expectations	4 = Exceeds Expectations
Reputation and experience	No proven experience and/or negative reputation.	Limited experience (1-3 years or minimal relevant projects) and mixed reputation.	Moderate to strong experience (several successful projects completed with generally positive reputation, well-regarded).	Extensive, proven experience (long-standing, consistent history of successful delivery in the industry) and excellent reputation (strong references from leading clients, widely recognised and trusted e.g. awards).
Information security	No information security procedures or controls in place. Ad hoc practices, no documented policies or procedures.	Some informal or partial information security controls exist, that may be inconsistent or undocumented. Password protection is in place, but no policy. Firewalls/antivirus used but not centrally managed. Limited security awareness staff training.	Formal information security policies and procedures documented. Basic access control and data protection measures in place. Some security awareness staff training in place. Some validation of security processes. Aligns with Commissioned Services CSA.	Comprehensive information security management system aligned with ISO 27001 certification or equivalent, demonstrating best-practice information security management with third-party validation.
Quality and compliance	No complaints, internal auditing or quality control procedures in place. Reactive approach.	Some informal complaints, internal auditing and/or quality control procedures exist, but they are inconsistent or undocumented.	Formal complaints procedure in place. Some internal auditing conducted. Some quality control procedures in place. Aligns with Commissioning Incident Management Policy.	ISO 9001 certification or equivalent, demonstrating best-practice quality management with third-party validation.

**Commissioned suppliers are assessed against the Contract Stratification Matrix, which is aligned to the above ratings in the Suppliers Register.

There are several ways to complete the evaluation including:

- Contacting the supplier directly to request information
- Public security, privacy, or quality documentation
- Government/industry regulatory compliance statements
- Contractual clauses that mandate security and insurance
- Published ToS that include security, privacy, complaints or support processes
- Information from customer portals or knowledge bases

If the supplier requires access to or to store company or confidential information (such as cloud-based applications), further due diligence must cover the provider's security controls for access to the confidential information, particularly personally identifiable information (PII) to ensure adequate risk management controls are in place.

If a supplier is approved, they must be entered into the List of Approved Suppliers by the Owner (i.e. the SME responsible for managing and monitoring that supplier), and an executed Master Services Agreement (MSA) or applicable Terms of Service (ToS) document must be recorded. These documents are saved with the services agreement.

For cloud services, the Master Services Agreement (MSA) or applicable Terms of Service (ToS) must specify provisions for confidentiality, intellectual property, and Service Level Agreements (SLAs).

In addition to the above requirements, the executed contract must contain the following:

- Cover a specified period
- Specify the exact pricing for the services
- Specify how the provider will access and treat SWSPHN information, including any highly confidential information, and expectations in managing the privacy and security of this data
- Include a non-disclosure agreement
- Specify services to be provided, including Service Level Agreements and penalties for missing the levels
- Allow for cancellation if contractual terms are not met
- Include an exit or termination clause that allows for the secure return and/or deletion of data upon the end of the contract
- Specify controls and standards for subcontracting of the services and reassignment of contract to manage privacy and security risks
- Cover liability issues
- Describe how and where to handle contractual disputes
- Where appropriate, provide a copy of their ISO Certifications or be able to access it

3. Monitoring and Review

Management monitors and reviews service and performance levels and fulfilment of security obligations formally on an annual basis for non-commissioned services using the **Supplier Annual Review Form** or alternatively for commissioned services through the review processes outlined in the Contract Management and

Compliance Policy and Procedure. A new assessment is to be performed if the non-commissioned supplier is not transacted with over a twelve (12) month period. Re-evaluation can take place at any time if the service provided by a supplier is not to desired standards.

Suppliers who score 1-2 on any of the assessment criteria will need to be approved by Executive and risks considered prior to continued engagement with the supplier.

Suppliers with complaints recorded against them will be discussed and reviewed in the Management Review.

4. Information Security Controls

Suppliers must be given the least amount of network, system, and data access required to perform the contracted services. This access must follow the Access Control Policy and be periodically audited.

There must be a mechanism for secure information exchange with all service providers. This will vary with the type of service the supplier provides but may include encrypted file exchange and MFA.

SWSPHN must also maintain a mechanism for verifying the other party's identity and confirming changes to the service. This prevents an attacker from using social engineering tactics to gain access to company data.

5. Termination of Suppliers

All access rights granted to the supplier must be immediately revoked per the Access Control Policy when a supplier contract is changed or terminated.

A change or termination of agreement with a supplier may need to be managed through a change management process to ensure that the criticality of the system is not compromised, including a reassessment of risks and maintaining and improving existing information security policies, procedures, and controls.

Further, any equipment, software or information in the supplier's possession must be returned.

6. Environmental Operations Control

Suppliers providing e-waste services must follow legal and other requirements regarding the effective disposal of e-waste. E-waste providers must provide a Certificate of Destruction upon collection and destruction of e-waste.

Associated Documents

Legislation and best practice guidelines

- ISO 27001 Information security management system – Requirements
- ISO 9001 Quality management systems – Requirements

Internal policies and documents

- Access Control Policy
- Information Classification and Handling Policy and Procedure
- Information Security Policy
- Commissioning Incident Management Policy and Procedure
- Commissioned Services Contract Stratification Matrix
- Commissioned Services CSA

- Contract Management and Compliance Policy and Procedure
- New Supplier Form
- Software Management Policy and Procedure
- Supplier Annual Review Form
- Suppliers Register

Roles and Responsibilities

Document Owner	Ensure that this document is published and implemented, progress is monitored and that it is reviewed according to the document control schedule outlined in the document.
Executive Sponsor	Provide advice to the document owner, approve the final document, and present it to the Senior Staff Meeting for approval.
Board	Maintain oversight of the risks and treatment strategies associated with the use of suppliers for business operations.
Executive	Manage the risks and treatment strategies associated with the use of suppliers for business operations. Ensure compliance with this policy and procedure.
Management	Lead the assessment and evaluation of suppliers in line with this policy and procedure.
SWSPHN Staff/Workers	Support the assessment and evaluation of suppliers in line with this policy and procedure.

Definitions

View related definitions in the Integrated Management System (IMS) Glossary.

Document Control

Document review every (choose most applicable) ☐ 1 year ☐ 2 years ☑ 3 years

Version	Date Commenced	Document Owner	Change Description	Review Date	Approver
V1.0	March 2023	IT Manager	New Policy	March 2026	Executive Manager of Corporate Services
V1.1	March 2025	IT Manager	File name update	March 2026	Director of Corporate Services
V2.0	November 2025	IT Manager	Revised Policy. Policy name change from Supplier Access to and Security of Information Systems and Data.	November 2028	Executive Manager of Corporate Services

This document will remain in effect until replaced.