STANDARD

Cyber Security
Supply-Chain Controls
FNC-STD-IS-05

This document applies to:

All Sites ☐

WRITTEN BY: Matt Hepple ENDORSED/CHECKED BY: Chris Pennycuick APPROVED BY: Kevin Lin

Table of Contents

1.0 Purpose/Scope

Stanwell maintains a Security Management Framework which moderates Stanwell's security exposures and vulnerabilities, ensuring the cyber security posture is maintained. The Framework does this by applying controls to cyber security risks, including those that threaten Stanwell's supply chain.

The purpose of this Standard is to provide guidance on the controls required to treat cyber security supply chain risk. It makes clear Stanwell's expectation that all parties apply cyber security controls to manage risk.

2.0 Responsibilities

Where the product or service relates to cyber security risk, all parties are responsible for managing applicable cyber security risks for their respective products or services when accessing Stanwell systems.

3.0 Supply Chain Cyber Security Controls

Stanwell leverages a significant supply chain, including some that expose Stanwell to cyber security risk. Where the product or service relates to cyber security risk, Stanwell expects the parties to establish and maintain effective cyber security measures. This will safeguard access to Stanwell's systems and/or Confidential Information from unauthorised access, use, tampering (Integrity), copying or disclosure. All parties are expected to use the same degree of care used to protect its own Confidential Information, or which a prudent person would use to protect their own Confidential Information or Integrity, whichever standard is higher.

Where the products or services relate to cyber security risk, parties must ensure their information technology, industrial & operation technology, and other business systems meet the following requirements when providing their product or service, or interfacing to Stanwell's systems.

3.1 General

a) Any technology systems utilised, or services provided by any parties, or significant modification of an existing system or services, must not expose Stanwell to material cyber security risk;

b) Parties will ensure they have conducted an appropriate cyber security risk assessment on their own systems and any other systems utilised in providing the product or service, in particular:

   i) undertake cyber security assessments to ascertain security posture and risk profile;

   ii) identify the key technical, and compliance measures required to ensure the confidentiality, integrity and availability of information is maintained; and

   iii) ensure that control measures applied are commensurate with assessed risk.

The results of any risk assessment will be made available to Stanwell on request.

c) Services owned, managed, or operated by all parties have notification, response, and recovery plans, with periodic testing to ensure services can be restored as soon as possible; and

d) On termination of a relationship, parties must ensure the following, including as applicable to any non-Stanwell systems utilised by the parties:

   i) the return, or the destruction, of Stanwell information;

   ii) any access to the Stanwell environment is terminated, and

   iii) any Stanwell intellectual property appropriately transitioned back to Stanwell.

3.2 Information Protection

If a data breach involving Stanwell's Personally Identifiable Information (PII – Privacy Act 1988 Cth) occurs in a hosted service, the provider will be required to do a serious harm assessment. If the assessment indicates serious harm is likely, the provider is required to report a Notifiable Data Breach to the relevant Government Authorities. The parties must ensure the following to the extent the product or service relates to Stanwell systems:

a) Establish and maintain effective change control processes including:
   i) determining the types of changes to the information system that are configuration-controlled with explicit consideration for security impact analyses;
   ii) documenting configuration change decisions associated with information systems;
   iii) complying with Stanwell's applicable change management processes; and
   iv) retaining adequate records of configuration-controlled changes to information systems to be provided to Stanwell on request.

b) Maintain response and recovery plans incorporating:
   i) Disaster Recovery Plans (DRPs) for critical systems, incorporating essential service continuity, response, and recovery requirements for these systems, and taking into consideration relevant cybersecurity threats and scenarios; and
   ii) DRP testing on a periodic basis to ensure procedures and controls are effective, and services restored can be restored within required as soon as possible.

3.3 Electronic Incidents or Threats

Where relevant to the product or services provided, if the parties become aware of an Electronic Incident or any Threat to their product or service:

a) notify Stanwell and take reasonable steps, at its own expense, to prevent, stop or remediate the Electronic Incident or Threat; and

b) upon Stanwell's request, parties will provide evidence of the prevention, remediation, or planned processes to prevent or remediate the Electronic Incident or Threat.

3.4 Network Integrity

When accessing Stanwell's networks, parties must do all things reasonably required to ensure that Stanwell's network Integrity remains protected, including:

a) Network security controls must be implemented at the gateway between network zones and achieved by enforcing rulesets to control and filter communications between network zones;

b) connections to the network should be restricted and authenticated:
   i) employing a "deny by default" approach, with rules that permit communications across zones being Internet Protocol (IP) source, IP destination and port specific; and
   ii) any rules that permit either all source IP addresses, destination IP addresses, or any type of service/protocol must not be used.

c) configuration work to be completed using Stanwell systems;

d) changes to the network should either increase/uplift protection or allow least privilege access; and

e) network data transiting 'over the wire' within the Stanwell network will be encrypted according to the data classification.

3.5 Access Controls

To the extent that access is required to any Stanwell information technology or business systems as part of the supplied products or services, parties must ensure that:

a) access to any Stanwell systems must be appropriately restricted to only the personnel requiring access to complete the product or service;

b) access procedures must cover identification, authentication, authorisation, and auditing requirements;

c) each user identity requiring access to Stanwell systems is linked to or owned by a uniquely identifiable individual;

d) users, privileged users, or service accounts will be provided the minimum access privileges required;

e) information related to, or generated by, account management activities must be documented and retained for auditing purposes;

f) local credentials/accounts require Complex Credentials to be deployed;

g) users, devices, and other assets are authenticated commensurate with the risk of the transaction and technical limitations; and

h) All identity will be authenticated by the following methods (only), in preferred order:

   i) Stanwell's 'Microsoft EntraID' or On-premise Active Directory;

   ii) If EntraID is not possible, identity should be provided by Multi-Factor Authentication (MFA); or

   iii) If MFA is not possible, identity should be provided by Complex Credentials.

3.6 Software Development

Where parties have developed software for Stanwell, suitable measures must be taken to ensure source-code or configuration for their Developed Software complies with the customer requirements. The parties must have conducted penetration tests for vulnerabilities and followed a secure Software Development Lifecycle process, providing evidence as reasonably requested by Stanwell to demonstrate this. Parties must ensure their Developed Software is:

a) designed and built with strong identifiable security properties, processes, and cyber security reviews;

b) free from any back door, time bomb, drop dead device or any other code designed to disable the Developed Software, unless the customer requirements specify otherwise; and

c) when delivered to the Customer, be free from any Harmful Code or Vulnerability.

3.7 Vulnerability Management

Where relevant to the product or services provided to, or on behalf of Stanwell:

a) Vulnerabilities rated at a medium or low must be mitigated or remediated within regular patch cycle from the vendor; and

b) Vulnerabilities rated at critical or high with:

   i) **known** proof of concept code (POC) or 'in the wild' exploit must be mitigated and/or remediated within 48 hours; or

   ii) **unknown** POC must be mitigated or remediated within regular patch cycle from the vendor.

3.8 Data Security

When accessing Stanwell's data, parties must do all things reasonably required to ensure that Stanwell's data security remains protected. Parties must ensure appropriate modern encryption standards are applied to Stanwell information, when:

a) moving 'Sensitive' or 'Personally Identifiable Information' data over-the-wire or if the data is stored-at-rest, including as applicable to any third-party systems utilised; and/or

b) information is exchanged and/or transferred through the internet, irrespective of its classification.

3.9 Remote Access to Stanwell Systems

To the extent parties require access to information technology or business systems located within Stanwell's network environment, which are provided as part of the product or service, parties must ensure:

a) remote access is securely designed and managed;

b) remote access is provided only to authorised parties for valid business reasons;

c) remote access is revoked where no longer required;

d) controls are applied to the secure operation of remote access; and

e) periodic review and monitor to remove access when no longer required.

3.10 Removeable Media

Parties must ensure that, where relevant to the specific product or service that:

a) all Removable Media is protected, and its use restricted only to those personnel requiring such access as part of the product or service;

b) documented procedures are maintained for the management of Removable Media, specification of approved media, processes of handling and disposal, and the technical enforcement of controls;

c) compliance with any security controls for Removable Media reasonably required by Stanwell and provide details of such compliance to Stanwell on request;

d) any Stanwell data that is copied across to removable media storage must be encrypted; and

e) Use of removable media storage devices in the Stanwell environment are logged and investigated.

4.0 Review, Consultation and Communication

Review:

This Document is required to be reviewed, as a minimum, every 3 year/s. Conditions may warrant earlier review as determined by the business, such conditions are:

- after an Electronic Incident or Threat;
- an increase or decrease in Security Alert Level; and
- as determined by the Head of Cyber Security and Architecture Governance.

Consultation:

The review and update for this document will be done in consultation with:

- Group Manager: Strategic Procurement;
- Head of Cyber Security and Architecture Governance;
- Legal Counsel Procurement: Finance, Governance and Commercial;
- General Manager: Information and Communication Technology; and
- General Manager: Procurement & Supply.

Communication/Requirements after Update:

This standard will be published on the Stanwell's Corporate Extranet, Policies and procedures - Stanwell web site and in Controlled Documents.

5.0 References

- Environmental Protection Act & Regulation
- Health & Safety Act & Regulation
- GOC State Archives – Public Records Act
- Notifiable Data Breaches scheme
- Cyber Security Assessments: contact Cyber Security for specific tools ict_security@stanwell.com
- ICT – Security Testing - Standard Operating: 20/105362
- Stanwell policy DRP/BCDR: ICT Security Team: 18/98448
- Data Governance Overview: 21/72117.

Document No	Document Title
FNC-PROC-IS-32	IT Security Procedure
GOV-PROC-48	Security Framework Management Procedure

6.0 Definitions

Word / Abbreviation	Definition
Availability	Ensuring timely and reliable access to and use of information.
Complex Credentials	As per 18/61141 IT Security Procedure: FNC-PROC-IS-32
Confidential Information	Any information in any form that is disclosed or made available by or on behalf of Us that is: a) personal information (as defined in the Privacy Act 1988 (Cth)); b) expressly provided or made available on a confidential basis; or c) ought reasonably to be expected to have been provided or made available on a confidential basis. But excluding any information that is in the public domain or otherwise lawfully obtained from a different source.
Confidentiality	Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Developed Software	Software developed by the parties will fully document the development process and will: a) manage the services in relation to creating the Developed Software; b) take timely corrective action to fix any Defects in accordance with the agreed methodology; c) ensure concurrent development and supply of user Documentation as specified in the Statement of Work; and d) ensure that the Developed Software is written and documented in a way which would enable future modification by a competent developer without further reference to the developer.
Electronic Incident *(Cyber Incident / Cyber Breach)*	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or that constitutes a violation or imminent threat of violating security

	policies, security procedures, or acceptable use policies. Also, an unauthorised action by a known or unknown person which is an attack, penetration, denial of service, misuse of access, unauthorised access, or intrusion (hacking) or introduction of Harmful Code affecting: a) the Customer's systems, data, or any Confidential Information; b) any systems which are used to provide the product or service.
Harmful Code	Any computer program or virus or other code that is harmful, destructive, disabling or which assists in or enables theft, alteration, denial of service, unauthorised access to or disclosure, destruction or corruption of information or data
Integrity	The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.
Network Segmentation	To "segment" from other networks and into smaller network segments or zones, based on factors such as management authority, level of trust, functional criticality, to segment a network from other networks with a differing level of trust and amount of communications traffic required to cross-zone boundaries.
Notifiable Data Breach	A data breach happens when personal information is accessed or disclosed without authorisation or is lost. If the Privacy Act 1988 covers your organisation or agency, you must notify affected individuals and us when a data breach involving personal information is likely to result in serious harm; see OAIC Data breach preparation and response for more details.
Over the wire	Data in transit; getting data from point to point or segment to segment.
Proof of Concept	Showing that something is possible. For example, a PoC proves that a specific vulnerability can be used to gain unauthorised access or perform unintended actions on a system.
Removable Media	Computer storage devices designed to be inserted and removed from a computer/system, including but not limited to optical discs and USB flash drivers.
Stored-At-Rest	Information stored on Removable Media or backup media stored by the parties at off-site premises.
Supply Chain	Processes, people, and systems/tools used to deliver or receive products or services between a supplier and customer.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

7.0 Revision History

Rev. No.	Rev. Date	Revision Description	Author	Endorse/Check	Approved By
0	20/05/21	Created to strengthen Supply-Chain and External Dependencies Management security practices.	Nicholas Cop	C. Pennycuick / P. Nahrung	K. Lin
0.1	07/06/21	Minor change - Updated with comments from Phil Nahrung. No signatures required	Nicholas Cop		
0.2	20/07/21	Minor Change technical issue with duplicated workflows. Confirmed now correct by P. Nahrung / Chris Pennycuick. No signatures required.		Desley Wood	
1	01/11/21	Improved & defined Cyber Security Controls, in line with Industry standards & expectations.	Mathew Hepple / Nicholas Cop	C. Pennycuick / P. Nahrung	K. Lin
2	10.12.2024	Updated technologies and role names for periodic review. Made mirror corrections to document on wording	Mathew Hepple	Chris Pennycuick	Kevin Lin