Standard

Cyber Security – Supplier Supply-Chain Controls

Document Number – FNC-STD-IS-05

This document applies to the following site(s):

All Sites ☒	

Table of Contents

1.0 Purpose/Scope

The purpose of this Standard is to provide guidance to all parties regarding Stanwell's expectations in managing supply chain cyber security risk.

2.0 Responsibilities

Stanwell maintains a Security Management Framework which seeks to moderate Stanwell's security exposures and vulnerabilities, ensuring the cyber security posture and maintaining appropriate risk exposures across the organisation. The framework applies cyber security controls to mitigate security threats to risk tolerance, identifies and treats vulnerabilities and demonstrates Stanwell's compliance with relevant regulatory and compliance requirements.

Effectively managing cyber security risks reduces impact and exposure to parties within a supply-chain. Both Stanwell and Suppliers are responsible for managing applicable cyber security risks for their respective products and services.

3.0 Supply Chain Cyber Security Controls

Stanwell leverages a significant supply chain, including some that expose Stanwell to cyber security risk. Where the Supplier's products or services relate to cyber security risk, Stanwell expects the Supplier 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, and use the same degree of care as it uses 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 relevant to the product or services provided, if the Supplier becomes aware of an Electronic Incident or any Threat to their product or service, the Supplier will immediately upon becoming aware, notify Stanwell and take reasonable steps, at its own expense, to prevent, stop or remediate the Electronic Incident or Threat. Upon Stanwell's request, the Supplier will provide evidence of the prevention, remediation, or planned processes to prevent or remediate the Electronic Incident or Threat. If a data breach involving Stanwell's personally identifiable information (PII) occurs in a product or service hosted or managed by the Supplier, the Supplier will be required to make the Notifiable Data Breach report to the relevant Government Authorities.

Where the Supplier has developed software for Stanwell, the Supplier has taken suitable measures to ensure source-code for their Developed Software complies with the Customer Requirements and the Supplier must have conducted penetration tests for vulnerabilities in accordance with a secure Software Development Lifecycle process, and provide evidence reasonably requested by Stanwell to demonstrate this. The Supplier must ensure their Developed Software is:

a) designed and built with strong identifiable security properties and cyber security peer 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.

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 business.

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

- **Group Manager**; Strategic Procurement;
- **Manager**; Architecture Governance and Security;
- **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

Source	Reference
Business Procedure	GOV-PROC-48 Security Management Framework Procedure.
Tools	Cyber Security Requirements – contact Cyber Security for Tools ict_security@stanwell.com

6.0 Definitions

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.
Developed Software	means software developed by the Supplier and the Supplier 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 Supplier.
Electronic Incident	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, any Customer Data or any of the Customer's Confidential Information; or (b) any Supplier systems which are used to provide the Deliverable or Service to the Customer and any such Deliverable 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
Personal Information	Information that when used alone or with other relevant data, can identify, trace or distinguish an individual's identity.
Supply Chain	Processes, people and systems/tools used to deliver or receive products and/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, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

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.
	07.06.2021	Minor change - Updated with comments from Phil Nahrung. No signatures required	Nicholas Cop		
	20.07.2021	Minor Change technical issue with duplicated workflows. Confirmed now correct by NCop/C.Pennycuick. No signatures required.			

8.0 Attachments

None.