Policy
(Board Approved)

Information Systems Usage

Document Number – FNC-POL-04

1.0 Policy Statement

The purpose of this policy is to outline the acceptable use of Stanwell's Information Systems.

Inappropriate use of Information Systems exposes Stanwell to legal risk, increases vulnerability to cyber-attacks and could compromise Stanwell's network, business systems and commercial interests.

2.0 Scope

The policy defines the appropriate use of Information Systems, which include, but are not limited to Stanwell's mobile and computing devices, software, cloud services and network resources. This policy applies to all users of Stanwell's Information Systems, including employees, directors, contractors and consultants.

This policy should be read in conjunction with the *Information Systems and Tools Usage* eLearning module and forms part of Stanwell's Code of Conduct policy framework.

3.0 Content

This policy applies regardless of whether a user is working at a Stanwell site, remotely, or using a personal internet connection to access Stanwell's Information Systems. Stanwell provides user access to Information Systems to facilitate business communications and advance Stanwell's business objectives.

Limited personal use of Stanwell's Information Systems is acceptable, but must not:

- negatively impact the user's work performance;
- breach this or any other Stanwell policy;
- consume significant resources;
- result in degradation of service or interfere with the work activities of others;
- be used to transmit or store excessive personal content; or
- decrease cyber security.

3.1 Breach of Policy

A breach of this Policy may also be a breach of Stanwell's Code of Conduct and Fair Treatment Policy and Social Media and Mobile Device Allocation Procedures.

Failure to comply with this Policy will be taken very seriously and may lead to disciplinary action. In certain circumstances, a breach of the Policy could be referred to an appropriate authority for investigation. Several consequences could flow from a breach, including termination of employment or contract and prosecution.

Following a serious allegation resulting in reprisals against the Discloser, the recipient of the information (such as the Manager or People & Culture) must treat the disclosure confidentially

and immediately report the disclosure to the Whistleblower Protection Officer (Company Secretary), so that the information can be dealt with under the Protected Disclosure Procedure.

Intentionally false or misleading information **must not** be provided when disclosing information about a breach of this policy or in connection with an assessment or investigation about a breach of this policy. Disciplinary action may be taken against anyone found to have intentionally provided false or misleading information. In some circumstances, providing false or misleading information could be a criminal offence.

3.2 Unacceptable use of Stanwell's Information Systems

The following activities are prohibited. This list is not exhaustive, but is intended as a guiding framework for activities which fall into the category of unacceptable use, including:

- engaging in activities for personal financial gain or profit;
- soliciting for activities unrelated to Stanwell's business or in connection with political campaigns or lobbying;
- infringing on another's intellectual property rights (e.g. copyright, moral rights);
- infringing on another's reasonable expectation of privacy;
- representing a personal opinion as that of Stanwell, either explicitly or implicitly;
- perpetrating fraud;
- revealing Stanwell's proprietary, classified or confidential information;
- accessing Stanwell information which is not reasonably required for the user's role;
- accessing, downloading, transmitting or storing material which could reasonably be found to be offensive, violent, defamatory, sexually explicit, pornographic, discriminatory, used for bullying, harassment or which is intended to or may inflict harm to another party;
- accessing materials that may be perceived as inappropriate for the workplace (e.g. weaponry or gambling websites);
- downloading, installing or using unapproved Information Systems for Stanwell business purposes (e.g. signing up for a cloud service without authorisation);
- improper use of email distribution lists and broadcast messages;
- broadcasting of unsolicited views on social, political, religious or other non-business related matters;
- attempting to penetrate the computer or network security of any company or another system, or attempting to access, without authorisation, another person's computer, email or devices;
- intentionally introducing computer viruses or malware; and
- violating or attempting to violate any law, including accessing illegal websites prohibited by the Australian Federal Government or Queensland State Government.

Users of Stanwell's Information Systems will immediately report to Information Communications Technology the receipt of inappropriate or prohibited content or content that is in breach of this policy. The information will not be stored, saved nor distributed further. All Stanwell users of its Information Systems must take reasonable action to avoid breaching this policy, including requesting that senders do not transmit such material.

3.3 Usage Monitoring

Stanwell retains the right to monitor, review, audit, intercept, access and disclose information stored, created, received or sent using Stanwell Information Systems.

3.4 Software and Hardware

Only software licensed and approved for use by Stanwell is to be installed on Stanwell systems. Similarly, only approved cloud services may be used for Stanwell business purposes. Users who download files or use unapproved cloud services may be held responsible for costs incurred by virus damage or unlicensed software.

From time to time, investigations may be made to explore and better understand emerging technologies (for example, Artificial Intelligence services). Due diligence should be taken to confirm licensing implications. As ethical standards for these technologies are yet to be defined, caution should guide usage (for example, review output from such systems). Input of sensitive or confidential information is prohibited without permission from the ICT Architecture Governance and Cyber Security Manager.

Only Stanwell supplied computer hardware and devices are approved for connecting to the Stanwell Corporate Network. Personal devices may be connected to the Stanwell Guest Network after users have taken reasonable steps to ensure personal devices are free from virus, malware or other malicious software. USB memory sticks can only be used with permission from the ICT Service Desk as a last resort and must be scanned for viruses and encrypted if they contain sensitive information.

3.5 Mobile Devices

The Mobile Device Allocation Procedure outlines to whom Stanwell issues mobile devices Users of Stanwell-issued mobile devices, such as smart phones and tablets, are permitted reasonable private use. Private use of Stanwell-issued mobile devices must comply with this policy. Users may access Stanwell email, calendar and contacts from their Stanwell-issued or personal mobile device once they have completed a Mobile Device Connectivity Agreement.

All risks and costs associated with personal devices are to be borne by the user and are not the responsibility of Stanwell.

Where pool mobile devices are used, users are responsible for a device while it is in their custody. Devices must be collected and returned in-line with specific rules that govern the device pool.

3.6 Security

Unique usernames and passwords are used to access Stanwell's Information Systems, and in some cases, multi-factor authentication (MFA) tokens are also required. Passwords must be changed when periodically prompted at log in.

It is prohibited to use another person’s username, password or MFA token. Users must not divulge their password or MFA token to anyone, or record their password where it is unsecured and associated with their username. A user must immediately change a disclosed password. Users must not re-use passwords from external sites or previous employers. Users’ passwords must be unique to Stanwell Corporation.

Under the *Security of Critical Infrastructure Act 2018* Stanwell has an obligation to manage the risk of Operationally Sensitive Information being stored outside of Australia. To aid in meeting this obligation, permission must be sought from the Architecture Governance and Security Manager prior to taking devices that hold Operationally Sensitive Information outside of Australia.

Access to Sensitive Information Systems (including ERP and Payroll) will be reviewed periodically.

3.7 Remote access

All reasonable care must be taken to ensure that any device being used to connect to Stanwell's information Systems is free from spyware and viruses by ensuring the device has installed appropriate firewall and antivirus protection. Users of Stanwell's Information Systems must ensure that devices are not left unattended or placed in a position or state where unauthorised access could occur. All remote access is subject to usage monitoring defined in this policy.

4.0 Responsibilities and authorities

All users of Stanwell's Information Systems must:

- **ensure** that information is not released or used inappropriately and confidentiality is maintained and that Stanwell is not brought into disrepute when using Information Systems for professional or personal purposes;
- **comply** with this policy and the standard of expected behaviour detailed in the Code of Conduct; and
- **follow** the Protected Disclosures Procedure to report any breaches of this policy.

Managers and supervisors must make sure their employees and contractors know about the Systems Usage Policy.

The General Manager, Information and Communication Technology must ensure that:

- this policy is maintained to reflect the current technical, information and cyber environment;
- that all approved software is free from viruses, trojans, malware and anything which would adversely affect existing systems; and
- that hardware is fit for purpose.

The Executive General Manager Business Services must ensure that our people are aware of, have read and understood this policy.

The **Executive Leadership Team** members must comply with this policy and related procedure and make sure users follow this policy and related procedures.

The **Stanwell Board** has ultimate accountability for the Stanwell System Usage Policy.

5.0 Review and Consultation (Prior to Approval)

Review:
This Document is required to be reviewed, as a minimum, every two years.

Communication/Requirements after Update:
This policy will be published through Stanwell's Controlled Documents.

All employees will be advised of this policy as part of the induction process when commencing employment, when signing a Smartphone Connectivity Agreement if receiving a Stanwell issued mobile device, and when completing the relevant eLearning training every two years.

6.0 Definitions

Cloud Services are applications, or other ICT resources hosted on or accessed via the internet.

Information Systems are Information Communication Technology system or components of systems including, but not limited to: computers, software and network resources such as internet, email and voicemail, and mobile devices including phones, smartphones and tablets.

Operationally Sensitive Information as defined in the *Security of Critical Infrastructure Act 2018*, is information specific to a critical asset such as the Stanwell Power Station or Tarong power stations and includes layout diagrams, schematics, geospatial information, configuration information, operational constraints or tolerances information and data that a reasonable person would consider to be confidential or sensitive about the asset.

7.0 References

GOV-POL-30 Code of Conduct

PEO-POL-21 Fair Treatment

GOV-POL-27 Confidential Information

STM-PROC-19 Social Media

FNC-PROC-IS-18 Mobile Device Allocation

T-2107 Mobile Device Connectivity Agreement

GOV-PROC-39 - Managing Performance and Conduct Procedure

GOV-PROC-36 - Protected Disclosures and Complaints Procedure

FNC-PROC-IS-32 – IT Security Procedure

Safe Work Australia – Guide for Preventing and Responding to Workplace Bullying

Australian Human Rights Commission Fact Sheet “Good Practice, Good Business – Workplace Discrimination, harassment and bullying”

The relevant State and Federal legislation includes:

- *Age Discrimination Act 2004 (Cth)*
- *Anti-discrimination Act 1991 (Qld)*
- *Disability Discrimination Act 1992 (Cth)*
- *Human Rights Legislation Amendment Act 1995 (Cth)Australian Human Rights Commission Act 1986 (Cth)*
- *Integrity Act 2009 (Qld)*
- *Racial Discrimination Act 1975 (Cth)*
- *Security of Critical Infrastrcture Act 2018 (Cth)*
- *Sex Discrimination Act 1984 (Cth)*
- *Work Health and Safety Act 2011 (Qld)*
- *Work Health and Safety Regulations 2011 (Qld)*

8.0 Revision History

Rev. No.	Rev. Date	Revision Description	Author	Endorse/Check	Approved By
	1.07.2011	Policy adopted on merger			CEO
	25.05.2012	Policy updated to cover Mobile Phones			
0	27.11.2012	Policy finalised	D Elsmore	J Gregg	R. Van Breda
1	07.05.2013	Policy Updated	D Elsmore	J Gregg	R. Van Breda
2	01.07.2104	Policy Updated	J Philp	J Gregg	R Van Breda
3	26.07.2016	Policy reviewed and updated	D Elsmore	J Gregg	
4	17.01.2017	Policy reviewed and rewritten at the request of the Board	A Gray	J Gregg	Board
5	25.02.2019	Biennial review of this policy was undertaken. Updates include reference to new technology such as Cloud Services and enhanced security procedures for accessing and monitoring Stanwell's Information Systems.	P Inacio	J Gregg	Board
6	03.06.2021	Biennial review undertaken. No changes required at this review.	K. Lin	G Smith	Board
7	11.05.2023	Biennial review undertaken, minor changes dues to SOCI Act, emergence of AI and mobility.	K. Lin	G Smith	Board