Systems Usage

Document Number **–** FNC-POL-04

1. Policy Statement

The purpose of this policy is to outline the acceptable use of Information Systems at Stanwell. Inappropriate use of Information Systems unnecessarily exposes Stanwell to increased legal risk, risk of computer viruses and other threats that may compromise Stanwell’s network and business systems.

1. Scope

The policy applies to the use of mobile and computing devices, software and network resources at Stanwell and all users of Stanwell’s Information Systems, including employees, directors, contractors and consultants.

This policy should be read in conjunction with the eLearning module of the same name and forms part of Stanwell’s Code of Conduct policy framework.

1. Content

Information Systems includes, but are not limited to, computers, software and network resources such as internet, email and voicemail, and mobile devices including phones, smartphones and tablets.

The policy covers data accessed by and stored on Stanwell systems and 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 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; or
* be used to transmit or store excessive personal content.
  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. A number of consequences could flow from a breach, including termination of employment or contract and prosecution.

Where a serious allegation has been made that could result in reprisals against the Discloser, the recipient of the information (such as the Manager or Human Resources) 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 making a disclosure of 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.

* 1. Unacceptable use of Stanwell’s Information Systems

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

* Engaging in activities for personal financial gain or profit
* Gambling, other than a raffle or competition organised by or endorsed by Stanwell
* Soliciting others for activities unrelated to Stanwell’s business or in connection with political campaigns or lobbying
* Infringing on another’s intellectual property rights (eg copyright, moral rights)
* Infringing on another’s right to privacy
* Representing a personal opinion as being the opinion of Stanwell, either explicitly or implicitly
* Perpetrating fraud
* Revealing Stanwell’s proprietary, classified or confidential information
* Accessing, downloading, transmitting or storing material which could reasonably be found to be offensive, violent, defamatory, sexually explicit, pornographic, discriminatory, harassing or which is intended to or may inflict harm to another party
* Accessing information which is not reasonably required for the user’s role
* Downloading software that is not licensed and approved for use by Stanwell
* Inappropriate 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 computer or network security of any company or other system, or attempt to access without authorisation any other person’s computer, email or devices
* Intentionally introducing computer viruses
* Violating or attempting to violate any law
* Inappropriate use of email, including sharing content which may contain:
  + Sexually explicit material including images, cartoons and jokes
  + Material including gossip or innuendo about co-workers
  + Harassing, bullying or unwelcome propositions
  + Profanity, obscenity, slander or libel
  + Political, ethnic, religious or racial slurs

In the event that inappropriate or prohibited content is received from either an internal or external source, delete the email immediately and do not store or distribute further. Users must take reasonable action, including requesting that senders do not transmit such material.

* 1. Usage Monitoring

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

* 1. Software and hardware

Only software licensed and approved for use by Stanwell is to be installed on Stanwell systems. Users who download files may be held responsible for costs incurred by virus damage or unlicensed software.

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. USB memory sticks should only be used as a last resort.

* 1. Mobile Devices

Stanwell issues mobile devices in accordance with the Mobile Device Allocation Procedure. Users of Stanwell issued mobile devices such as smart phones and tablets are permitted reasonable private use.

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.

* 1. Security

Stanwell’s Information Systems are accessed by unique usernames and passwords. Passwords must be changed when periodically prompted at log in.

It is prohibited to use another person’s username and password. Users must not divulge their username or password to anyone, or record their password where it may be associated with their username. If a password is disclosed, the user must immediately change the password.

Access to sensitive systems (including ERP and Payroll) will be reviewed on an annual basis.

* 1. 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 appropriate firewall and antivirus protection. Users must ensure that devices are not left unattended or in a position where unauthorised access could occur.

1. Responsibilities and authorities

**Our people** must:

* **ensure** that Stanwell is not brought into disrepute when using Information Systems for professional or personal purposes, or release confidential information;
* **comply** with this procedure; and the standard of expected behaviour detailed in the Code of Conduct; and
* **follow** the Protected Disclosures Procedure to report any breaches of the Policy

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

**The General Manager Information and Communication Technology** must ensure that the Policy is maintained to reflect the current technical 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 trained on the Policy

The **Executive Leadership Team** members must comply with the Policy and Procedure and make sure that the Policy and Procedure are followed.

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

1. 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.

1. Definitions

|  |
| --- |
| Not applicable |

1. 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  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)](http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/I/IntegrityA09.pdf) * Racial Discrimination Act 1975 (Cth) * Sex Discrimination Act 1984 (Cth) * Work Health and Safety Act 2011 (Qld) * Work Health and Safety Regulations 2011 (Qld) |

1. 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 |