HR4.8 Information Technology

Purpose

1. To establish a clear written policy regarding the security of SAVVY Information and Communication Technology (ICT) that:
    a. Protects the organisation from risk of litigation
    b. Protects the organisation's information from a range of threats
    c. Protects end users from the risks associated with the Internet.

Alignment with Practice Standards

1. Module 2: Provider Governance and Operational Management

Legislative Alignment

1. NSW Industrial Relations ACT 1992
2. Privacy Act 1988 (Cth)
3. Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)
4. Workforce Surveillance Act 2005

Key Responsible Executive

Chief Executive Officer

For More Support

Your People Manager

Policy Statement

1. SAVVY is committed to ensuring that appropriate measures are in place to protect participant and corporate information, the ICT systems and equipment, as well the associated ICT infrastructure.

2. Security is an ongoing endeavour and includes hardware and software components, but also processes and the habits of users.

3. All these elements combined contribute to the security posture of the organisation.

Procedures

1. Network Access
    a. Access to ICT systems and platforms will be completed as part of the new starter induction process.
    b. End users are held accountable for any actions undertaken through their user ID, and as such maintain the confidentiality of their user ID and password.
    c. Password requirements are established via the individual software solution.
    d. End users never leave a computer system to which they are logged in unattended.

2. Information Protection
    a. Only authorised users are permitted to use SAVVY computer facilities.
    b. SAVVY data (including information and documents) is stored on file servers, which are backed up on a regular basis. Access to the servers is physically restricted and there is computer infrastructure in place that restricts electronic access, such as firewalls and proxies. Confidential information is stored in folders with appropriate permission levels ensuring access is restricted to only those employees who genuinely require it.
    c. Confidential information is never stored on the local drives of end user resources (laptops, PC's, smartphones, etc).

3. Mobile Resources
    a. Where a mobile phone is provided to an employee as a business tool relating to their role, these mobile devices are issued to end users with sim PIN, screen lock, and passcode activated. End users do not disable or change these settings.

4. E-Mail
    a. SAVVY uses a mail filtering service which restricts delivery of messages that are considered spam or meet certain other criteria.
    b. SAVVY restricts the delivery of email where the email:
        i. Contains a known virus
        ii. Contains an attachment of a specific file format which may be prone to virus such as executable files, script files etc.
        iii. Is caught by mail filtering service

5. Viruses
    a. SAVVY systems are protected by anti-virus programs which are updated regularly. It is the job of these programs to monitor, detect, and quarantine/remove viruses, should they exist.
    b. End users are constantly vigilant for viruses. E-mails where the sender cannot be verified or that contain an unfamiliar attachment, are viewed suspiciously, they are generally treated as spam and deleted permanently by the end user. If a virus is suspected, the team member should stop work immediately and report the issue to the IT Department.

References to other SAVVY policies and external sources

1. HR4.9 Workplace surveillance
2. HR4.18 Social networking

Summary of attachments

1. Nil

Version Control

1. 1 April 2023 - New Policy Creation