Information Technology Security Policy

Section 1 - Definitions

(1) For the purpose of this policy:

a. Information Security Management System (ISMS)
    i. A management framework based on a business risk approach to establish, implement, operate, monitor, review, maintain and manage Information Security.
b. Information System Custodians
    i. The Technology Services based managers of information systems.
c. Information System Owners
    i. The business stakeholders of information systems.
d. Information System Administrators
    i. The technical staff responsible for administering systems.

Section 2 - Policy Statement

Part A - Policy Declaration

(2) Southern Cross University acknowledges the strategic and operational importance of our Information Technology (IT) environment. Effective Information Security measures are critical to maintaining the confidentiality, integrity and availability of University information and services. While Technology Services implements a number of central measures to maintain a secure environment, all end users are responsible for, and play a role in, ensuring that these measures remain effective.

Part B - Policy Description

Overall Objectives

(3) This policy seeks to ensure that University requirements for Information Security are met by:

a. Outlining practices that enable the establishment and maintenance of a safe and secure computing environment,
b. Defining standards for Information Security that adequately protect the confidentiality, integrity and availability of University information and systems.

Part C - Content and Implementation

Account (Login) and Password Standards

(4) Staff and students are issued individual user accounts to access various SCU IT systems.

(5) The username (or login id) will generally be unique to an individual and will be generated by the University along with an initial password.

(6) Your username and passwords are the principal element protecting unauthorised access to University information and systems.

(7) For this to be effective, users should be aware of and observe the following practices in relation to passwords:

a. Change your password as soon as practicable after you receive it.
b. Use a password with a minimum of eight (8) characters that includes at least one upper case character and at least one numeric character.
c. Change your password regularly (generally every 90 days where practicable).
d. Keep passwords confidential i.e. don't disclose them or keep them written down.

(8) Further details on management practices including how to change your SCU password and how to choose a safe password can be found on SCU's "How to change your password" website.

Virus and Malware Prevention

(9) Viruses and malware are unauthorised programs that either disrupt the operation of the computer, or capture information which may then be used to gain unauthorised access to information or resources. Examples include persistent pop-up advertising, automated opening of unintended web sites or capture of sensitive information such as passwords or banking details.

(10) The installation of these programs usually occurs without the knowledge of the user and is often referred to as an "infection".

(11) To protect against viruses and malware, all devices connected to the University network must have up-to-date virus protection software along with relevant operating system and application updates installed.

(12) University owned workstations and servers will have anti-virus software installed as part of the Standard Operating Environment and will be regularly and automatically updated with system and application updates.

(13) While these measures provide good protection against "infection" from viruses and malware, there are a number of steps users should take to further reduce their risk:

a. Avoid clicking on unknown or untrusted websites that offer 'spyware or virus infection removal' programs. It is also worth noting that illegal or "pirate" software downloads are a common source of viruses and malware.
b. Avoid opening unknown or untrusted attachments.
c. Avoid clicking on links in emails suggesting you have won something or asking you to respond to or update your account details.

(14) As staff may also use personal computers to access University systems, anti- - virus software is made available (at no charge) for all current staff to download and install on their home computers.

(15) This software can be downloaded and installed by visiting the Technology Services website

Spam and Phishing Emails

(16) Spam and Phishing are forms of unwanted email that may seek to gain access to personal information which could be later used for criminal activities such as illegal data access or fraud.

(17) They are also frequently used to deliver viruses or malware.

(18) While SCU has implemented technologies to significantly limit the amount of these emails received by staff and students, their ever changing nature means that from time to time, spam or phishing emails may still be received.

(19) It is important that users do not reply to these emails or click on the web links contained in them.

(20) For the avoidance of doubt, the University will NEVER ask staff or students to validate their account details (e.g. username and password) by visiting a web site, or ask users to provide identity information such as usernames, passwords, full names, date of birth, drivers licence, credit card or other confidential information via email.

(21) For further information on phishing including tips on how to recognise phishing emails, visit the SCU Information Security site on Phishing or the Information Security Site on Identify Theft. If a user is in any doubt as to the contents of such an email, they should contact the Service Desk (email servicedesk@scu.edu.au) to check its authenticity.

Mobile Devices

(22) An increasing number of Mobile devices are now being used to access to University systems as well as to store both personal and University information.

(23) Sensitive information commonly stored on these devices could include phone numbers, passwords, emails and SMS messages.

(24) To protect this information in the event the device is lost or stolen, wherever possible, users should enable passcode protection on these devices.

(25) Prior to disposing of, or transferring the device to another user, user data must be removed.

(26) Technology Services is able to provide advice and assistance with this.

(27) If you are uncertain as to how to do this, please contact the ITS Service Desk.

Security Breach and Incident Management

(28) Security breaches and incidents have the potential to disrupt business operations and/or adversely impact the University's reputation.

(29) As part of managing the IT security risk to the University and its users, Technology Services may monitor and investigate computer usage activity or suspected security incidents.

(30) The operation of this monitoring is outlined in the Computing Conditions of Use policy.

(31) Where this monitoring highlights a potential security or policy breach, systems or accounts may be disabled without notice until such time as the issue is resolved.

(32) While Technology Services does implement University wide security systems and strategies, staff and students must continue to take reasonable steps to prevent security incidents.

(33) Where staff become aware of, or suspect that a security breach or incident have occurred (such as virus or malware on their computer, or accidental reply to spam/phishing email), they must immediately report the incident to the Service Desk.

(34) The Service Desk will provide advice or assistance to deal with the issue or concern.

Information Classification and Access Control

(35) IT based systems and information are a strategic asset of the University and have varying degrees of sensitivity

and criticality.

(36) Access controls will be used to limit who has access to systems or information to ensure the confidentiality, integrity and availability of IT systems and information is maintained.

(37) An SCU information classification scheme provides the following categories:

a. Public (open to the public)
b. Internal Use (restricted to authorised University constituents)
c. Confidential/Restricted (restricted to recognised University delegates) The University will, through the various system owners, determine which classification data or information falls into and will ensure appropriate access controls exist to protect this University Asset.

Section 3 - Related Policies, Documents, Legislation and Strategic Priorities

Southern Cross University Policies and Guidelines

(38) This policy provides a framework for other Information Security related policies at Southern Cross University.

Related Legislation

(39) Information Technology security is impacted by various legislative Acts associated with areas including privacy, copyright, duty of care, acceptable use and cybercrime.

(40) The University has a legislative duty of care to ensure that reasonable steps are in place to adequately protect Information Technology based Systems and Systems Information.

Institutional Context

(41) This policy is intended to enable and support the University's operational business processes, as well as facilitate strategic priorities relevant to the University.

Section 4 - Responsibilities

(42) All Users will be responsible for:

a. ensuring they are aware of, understand and comply with this policy; and
b. notifying any breaches of IT Security to the Service Desk.

(43) The Information Technology Steering Committee and Chief Information Officer will be responsible for:

a. strategic representation of the University's requirements for Information Security;
b. providing input into the risk management process for Information Security; and
c. providing input into the development and content of policies where appropriate.

(44) VC and Executive will be responsible for:

a. ensuring the University's legal, auditory, regulatory and contractual obligations are met with compliance in relation to Information Security.

(45) Information System Business Owners will be responsible for:

a. determining appropriate classifications of information as either public, internal use or confidential/restricted, as well as specify retention periods where applicable; and
b. ensuring business continuity plans are in place for systems owned.

(46) Information System Technology Services Custodians will be responsible for:

a. ensuring Technology Services based security controls are applied in accordance with the information classification associated to it by the system owner, including applying appropriate IT security access controls and ensuring backup and recovery procedures are in place.

(47) The Director, Technology Services, will be responsible for:

a. provision and management of the technical infrastructure to provide security protection; and
b. ensuring infrastructure based Information Security resourcing is aligned with the University's requirements.

(48) Head of Work Units e.g. Faculties, Departments, Centres, Schools, Directorates and the University Library, will be responsible for:

a. ensuring security incidents and breaches that occur in their area are reported; and
b. maintaining local business continuity plans to operate in conjunction with Disaster Recovery.

(49) The Manager, IT Infrastructure will be responsible for:

a. maintaining standards and architecture for security technologies;
b. ensuring Technology Services infrastructure based systems are maintained in line with security requirements; and
c. assisting in audits, security testing, incident response and applying technical controls.

(50) The Information Security Manager will be responsible or:

a. maintaining the ISMS and associated Information Security related policies and procedures;
b. providing research, guidance, advice and recommendations on Information Security; and
c. assisting with internal and external audits and conducting risk management assessments.

(51) Information System Administrators will be responsible for:

a. implementing Information Security policy and related codes of practice on information systems; and
b. monitoring and reporting the security of the information systems under their technical control.

Status and Details

Status	Historic
Effective Date	14th August 2012
Review Date	14th April 2015
Approval Authority	Vice Chancellor
Approval Date	10th August 2012
Expiry Date	17th February 2019
Head of Work Unit	Naomi Downs Chief Information Officer
Enquiries Contact	Naomi Downs Chief Information Officer