Network Policy

Section 1 - Definitions

(1) For the purpose of this policy:

a. Access Control - The process of limiting access to the resources of a system only to authorised programs, processes, or other systems.
b. Authentication - Authentication refers to the verification of the authenticity of either a person or of data. Authentication techniques usually form the basis for all forms of access control to systems and / or data.
c. Data classification - Data classification is the conscious decision to assign a level of sensitivity to data, as it is being created, amended, enhanced, stored, or transmitted. The classification of the data should then determine the extent to which the data needs to be controlled / secured.
d. Encryption - The process by which data is temporarily re-arranged into an unreadable or unintelligible form for confidentiality, transmission, or other security purposes.
e. Firewall - A device and/or software that prevents unauthorised and improper transit of access and information from one network to another.
f. Hardware -Physical equipment: - processors, screens, keyboards, mice, printers, scanners, network routers, hubs, bridges, racking, disk drives, portable drives, etc.
g. Information Systems - The computer systems and information sources used by an organisation to support its day-to-day operations.
h. ID Cards - Identification cards
i. Internet - Worldwide information service, consisting of computers around the globe linked together by telephone cables.
j. Intranet - A Local Area Network within an organisation, which is designed to look like, and work in the same way as, the Internet. Intranets are essentially private networks, and are not accessible to the public.
k. Intrusion - The IT equivalent of trespassing. An uninvited and unwelcome entry into a system by an unauthorised source.
l. IT - Information Technology
m. LAN - Local Area Network - a group of computers and associated devices that share a common communications line or wireless link.
n. Network - A configuration of communications equipment and communication links by network cabling or satellite, which enables computers and their terminals to be geographically separated, while still connected to each other.
o. Operating Systems - Computer programs that are primarily or entirely concerned with controlling the computer and its associated hardware, rather than with processing work for users. Computers can operate without application software, but cannot run without an operating system.
p. Passwords - A string of characters input by a system user to substantiate their identity, and/or authority, and/or access rights, to the computer system that they wish to use.
q. 18. Protocol - A set of formal rules describing how to transmit data, especially across a network. An example of a protocol is: TCP/IP, the protocol used on the Internet to send and receive information.
r. 19. Remote Data Store - An off-site location, i.e. some distance from the computer system, devoted to the

storage of computer media, and in particular backup files. Storage of data files etc. in another department of the same building is not considered to be 'remote'.

s. SCU - Refers to Southern Cross University
t. University - Refers to Southern Cross University
u. UPS - Uninterrupted power supply
v. VPN - Virtual Private Network (logical LAN through switching technology)

Section 2 - Policy Statement

Part A - Policy Declaration

(2) The Network Policy for the University is designed as a resource to assist the University in maximising the integrity, availability and efficacy of University information whilst minimising the risk of unauthorised collection, disclosure, modification or destruction of University data.

(3) Access to the University Network is the starting point for extending the reach of the University, expanding the educational and research resources available to staff and students and also for encouraging internal collaborations within the University itself. The University is committed to the principle that information should be shared subject to privacy and confidentiality requirements and consequently to an open flow of information within the University.

(4) The University's Network is a powerful tool for institutional effectiveness and efficiency only to the extent that network connections are easily established and broadly available. The University must make decisions concerning security of the network based on an objective assessment of potential risks balanced against the costs and other organisational priorities. Responsibility and accountability for the security and privacy of the network and the data that it contains rests solely with the University.

(5) The University has become more and more reliant on this network for business function and efficiency.

(6) The University network is a single entity that supports all core information systems and services for the University and its partners. Other networks may exist within the University that operate independently.

Part B - Policy Description

Objectives

(7) This policy has been developed for Southern Cross University and forms part of the Technology Services Policy Framework. It seeks to define the management of the computing network within the University and provide a foundation for the conditions of use that informs the University community of their rights and responsibilities.

Scope

(8) This policy applies to management of the University Network and is specifically related, but not limited to, those facilities administered by Technology Services.

Part C - Content and Implementation

(9) This Policy addresses detail necessary for the overall Network Policy to operate effectively throughout the University. It covers the areas of:

a. Access and Availability;
b. Security;

c. Management and Monitoring;
d. Equipment Acquisitions and Installation;
e. Maintenance and Support;
f. Training; and
g. Advice and Assistance.

(10) This policy is underpinned by the Computing Conditions of Use Policy.

Access and Availability

Provision of Network Access Control

(11) The Director, Technology Services will ensure that the network is capable of providing access controls to the University network based on defined security levels that reflect requirements for access to information system needs as defined by the information systems owners.

Part D - Network Availability

(12) Network availability will ensure continuity of the University's information systems. These information systems will determine network availability and network maintenance windows will be negotiated with the information system owners.

Part E - Authority to be connected to the SCU network

(13) Any partner or joint venture wishing to connect to the University network must conform to SCU network security policies in order to protect both the University and the partner involved.

Physical Security

Location of Network Equipment

(14) The sites chosen to locate network equipment and cabling will be suitably protected from physical intrusion, theft, fire, hazardous materials, flood and other intrusions.

Physical Access Control to Secure Areas

(15) All premises housing network equipment must be protected from unauthorised access using an appropriate balance between simple ID cards to more complex technologies to identify, authenticate and monitor all access attempts.

Communications Cabinets

(16) All network devices and communication services located outside of designated secure areas should be contained in secure cabinets with locking hardware. There should be no signage indicating the presence or importance of such facilities.

Environmental Conditions

(17) When locating network equipment, adequate cooling and power supplies will be provided to guard against excessive ambient temperature / humidity.

Uninterrupted Power Supply (UPS)

(18) An uninterruptible power supply is to be installed to ensure the continuity of essential services during power

outages. All hardware devices required for continued operation will be powered through the UPS.

(19) An annual check will be conducted to ensure that all UPS devices comply with industry standards.

Management and Monitoring

Monitoring Network Access and Use

(20) The University network will be monitored to identify breaches of the Computer Conditions of Use Policy.

Firewalls

(21) The University network will be protected by Firewalls in accordance with industry best practice.

Network Audit

(22) An audit of Network policies, procedures and standards will be conducted periodically in order to evaluate current policies and to identify key risks that may have arisen.

Interconnecting with other Networks

(23) Any external network that is connected to the University network will be considered untrusted.

Accessing Trusted Information through an External Network

(24) Users wishing to access corporate information systems on the University network from external networks will require adherence to SCU standards for strong authentication.

Equipment Acquisitions and Installation

Network Equipment Acquisition

(25) The acquisition of all network equipment must meet current standards and be approved by the Director, Technology Services.

Network Installation

(26) Network installation and cabling will be required to meet current standards and specifications as outlined by Technology Services. All new installations will require auditing and approval by Technology Services before being connected to the SCU network.

Preferred Suppliers

(27) The installation, maintenance or alteration of network equipment and cabling must be carried out by an SCU preferred supplier or contractor. Technology Services must be notified of all such work and is subject to approval by Technology Services.

Maintenance and Support

Media Management (Data Storage)

(28) Network configurations, documentation and software will be stored in a secure location. Duplicate copies will be made and kept at appropriately secure offsite locations.

Network Disaster Recovery Plan

(29) A network disaster recovery plan will be established and maintained so that the University will have a controlled,

timely, and effective response to a disaster. The main goal of the Network Disaster Recovery Plan will be to avoid or minimise damage to the University's resources, reputation and ability to operate. This plan will be regularly tested.

Equipment Maintenance

(30) Equipment maintenance and replacement strategies will be in place to ensure that loss or failure of network components is recoverable in a timely fashion. There will be adequate network hardware arrangements in place to ensure the network can be maintained with minimal disruptions to the information systems operating at the University.

Change Control

(31) All changes to system hardware and configurations are to be performed through formal change control procedures to ensure that all changes are recorded and included in network documentation.

Training

Network Training

(32) The Director, Technology Services will be responsible for the training of the University community in policies, procedures and standards for the Network.

(33) Training will be made available to reflect the individual staff member's responsibility for configuring and maintaining the network. Staff not involved in the actual function of the network need to be aware of the relevance of policies that drive the network.

Advice and Assistance

(34) For further advice and assistance, staff and students should first contact the relevant IT Service Desk

a. Lismore Campus - Email servicedesk@scu.edu.au or Phone: 02 6620 3698
b. Tweed/Gold Coast Campus - Email servicedesk@scu.edu.au or Phone: 02 6620 3698
c. Coffs Harbour Campus - Email chec.servicedesk@scu.edu.au or Phone: 02 6659 3080

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

(35) Institutional Context - The issue of network security has become more prevalent as a greater amount of information is stored and passed using networked systems. There is often a belief that security is purely about ensuring the safekeeping of information. From the perspective of the University, Network Security refers to:

a. Legitimate use;
b. Confidentiality;
c. Integrity;
d. Availability; and
e. Audit ability.

Legislation

(36) There are a number of legislative requirements that the University must abide by on both a State and Federal level. While much of this information relates specifically to privacy related issues, it is important that other relevant

legislation is taken into account, in regard to such areas as archiving, evidence and Freedom of Information. The University also needs to be aware of issues of contract law in regard to arrangements made with regard to the security of data provided by and to corporate joint venture partners.

(37) Of specific concern in the preparation of this document are the following:

a. Privacy and Personal Information Protection Act (NSW) 1998
b. Privacy Act (Commonwealth) 1988
c. National Privacy Principles have a significant impact on the need to ensure that at least reasonable efforts are made to secure electronic data:
    i. An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

(38) The Privacy and Personal Information Protection Act (NSW) 1998 states at Section 12 Retention and security of personal information:

> "A public sector agency that holds personal information must ensure:
>
> (c) that the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse,"

(39) This Policy should be read in conjunction with the following:

a. Telecommunications Act 1997
b. Broadcasting Services Amendments (Online Services) Act 1999
c. Computer Related Commonwealth Law
d. Privacy and Personal Information Protection Act 1998
e. Privacy Act 1988

Section 4 - Responsibilities

Responsibilities and Approvals

(40) The Director, Technology Services will be responsible for establishing standards for network equipment, protocols for which these systems operate and arrangements with preferred suppliers.

(41) The Director, Technology Services is responsible for ensuring the availability of network services as dictated by the needs of the University.

(42) The Director, Technology Services is responsible for ensuring the management of the Network is consistent with the University's needs.

Information Systems Owners

(43) Responsibility for information systems that operate on the University network will fall to the Head of the department from which the system originates. For example, Financial Operations will be the custodian for the E-Trans system.

Users

(44) The University community will use the University Network in a responsible manner consistent with the Computing Conditions of Use Policy.

Section 5 - Procedures

(45) Refer to Part C - Content and Implementation.

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	Damon Ferris Executive Director, Global