UNSW Technology Policy:

UNSW Data Network Connection Policy

UNSW Policy	
Responsible Officer	Chief Information Officer
Contact Officer	Manager Infrastructure Services Support UNSW IT Services Ph: x 51141; email: g.sawyer@unsw.edu.au
Approving Authority	Chief Information Officer
Date Approved	*2 August 2006*
Date Effective	*18 September 2006*
History	New policy, although process has been implemented informally as a result of Net98 project.
Review Commencement Date	September 2008
Related Policies & Documents	UNSW IT Security Policy; UNSW IT Security Policy Standards and Guidelines; Electronic Recordkeeping Policy; Rules Relating to Student Use of Computing and Electronic Communications Facilities at UNSW; Student Misconduct Rules; UNSW Code of Conduct
File Number	*[will be provided by Policy Management Unit]*

1. Preamble

The University recognises that access to, and security of, its data communications network is critical. This document establishes the responsibility of UNSW IT Services in managing the network as well as its authority to detect, prevent or rectify incidents or risks which threaten the network and thus the activities of the University and its members.

1.1 Purpose

UNSW IT Services, as a key part of its role, is responsible for the ownership, development, installation, operation and maintenance of the data communications network on behalf of UNSW and its members. With this responsibility comes the authority to take action necessary to safeguard the integrity of the network to minimise and contain potential risks to the University and its members, both operational and legal, from the consequences of network-related security violations and misuse.

In this context, the purpose of this policy is to state clearly both UNSW IT Services' responsibility and authority for the University's network infrastructure and devices connected to that infrastructure and; users' responsibilities in using such devices.

1.2 Principles

1.2.1 UNSW IT Services holds sole responsibility for, and authority over, the UNSW data communications network.

1.2.2 Only registered users or those given permission by the designated UNSW IT Services Authority are permitted to use the UNSW data communications network.

1.2.3 Only UNSW IT Services (or its approved delegate(s) may modify/attach devices to the UNSW data communications network.

2. Scope

This policy applies to:

- The University's internal data communications network, devices connected to it and supplied by, or otherwise approved for connection , by UNSW IT Services, and the network's connection to AARNet and the Internet;
- All devices using this infrastructure, including those connecting via wireless technology;
- All users of such devices;
- The protection, detection and action against threats, including but not restricted to:
    - Virus attacks
    - Denial of service attacks
    - Hacking (internal or from external sources)
    - Downloads and uploads of unacceptable material
    - Unacceptable content of outgoing email
    - Unsolicited bulk email (spam)
    - Unauthorised connection of devices to the network.

The coverage of this policy includes threats from, but excludes risks to:

- On-campus devices not approved for network connection by UNSW IT Services;
- On-campus networks not installed or approved by UNSW IT Services;
- Off-campus networks and devices.

3. Definitions

For purposes of this policy, unless otherwise stated, the following definitions shall apply:

Designated UNSW IT Services Authority: UNSW Chief Information Officer or authorised delegate within UNSW IT Services.

Network Devices: Active equipment required to operate the University's data network. These devices provide transient services including switches, routers, firewalls and wireless access points.

4. Policy Statements

This policy addresses the following:

- Who can and cannot make use of the University's data connection network;
- Who can and cannot extend, remove or change the cabling and fibres that constitute the University's data connection network, either within or between University buildings;
- What connections or changes can and cannot be made to the network;
- What devices can and cannot be attached to the network;
- Who can and cannot attach such devices;
- What they can and cannot use it for;
- How UNSW IT Services manages the control of the network and the approval of connections both from devices and from other networks;
- How UNSW IT Services is able to detect or prevent security threats and rectify the consequences of those threats to the network;
- What sanctions are available to UNSW IT Services when threats and misuse are encountered, to deter further misuse of the network.

4.1 Users of the Network

Only registered users or those given permission by the Designated UNSW IT Services Authority are permitted to use the UNSW data network.

4.2 Modifiers of the Network

Only UNSW IT Services and University approved data communications contractors are permitted to modify the network infrastructure.

4.3 Network Devices

Only UNSW IT Services and University approved data communications contractors are permitted to install such devices, which will be solely managed by UNSW IT Services. These devices shall be located in UNSW IT Services cabinets. No other equipment shall be housed within these cabinets.

4.4 User Devices

Any device, other than network devices (as defined in Section 3) is defined as a user device. User devices fall into two categories – client and non-client:

4.4.1 Client devices

Client devices are defined as equipment generally used by one person with traffic terminating on the device, eg PC's, laptops, Macintoshes or PDA's. Network connectivity is achieved by either plugging this equipment directly into an activated data point on the University network or indirectly by enabling a connection via a wireless access point.

University-owned client devices may be connected to the network by any user of the University provided the equipment is used in accordance with the aims and policies of the University) and for no other purpose.

4.4.2 Non-client devices

A non-client device, eg a server, is defined as equipment which provides a service to one or more users.

University-owned non-client devices may be connected to the network by competent users provided the recognised owner of the equipment shall agree to keep it updated in terms of anti-virus and operating system security patches.

5. Legal & Policy Framework

Use of UNSW networks will generally be subject to regulation consistent with all relevant legislation and UNSW policies and guidelines. Self-regulation is expected and the University will impose limits or take action only where and when necessary to protect its data network.

6. Implementation

6.1 Responsibilities

UNSW IT Services are responsible for:

- Managing access to the Data Network by the University's users;
- Managing the risks of any network device connected to the network and implementing any necessary security measures to protect the network;
- Managing the provision of IP addresses; protection via access lists; authentication and data point activation.

UNSW IT Services holds sole authority and responsibility for the connections of networking equipment to the network, eg hubs, switches, routers and wireless equipment.

Traffic entering the UNSW network will be monitored and managed by UNSW IT Services.

Owners of any equipment connected to the network are responsible for:

Ensuring that all machines have the latest level of anti-virus software and security patches installed, and that these are kept up to date.

6.2 Support

The Infrastructure Services Support team within UNSW IT Services can provide guidance and advice regarding the implementation of the policy. Contact the IT Service Desk in the first instance for assistance.

6.3 Compliance and Breaches

UNSW IT Services, on behalf of the University, are responsible for investigating, containing and resolving breaches of security, and may disconnect, block traffic to/from, or log information about any machine using the data network.

UNSW IT Services are authorised to investigate any apparent breaches of this policy.

If a breach is found, UNSW may ban users without notice, pending resolution of the incident. Depending upon severity or unlawfulness, breaches may be reported to the NSW Police.

Where a proven breach of this policy occurs, the relevant organisational unit will be liable for all costs incurred in rectification.

6.4 Communication Strategy & Implementation Plan

[This will be developed as an Appendix to this document]

How will the University Community be informed of changes to University practice? Identify communication & training, as required.

7. Evaluation

The success of this policy and its technological implementation will be evaluated periodically.

Stakeholders, including users, University staff, the student body, Heads of Budget units, Deans and the University Executive will be consulted as part of any evaluation.

Evaluation criteria will include:

- The degree of compliance with the Policy
- The degree to which network facilities are available to staff and students.

8. Associated Documents

Commonwealth Spam Act, 2003

http://www.austlii.edu.au/au/legis/cth/consol%5fact/sa200366/

UNSW Code of Conduct (Staff)

http://www.hr.unsw.edu.au/employee/codecond.html

UNSW IT Security Policy, Standards and Guidelines

http://www.its.unsw.edu.au/policies/pol_security.html

UNSW Electronic Record-Keeping Policy

http://www.infonet.unsw.edu.au/poldoc/electronic_recordkeeping.htm

Student Misconduct Rules

http://www.infonet.unsw.edu.au/poldoc/stumis.htm

Rules Relating to Student Use of Computing and Electronic Communications Facilities at UNSW

http://www.infonet.unsw.edu.au/poldoc/rulcomp.htm

9. Document Version Control

4/7/06	V0.1	G.Sawyer	Initial draft
25/7/06	V1.0	J. Beatson	Re-format to new PMU template

10. Document History and Approval

This technology policy was developed by Greg Sawyer, Manager Infrastructure Services Support, UNSW IT Services. It was peer-reviewed by the ISS team and by Jenny Beatson, IT Policy and Compliance Officer.

The policy was approved by Chief Information Officer Tim Cope on August 3, 2006.

……

T. Cope

Chief Information Officer

University of new South Wales