MASSEY UNIVERSITY

Information Technology Services

Data Network Policy and Procedures

Palmerston North and Auckland Campuses

Document Approval

Principles endorsed by Vice Chancellor’s Executive Committee
21st September 1998

Document Revision

First Draft - May 1997
Second Draft August 1997
Third Draft - September 1997
Published Version - September 1997
First Edit - August 1998
Second Edit - September 1998
Data Network Policy and Procedure Contents

1. Introduction

2. Infrastructure
   2.1 Physical Media
   2.2 Active Network Components
   2.3 Protocols
   2.4 Addressing of Network Interfaces
   2.5 Monitoring
   2.6 Management of the Network
   2.7 Security

3. Network Devices
   3.1 Physical Connectivity
   3.2 Configuration Parameters
   3.3 Protocols - Transport Layer
   3.4 Network Addressing
   3.5 Prevention of Unauthorised Access
   3.6 Fiscal Responsibility
   3.7 Security

4. Operating Systems
   4.1 Configuration and Management
      4.1.1 Non Standard Operating Systems
      4.1.2 Standard Operating Systems
   4.2 Applications Services
   4.3 College and Department System Security
   4.4 Network User Authentication

5. College, Institute, School and Departmental Private Networks

6. Trading Group Networks

7. External Organisations Campus Network Connectivity

8. Network Services
   8.1 Gateway Services
   8.2 Remote Access Services
   8.3 Name Services
      8.3.1 Domain Naming
      8.3.2 WINS
      8.3.3 DHCP/RARP/Bootp
1. **Introduction**

Fulfilment of the University’s Strategic Plan is dependant on the establishment and maintenance of a communications infrastructure of both high integrity and reliability. The data network which comprises both the campus/site networks and the interconnecting networks forms a significant and mission critical component of this communications infrastructure. It is essential that appropriate policies are established and adhered to. This will ensure that the University can meet the stated objectives identified in the Strategic Plan and deliver mission critical business applications.

**Principles**

S The University will seek to provide parity of communications services across all campuses and sites.

S All communications infrastructure is owned and managed by the University.

S The University requires that all network users be authenticated to use the communications infrastructure.

S The University will on behalf of it’s network users negotiate and maintain all external network service level agreements with network provision organisations.

S Activities which could compromise the delivery, integration and security of the communications infrastructure and/or network services will not be permitted.

S The University will manage on behalf of it’s network users the campus and inter site networks to provide the most cost effective solution to meet business requirements.

S The University will present to the external world a single, managed entity to facilitate seamless communications with a multi campus, multi sited organisation.

S The University reserves the right to disconnect without prior notification any component of the network in order to protect the security and/or integrity of the whole network.

2. **Infrastructure**

2.1 **Physical Media**

The physical media is the internal building cabling or external feeder building cabling that is used to construct the physical network. This cable can include fibre optic, unshielded twisted pair, shielded twisted pair, voice grade copper cable, thin net coaxial cable and video coaxial cable.

All physical cable infrastructure or media is owned by the University and is the responsibility of Information Technology Services or their designated representatives. The following policies apply in order to protect network users from disruption of services.

**Policy**

- No modifications or extensions can be made to the cable infrastructure by any unauthorised persons.
No network attached devices which includes servers, network printers, terminals, servers, repeaters, hubs, bridges, switches and routers may be disconnected from the University network by any unauthorised persons.

In special circumstances local patching may be delegated to an appropriately trained and University authorised College, Institute, School and Departmental staff member.

Procedure to Change Cable Infrastructure

A College, Institute, School or Department network user that requires network cabling changes and/or additions should consult with the Technical Services Manager of Information Technology Services providing the following:

- The nature of the infrastructure change or addition that is required.
- The building and room location where the change or additional network outlet is required.
- The network device that is going to be attached to the changed or new network outlet.
- The date the change or addition is required by.
- The source of funds in the form of a University purchase order to which the cost of the change or addition is to be debited.

2.2 Active Network Components

Active network components are defined as equipment which is attached to the physical cable to create the network. This includes repeaters, bridges, routers, repeating hubs, switches, print and terminal controlling devices.

In order to provide an integrated University wide communications infrastructure the following policy applies.

Policy

- All network components are owned by the University and are the responsibility of Information Technology Services or their designated representatives. The redeployment, substitution or upgrade of this equipment is determined and managed by the Network Section of Information Technology Services on behalf of the University network users.

Procedure

Should a College, Institute, School or Department network user require changes or an increase to the capacity of the network or changes in the logical configuration of the network they should consult with the Communications Manager of Information Technology Services identifying the following:

- The nature of the network services or configuration change that is required.
The building and room location where the configuration change is required.
The date the service or change is required by.

The cost of the network service change request will be established and then submitted for funding approval to the appropriate University funding committees.

2.3 Protocols

The protocols considered in this section are the first layer protocols (ISO layer 1) that run over the physical network and can be categorised into;

- Campus Local Area Network Protocols
- Wide Area Network Protocols

The policies for the first layer protocols are required so that network devices which include personal computers, printers, terminal servers and scanner/photocopiers can be attached to the University campus or site networks and wide area networks. Adherence to these policies will ensure that network attached devices will communicate appropriately with the network equipment that is used to create these networks.

Policy

- The University will only support Ethernet II framing over the physical media on the campus or site networks.
- The University will only support point to point protocol (PPP) and frame relay as the transport protocol on the serial links which form the wide area network used for inter-campus connectivity, satellite office and remote access.

2.4 Addressing of Network Interfaces

The addressing in this section relates to the network interfaces that attach the network devices to the physical campus or site networks. The University network policies require each network device to have an address associated with it so that it can participate in network communications successfully without risk of devices interfering with each other.

Policy

- All network interfaces will have a unique and static address provided by the interface manufacturer.
- Network users are not permitted to intentionally or otherwise tamper or change the manufacturer provided network interface address.
- All network interface addresses will be registered in the University administration database before the network equipment is permitted to be attached to the
University campus or site networks.

Procedure

For registration please refer to section 3.1 - physical connectivity.

2.5 Monitoring

Network monitoring can be defined as the process or procedure that is used to gather electronic statistical or diagnostic information on the performance or usage of University’s campus, site or wide area networks.

In the course of traffic analysis and fault diagnostics, the University through Information Technology Services reserves the right to monitor, decode and store frame level network information. The constraints of privacy legislation dictates that this information will not be released to network users or third party organisations.

Information Technology Services network support personnel are bound by the University Code of Practice (see section 2.7 for document web address) for the use of information and communications systems with respects to network monitoring.

Policy

- Information Technology Services or it’s designated network agent are the only agents authorised by the University to perform network monitoring for the purpose of electronic statistical or diagnostic information gathering.

Procedure for Monitoring

Should a College, Institute, School and Department suspect a network event which requires monitoring, the Head of College, Institute, School and Department should contact the Communications Manager of Information Technology Services on ext. 4041. To initiate monitoring, the Head of College, Institute, School and Department should state the nature of the monitoring required, urgency and duration.

It should however be noted that network monitoring will only be undertaken if the criticality of the monitoring is established by the requesting College, Institute, School and Department.

2.6 Management of the Network

This section covers the management of the physical network and active components that are configured to create the campus or site networks and wide area networks. These active components are managed to ensure they are functioning correctly without fault in the University networks and network events information is relayed and reacted to by Information Technology Services network support personnel.
Policy

- Information Technology Services or its designated agent are the only agent authorised by the University to alter the physical network topology, redeploy active components or isolate any segment of the network to undertake fault diagnostics or capacity management.

- All active network component logical configurations will be managed from an integrated University network management system.

- Colleges, Institutes, Schools and Departments are not permitted to implement any form of network management which could actively change the logical configuration, poll or trap statistical information from these active components without the knowledge and written authorisation from the Director of Information Technology.

2.7 Security and Privacy

The security and privacy of the University campus, site and wide area networks are paramount and any identified breaches of security may result in disciplinary action as identified in the University Code of Practice for the Use of Information Communication and Processing Systems (http://www.massey.ac.nz/~wwits/codeofpractice.htm).

Policy

- The University will not allow under any circumstances physical or electrical tapping of the network infrastructure which could facilitate the collection, monitoring or decoding of network traffic.

3 Network Devices

3.1 Physical Connectivity

The University requires all network connected devices which includes personal computers, workstations, network servers, printers, terminal servers, scanners, repeaters, hubs, bridges and routers to be registered and maintained in the University administration database. The University administration database is used for network authentication, authorisation and attributing network related connection and traffic charges to the network device, user, College, Institute, School or Department.

Policy

- All network devices must be registered in the University administration database prior to being attached to the University campus or site network.

- All changes to network attached devices must be registered in the University administration database at the time of change.
Procedure to Connect Network Devices

To connect a new network device to the University campus or site networks, College, Institute, School and Departmental staff member must discuss and validate the requirement with the Communications Manager of Information Technology Services.

Once it has been established that it is possible to connect the network device the client must register the network device with Information Technology Services and this can be done by completing a network registration form. The network registration form can be obtained by contacting the Information Technology Services Reception on extension 5163 or email to ccadmin@massey.ac.nz.

After registration the network device may be connected by an appropriately authorised computer support personnel.

Procedure to Move Network Connect Devices.

College, Institute, School and Departmental staff that wish to move a network connected device from one location to another location, should (to assess the viability of the move) contact the Communications Manager of Information Technology Services on ext. 4041. If the move is viable the following information will be required:

- The building and room location where the network device is going.
- The description of the network device including the IP number and host name.
- The planned date of the move.
- Whether there are College, Institute, School and Departmental support staff that can undertake the move.
- A University purchase order or funding authority which authorises the move and associated costs.

3.2 Configuration Parameters

This section covers the configuration parameters of the network settings for network attached devices that use the University campus or site networks. These settings are maintained in the University administration database. They are essential for network attached devices to operate on the University network, ensure wide area communications and minimise the impact of network changes to the users.

Policy

- All network devices must be configured to support a dynamic configuration protocol, eg dynamic host configuration protocol (DHCP) or reverse address resolution protocol (RARP).

- Colleges, Institutes, Schools and Departments are not permitted to implement services that respond to configuration parameter requests from network devices.
3.3 Protocols - Transport Layer

The protocols that are considered in this section are at the transport layer (ISO layer 3) and are configured to run on the network interfaces of the network attached devices.

In order to reduce the complexity, maintenance and support costs of the University networks the number of inter computer communications methods (protocols) will be constrained.

The University will encourage and support Colleges, Institutes, Schools and Departments to migrate from legacy system protocols (such as IPX) to standard IP environments where ever possible (currently IP version 4).

Policy

- The University campus networks are designed to support the following protocols.

  - IP
  - EtherTalk Phase 2

- The University will not support protocols that can not be routed on the campus or site networks and the wide area networks.

- Routing non routable protocols can only be accommodated if they are tunnelled through IP. This will only be allowed in special circumstances due to the inefficient use of bandwidth and has to be authorised by the Communications Manager of Information Technology Services.

Procedure

Colleges, Institutes, Schools and Departments that require advice on the migration of protocols should contact the Communications Manager of Information Technology Services on extension 4041.

3.4 Network Addressing

The internet protocol (IP) network address block assigned to Massey University by Asia Pacific Network Information Centre (APNIC) is currently two Class B networks (130.123 and 161.140) and one Class C network (202.49.82). These are reserved for exclusive use of the University.

Each network device has a unique network identifier or Internet Protocol (IP) address that is assigned to the network device when it becomes active on the University campus networks. Such addresses are provided with other associated configuration information from the University administration database when the device becomes active on the University network.

The following policies must be adhered to so that individual devices will not have to be
manually reconfigured with every network topology change and the network device address ensure that the device can correctly participate seamlessly in University wide communications.

Policy

- All network attached devices will be required to support and implement protocols which allow a dynamic address assignment.
- All network attached devices must have a University allocated network address. Network users are not permitted to allocate their own addresses.
- Colleges, Institutes, Schools or Departments are not permitted to implement or maintain separate address registers or allocation processes.

3.5 Prevention of Unauthorised Access

This section covers the prevention of unauthorised access to infrastructure devices such as routers, bridges, terminal servers and repeating hubs. Alterations or changes made to network devices can disrupt services or compromise network security which could result in the loss or destruction of the University information asset.

Policy

- Network infrastructure devices that support an authentication protocol must be configured to prevent unauthorised access to the device.
- Network infrastructure device password will be routinely changed and a register of current passwords will be held in a secure location.

3.6 Fiscal Responsibility

All network attached devices, user codes and the associated resources consumed will be attributed to the account code associated with the chargeable entity. Arrangements for postgraduate students allowing restricted user status may be made. Undergraduate students attract consumable charges only.

Collected charges are used to meet network traffic consumable costs associated with the delivery of University wide network service.

Policy

- All staff (including short term visitors), postgraduate and undergraduate students requiring access to the University network infrastructure must be registered in the University administration database.
- Full registered user codes may not be shared.
Colleges, Institutes, Schools and Departments are responsible for any charges associated with staff, postgraduate and undergraduate student network user. This includes visiting staff who consume University network resources.

Procedures

User Registration

User registration is initiated by completing the user registration form which can be obtained for the Information Technology Services Reception by contacting extension 5163 or sending email to ccadmin@massey.ac.nz.

Billing Enquiries

Billing information can be obtained by contacting the Departmental its reports access controller. If the user is unsure of who the contact is within their Department they can send email to its.reports.help@massey.ac.nz.

For all billing inquires users are requested to contact Computer Services reception on 5163.

3.7 Security

In order to support the protection of the University information assets, network policies are designed to provide a high level of security and integrity associated with University campus, site and wide area networking services.

The security and the integrity of the University’s campus, site and wide area networks are of paramount importance to the continuing operation of the University. Any activity which knowingly or otherwise places the operation of the University networks in jeopardy may result in disciplinary action.

Policy

- The University will not allow unauthorised persons to attach network devices capable of monitoring the network for any purpose.

- The University will not allow anyone to change or alter in any way the Ethernet or IP addresses assigned to a network attached device.

- The University will not permit anyone to knowingly assume the network identity of another user for whatever purpose.

Further background information on the use of University infrastructure, systems and services can be obtained from the University Code of Practice for the use of information communications and processing system at the following web location http://massey.ac.nz/~wwits/codeofpratice.htm.
4 Operating Systems

4.1 Configuration and Management

4.1.1 Non Standard Operating Systems

The introduction or use of non standard operating systems may compromise network security and performance thereby exposing the University to the potential loss of its information assets.

Policy

- For all non standard operating systems the University network and systems management must be alerted to the intended use of this operating system to assess the impact of its use.

Procedure

For all non standard operating systems, deployment must be formalised and approved by writing to the Director of Information Technology.

4.1.2 Standard Operating Systems

The mismanagement of multi-user operating systems may compromise network security and performance thereby exposing the University to the potential loss of its information assets.

Policy

- Formal permission to establish a local server on the University network must be obtained from the Head of Department, School, Institute or College Pro Vice Chancellor.

- Multi user systems must have a nominated systems administrator contact who is suitably qualified and a full time employee of the University.

- A register of system administrators will be maintained by ITS.

- Systems administration privileges must be restricted to specific users for each system and this information must be made available upon request to the Director of Information Technology.

- It is recommended that passwords for systems administration users should be registered with the Head of College, Institute, School and Department to ensure access can be gained in emergency should the systems administrator not be available.
The University provides configuration guidelines with respect to standard operating systems, this information can be found at the following world wide web location.

http://www.massey.ac.nz/~wwits/services/system_config/unix_systems.html
http://www.massey.ac.nz/~wwits/services/system_config/winnts_frame.html

Procedure

Nominated systems administrator details must be forwarded to the Director of Information Technology and should include the following details:

- Name
- Day time contact number
- Out of hours contact number
- Email address
- Home address
- A declaration attesting to their awareness and knowledge of the University Code of Practice; Data Network Policy and Procedures and other related Information Technology regulations.

4.2 Application Services

Performance, reliability and delivery of campus or site network services can be compromised by the introduction of local College, Institute, School or Departmental services. In order to avoid such disruption it is necessary to ensure that appropriate consultation occurs.

Policy

- College, Institute, School and Departmental network or system applications must not conflict with University wide network or system services.

- College, Institute, School and Departmental network or system services must not be mounted without, appropriate consultation with University network and/or systems support staff.

- College, Institute, School and Departmental initiatives that mount services for University customers and clients will be monitored by the University to ensure appropriate security, integrity and quality of service.

Procedure

Colleges, Institutes, Schools or Departments should contact the Communications Manager of Computing Service to provide the following details about their planned service.

- The location of the new service.
- The business case or justification for the new service.
- Evidence of University approval process having been completed.
- The anticipated bandwidth requirements, both campus and wide area, for the new service.
- The planned start date for the new service.
- The source of funds for the new service establishment and on going costs associated with the new service.

4.3 College and Departmental Systems Security

The section considers security issues related to network attached devices or work stations that are administered by College, Institute, School and Departmental support staff.

Policy

- The nominated College, Institute, School and Departmental systems administrator will be responsible and accountable for any security breaches that originates from a network attached work station or system for which they are responsible.

- System administrator are responsible for implementing an acceptable use policy in line with the University Code of Practice for network attached work stations and systems for which they are responsible.

(See Massey University Code of Practice as an example http://massey.ac.nz/~wwits/codeofpractice.htm)

4.4 Network User Authentication

Before any user may access a the University’s network or system service they must be establish an authorised identity. This section considers the network user authentication requirements and the administration of these requirements.

Policy

- Any network user that requires access to University network infrastructure, internal or external services must be authenticated against the University Authentication Service.

- All user accounts will be password protected and network users must be encouraged to select discrete passwords and change them on a regular basis.

5. College, Institute, School and Department Private Networks

In order to ensure an integrated, University wide communication and information systems, the establishment of isolated networks should only be considered in exceptional circumstances. The establishment of private networks may compromise the security, functional integrity and parity of service across the University. Further the University will
not support any networks which compromise the University routing or VLAN integrity on campuses or sites.

Policy

- College, Institute, School and Departmental private local area networks and/or private connections to external organisations will not be permitted to connect to the University network.

- Colleges, Institutes, Schools and Departments may in exceptional circumstances have disjointed local area networks (i.e. not connected to the University campus or site network) but they will be required to register the disjoint network attached devices as per section 3.

Procedure

Colleges, Institutes, Schools or Departments should contact the Communications Manager of Information Technology Services to discuss the following details about their planned network requirements:

- The reason for the disjoint network.
- The specific security or bandwidth requirement for the disjointed network.
- The number of devices in the disjointed network.
- The infrastructure requirements for the disjointed network.
- The source of funds for the implementation of the disjointed network.
- The planned date of the implementation of the disjointed network.

6. **Trading Groups Networks**

In order to ensure an integrated, University wide communication and information systems, Trading Group networks will be established as isolated networks.

Policy

- Trading Groups are not permitted to implement private local area network on the University campuses or sites.

- Trading Groups that require network infrastructure on campus or in a University owned building are required to consult with Information Technology Services.

Procedure

Trading Groups that require campus network connectivity for specific projects must write to the Communications Manager of ITS identifying the following:

- The reason for the network.
- The specific security or bandwidth requirement for the network.
- The number of devices in the network.
- The infrastructure requirements for the network.
- The source of funds for the implementation of the network.
- The planned date that the network is required by.

7. **External Organisation Campus Network Connectivity**

This section considers external organisations wishing to connect to the University campus or site networks.

**Policy**

- No commercial organisation may connect any network device to the campus or site network other than through the University Commercial Network for Web Server Telehousing purposes (currently sited at Turitea).

8. **Network Services**

8.1 **Gateway Services**

In order to ensure an integrated, University wide communication and cost effective external access, the University provides a number of gateway services for electronic mail, Telnet, file transfer and world wide web. The use of the gateway services ensures security, functional integrity and parity of service across the University and preserves the University Corporate image and controls the cost of access.

**Policy**

- Colleges, Institutes, Schools and Departments must use the University gateway services for communicating with the world.

- Colleges, Institutes, Schools and Departments are required to adhere to the University address structure when communicating through the University gateway services.

- Colleges and Department are not permitted to establish independent external connections and gateway services will external network suppliers.

- The University will monitor gateway traffic and protocols and enforce where appropriate traffic management policies to ensure that priority traffic is not impacted by general traffic.

8.2 **Remote Access**

In order to ensure the security of the University network and reduce the cost associated with telephone system resources being used for individual desk top remote access, the University has implemented a remote access service in Palmerston North for staff and post
graduate students.

Policy

For details on the policies relating to the University remote access service please refer to the following web location.

http://www.massey.ac.nz/~wwits/services/remote_access/mraintro.htm
http://www.massey.ac.nz/~wwits/services/remote_access/mraservice.htm

For details on the policies relating to desktop modems please refer to the following web location.

http://www.massey.ac.nz/~wwits/services/telecomm/telpol.html

Procedure

For Colleges and/or Department that have specific remote access requirements that can not be provided for through the University remote access service should contact the Communications Manager at ITS providing the following information.

- The type of remote access service required.
- The network attached devices which will be involved in the provision of the proposed service.
- The College, Institute, School and Departmental security policies that are enforced for the proposed service.
- The date the proposed service is required by.
- The source of funds which has been identified for the provision and on going operational costs for the proposed service.

8.3 Name Services

8.3.1 Domain Naming

This section considers the policies that apply to the internet domain naming service and the concept of domain naming in the Windows NT server environments. In order to provide an integrated network, which is simple to administer and reduces confusion among the network users the following naming policies must be adhered to. This will ensure that the University maintains it’s Corporate image in the internet community and seamless operations with other name services.

*Internet Domain Naming Service*

The domain name management and administration for the University has been delegated to the University by the Internet Society of New Zealand (ISOCNZ).

The University uses Network Information Services (NIS) on the majority of it’s servers which do not support sub domain or hierarchical domain structures and therefore the
following policies apply.

Policy

- The University operates a flat name space and will not support requests for sub domains.

- Where for strategic reasons Colleges, Institutes, Schools and Departments have a need of external domains to reference a University IP address (refer to section 3.4), this may be permitted on application to the Communications Manager. These Domain names will be registered and administered on behalf of Colleges, Institutes, Schools and Departments.

- Inclusion of a University IP address (refer to section 3.4) in internet domains served by external organisations is prohibited.

Procedure

Colleges, Institutes, Schools and Departments that require an external organisation to point at a University address range should write to the Communications Manager of Information Technology Services providing the following information:

- The nature of the strategic relationship and associated requirements between the College, Institute, School and Department and the external organisation.
- The intended address which the external organisation wishes to share.
- The time frame for the implementation of the reference.
- The College, Institute, School and Department and external organisation contacts.
- The Head of College, Institute, School and Department authority.

Windows NT Domain

This section considers the policies that are required for use authentication in the Windows NT environments. For the University’s infrastructure to remain integrated and secure, it has been necessary to establish a University authentication domain and the following policies apply.

Policy

- Colleges, Institutes, Schools and Departments who mount Windows NT resources (printing, applications, file space, etc) will be required to establish these resource in a Windows NT resource domain.

- The University administers and maintains the authentication domain and will require all other Colleges, Institutes, School and Departmental Windows NT resource domains to use the authentication domain for the purpose of user authentication.
Procedure

Colleges, Institutes, Schools and Departments that are implementing Windows NT server that want to participate in the University’s Windows NT environment must consult with the Communications Manager of ITS to establish the following details.

- The intended resource domain that the College, Institute, School and Department is trying to establish.
- The intended name of the resource domain.
- The time frame for the implementation of the resource domain.
- The server administrator contact details.

8.3.2 Window Internet Name Services (WINS)

This section considers the policy that apply to the WINS service which provide IP address to Computer Name translation for Windows 95 and Windows NT network attached devices. Adherence to the policy is required to ensure seamless communications in the University Windows network environment.

Policy

- The University maintains and supports a WINS service and therefore Colleges, Institutes, Schools and Departments will not be permitted to run a WINS server under any circumstances as this could prevent network users connecting to file and print services.

8.3.3 DHCP/RARP and Bootp

DHCP, RARP and Bootp are integral to the operation of the University network and the delivery of network services and therefore will be provided as a University wide communications services. These services supply the network information required by a network attached device to function and communicate on the University campus networks.

Policy

- The University maintain and supports DHCP, RARP and Bootp services and therefore Colleges, Institutes, Schools and Departments will not be permitted to implement these services under any circumstances as this could compromise the integrity of information forwarded to all network users and prevent them communicating on the University networks.