

## University of New England

### INFORMATION AND COMMUNICATIONS INFRASTRUCTURE POLICY

#### Document data

<b>Document Type</b>	Policy and Procedures
<b>Administering entity</b>	Information Technology Directorate
<b>Date approved</b>	26 <sup>th</sup> November 2009
<b>Approved by</b>	Information and Communication Technology Committee
<b>Indicative time for review</b>	Annually
<b>Responsibility for review</b>	Director, Information Technology
<b>Related policies or other documents</b>	
<b>TRIM Reference No.</b>	D09/34605

#### 1. Rationale and Scope

- 1.1 This policy provides a standardised, consistent and robust approach to campus Information and Communications Technology (ICT) infrastructure on campus.
- 1.2 It empowers the Information and Communications Technology Committee (ICTC) as the appropriate governing body with the means to:
  - a. direct ICT policy in accordance with the University's strategic goals;
  - b. have a clear and effective means to control costs relating to ICT; and
  - c. to ensure that security, reliability and availability goals are met by all UNE parties responsible for ICT.
- 1.3 This Policy document replaces the following policies:
  - a. Protocol for the Design, Installation and/or Modification of the Data and Voice Network Infrastructure at UNE (Internal Building Cabling); and
  - b. Departmental Server Guidelines

#### 2. Principles

- 2.1 ICT systems are a core part of UNE and are vital to its day-to-day operation.
- 2.1 Reliability, cost effectiveness, security, integrity and maintainability of ICT infrastructure are kept within standards required by the University in order to function appropriately and meet strategic goals.

#### 3. Authentication Systems

- 3.1 UNE will have the minimum required number of centralised authentication systems.
- 3.2 Duplication or provision of alternate authentication systems may not occur without the written approval of the Director of Information Technology (DIT) or his nominee.
- 3.3 Additional centralised authentication systems may only be provisioned with the written approval of DIT or his nominee.
- 3.4 All alternate or duplicated authentication systems are to be removed and replaced with the approved central authentication systems.
- 3.5 Removal of duplicated authentication systems will not be immediate and will occur as the natural result of following this policy.

#### **4. Servers**

- 4.1 Procurement of departmental servers must be approved by ITD before authorisation of hardware purchase.
- 4.2 Procurement of servers will be performed in accordance with the relevant University procurement policies.
- 4.3 ITD will approve server requests without prejudice where the requisition is shown to not duplicate the function or data retention of existing or planned University information systems; including but not limited to:
  - a. Network services which are considered core to university requirements
  - b. Centralised authentication and authorisation services
  - c. Student Information and Financial control systems
- 4.4 ITD will conditionally approve server requests where the requisition is shown to justifiably duplicate an existing service and has been endorsed by the Information Technology Investments Governing Board, the ICTC and Service Quality Governing Board (or equivalent).
- 4.5 ITD will approve server requests which represent a direct replacement of existing equipment in order to provide business continuity. A service delivery review may be recommended in order to plan for changes or consolidation of services provided by the departmental server in question.

#### **5. Equipment Security**

- 5.1 Server equipment should be located within an area which is physically secure at all times.
- 5.2 Access to server equipment should be limited to authorised personnel only. Risk of damage to server equipment from physical threats, e.g. fire, water, theft, interruption to communications or power; should be minimised through the appropriate selection of equipment location and the adoption of appropriate risk management controls.
- 5.3 Environmental conditions which could affect the operation of equipment, such as temperature and humidity, should be kept within the operating parameters of the relevant hardware.
- 5.4 Equipment should be protected from power supply disruption.
- 5.5 Communications cabling should be of the appropriate standard and connected in such a manner as to prevent disruption of service.
- 5.6 Supporting utilities should be inspected and maintained at regular intervals.
- 5.7 Server equipment should be under maintenance and support agreement.
- 5.8 Equipment should be maintained in accordance with manufacturers recommended service procedures.
- 5.9 Records should be kept of all actual and suspected equipment faults.

#### **6. Data protection and system availability**

- 6.1 Server data should be configured on storage systems which provide adequate redundancy (as recommended by ITD), reducing the risk of data loss via hardware failure.
- 6.2 Backups of server configuration and essential data should be performed at regular intervals.
- 6.3 Backup retention should be sufficient to provide a restore window capable of a complete systems and data restore.
- 6.4 Backup media should be stored in a secure facility, physically separate from the server equipment.
- 6.5 Servers should be patched at appropriate regular intervals to reduce the risk of system compromise, with critical patches being applied as a priority.

- 6.6 Complex passwords should be used for administrative accounts
- 6.7 Administrative passwords should be documented and stored in a secure method in order to ensure business continuity in the event of injury, loss or change in personnel.
- 6.8 Departmental servers should not be providing a service which is required to be “highly available”. High availability services should be provided by centralised IT systems and resourced appropriately.
- 6.9 **Procedures**
  - a. ITD is to be advised of the location of all off-site backup storage locations so that data can be recovered in the event of a disaster or personnel loss.
  - b. In order to maintain business continuity backups should be stored at least 400m away from the data being backed up so that a 200m radius exclusion zone in the event of a disaster does not affect both the data and the backups.
  - c. ITD has the right to audit any server providing a service to UNE staff or students for compliance with these policies
  - d. Should a server not comply with these policies after a reasonable period of time as determined by the DIT or his nominees, ITD may move the server to an appropriate server room location and assume control of the server in order to meet compliance. In this case ITD will also provide a written explanation to the relevant HOS or Director.
  - e. Finance procurement and purchasing procedures shall require approval from the DIT or his nominee of any purchase or attempted purchase of server hardware.

## 7. **Data and Voice Network Infrastructure**

- 7.1 The Data and Voice Network Infrastructure is defined as the following
  - a. all physical cabling infrastructure including but not limited to copper and fibre technologies up to and only including wall sockets at the client endpoint
  - b. all spectrum used to contain radio, laser or any other technology not requiring transmission across a physical medium
  - c. all equipment including but not limited to passive, electronic or optical technologies used for the transmission or distribution of Data or Voice Communications.
- 7.2 ITD is responsible for the planning, design, security and maintenance of the UNE Data and Voice Network Infrastructure.
- 7.3 ITD is the authority responsible for monitoring and regulating the uses to which the Data and Voice Network Infrastructure is put where policy and agreed parameters have been defined.
- 7.4 Where new uses of the Data and Voice Network Infrastructure, or uses outside the agreed parameters are proposed the ITD is responsible for bringing these to the attention of Information and Communications Technology Services and Service Quality Governing Board who will make a determination taking into account resourcing and related issues. Any policy changes required as a result of this determination will be passed onto the ICTC for approval.
- 7.5 **Procedures**
  - a. All installation, upgrades and maintenance will be performed or approved by appropriately qualified staff or contractors approved by the DIT or his nominee via a fair and impartial process.
  - b. Before any new component of the Data and Voice Network Infrastructure can be used it must be tested by ITD staff or meet the specifications they define via standards approved testing mechanisms.
  - c. The DIT or his nominee must be advised of all proposals to implement, upgrade, extend or modify any Data or Voice Network infrastructure within buildings on the campus.

- d. All planning and design work for any proposed additions, upgrades, extensions or modifications to any part of the Data or Voice Network infrastructure network must conform to the "University of New England Design Standards and Procedures" (Section 17 Telecommunications).
- e. All components proposed for use must meet the specifications laid down by ITD in the "University of New England Design Standards and Procedures" (Section 17 Telecommunications)
- f. All work shall be implemented and completed to the standards contained in the "University of New England Design Standards and Procedures" (Section 17 Telecommunications).
- g. Copies of all 'as installed' plans and test results showing compliance with standards set out in the "University of New England Design Standards and Procedures" (Section 17 Telecommunications) will be forwarded to ITD
- h. Upon receipt of these documents ITD will authorise, and undertake, connection of the installation to the network.
- i. Any additions, extensions, upgrades or installations or any other modifications carried out to the Data and Voice Network infrastructure in contravention of this protocol will be decommissioned and rectified at the discretion of ITD. The full cost of the rectification will be borne by the operational unit responsible for the contravention.