University of South Australia

IT Network Policy

Responsible Officer:	Deputy Director: Infrastructure
Last Updated:	March 2014
Date of Review:	March 2017
Audience/Application:	Staff, Students and External Users
Related Documents	– Acceptable Use of Information Technology (C-22) – IT Purchasing, Maintenance & Disposal Policy – UniSA Design & Construction Guidelines – Data Centre Access and Management Policy

1. PURPOSE

This policy governs the development and management of the University IT network.

The Telecommunications Act and the University's contractual arrangements with carriers and other network providers impose some limitations on the use that may be made of the University's IT network and its connections to the internet and the public telephone system.

Access to the University's IT network infrastructure is available to staff, students and in some case external users. All users of the University's IT network should be aware of their responsibilities as described in the Acceptable Use of Information Technology (C-22)

2. SCOPE

In the context of this policy the University IT network includes:

- the inter-building and intra-building wired or wireless transport systems up to and including the "socket on the wall",
- the devices that route and manage the transport of data, video and voice signals, including perimeter and interior firewalls, routers, switches, telephone handsets, voice mail servers, and wireless network base stations and access points, and
- the interconnections to and from voice and data networks external to the University

3. RESPONSIBILITIES

The Information Strategy & Technology Services Unit (ISTS) is responsible for:

- designing, installing, documenting, monitoring, maintaining, and supporting the IT network (including the wireless network);
- determining standards for equipment suitable for connection to the University IT network;
- managing University wide agreements which permit interconnections to and from voice and data networks external to the University;
- ensuring compliance with telecommunications and other relevant legislation;

- providing a guaranteed dial tone for emergency telephones and systems, building management systems, fire monitoring systems, and security telephones;
- the management of IP address spaces (public and private), telephone extension number allocation and wireless radio frequency spectrum and SSIDs; and
- the provision of remote access services (including VPN, dial up modems and remote access servers) which permit access to the University's Information Technology facilities from offsite locations.

Cost centres managers are responsible for:

- the costs of providing equipment (such as computers, telephone handsets, and facsimile machines) and associated wiring to connect these devices to the IT network.
- ensuring all equipment that connects to the IT network meets applicable ISTS policies, standards and guidelines. Refer to the IT Purchasing, Maintenance & Disposal Policy
- for more details.

4. MODIFICATIONS

All cabling modifications or additions to the IT network must be coordinated through ISTS to ensure they comply with national, state and local codes as applicable to wiring methods, construction and installation of data and communications cabling systems, and equipment, as detailed in the UniSA Design & Construction Guidelines.

Only ISTS and approved nominated contractors are authorised to place equipment or cabling in wiring closets, equipment rooms, etc.

Users must not make any modifications to the IT network. Only wireless networking equipment installed and managed by ISTS is allowed to be connected to the University IT network.

Where existing equipment needs to be relocated, or new equipment needs to be connected, advice should be sought from ISTS to confirm that the network connection point is activated and suitable for the intended use, and that the new equipment is suitable for connection to the network.

Any device (hardware or software) which has the potential to interfere with the IT network must not be connected, installed or run on any computer connected to the IT network without the prior approval of the Chief Information Officer (CIO) or nominee.

5. ACCESS TO NETWORK INFRASTRUCTURE

Access to communication rooms, cable trays, conduits, risers and cabling is restricted to ISTS staff and contractors authorised by ISTS staff to undertake work in these areas. The Data Centre Access and Management Policy details how access to communication rooms is governed.

Equipment cannot be installed in communications rooms without prior written approval from the Chief Information Officer (CIO).

Access to the management features of any part of the IT network is limited to ISTS staff.

6. DISCONNECTION

Any device (hardware or software) which:

- interferes with the normal operation of the IT network; and/or
- is identified as a security risk.

may be logically or physically disconnected from the IT network.

When a device is disabled in this way, ISTS staff will attempt to contact the owner of the device, and/or relevant IT support staff, to advise them of the action taken and the reason why.

7. THIRD PARTY ACCESS

Permanent connection or access to the IT Network by a third party (for example by commercial organisations onsite) must be approved by the Chief Information Officer (CIO) or nominee.

8. LOGGING OF USE

The University may maintain logs of voice and data network usage for management, service rectification and accounting purposes without infringing the privacy rights of individual users.