1. Introduction

1.1. This information security policy document covers management, operation and use of the University data networks and is a sub-document of Information Security Policy (ISP-S1).

1.2. Definitions:

- **Network device** - a device that is part of the network infrastructure such as a router, switch, gateway, firewall, network wall socket, wireless access point etc.

- **Networked device** - any device that can communicate via the University network including: PCs, servers, workstations, Personal Digital Assistants (PDA’s), environmental sensors, access control systems, cameras, printers, scientific instruments, IP phones etc.

- **Device** – a “Network” or “Networked” device (see above).

- **Network interface** - part of a device that enables it to communicate via a network.

- **MAC (Media Access Control) address or “Ethernet address** - a 48-bit number used to uniquely identify each network interface in a network. The network interfaces in most devices have a unique MAC address set during manufacture.

- **IP** - Internet Protocol. Currently IP version 4 (IPv4) is used as the communication language by almost all devices connected to the University network.

- For correct operation IP network interfaces must be configured to use suitable 32-bit numbers for the “IP address”, “subnet mask”, “default gateway” etc. (The IP address of a device is often also referred to as its “network address”.)

- **Two significantly different levels of network connectivity are available depending on whether the user connects to the “wired” or “wireless” network. Wireless connections provide access to the Internet and to a limited range of Internet enabled University computing services.**

- **Network Organisation** – an IT Services term meaning a group of networked devices which are managed by a particular sub-organisation of the University.

- **Network Authority** - an individual, nominated by a Head of Department, to be the primary point of contact for matters relating to security of networked devices in a particular Network Organisation; they authorise connection of devices to the “wired” network and may delegate this task to assistants known as “Network Authorisers”.

- **NDOR** - the IT Services “Network Device Online Registration” database. It holds network address and other data about devices registered for connection to the “wired” network.
1.3. This document includes statements on:
- Management of the network
- Network design and configuration
- Physical security and resilience
- Connecting devices to the network
- Management of networked devices
- Acceptable use of the network
- Network services and protocols
- Controlling access to and from other networks
- Incidents and emergency procedures

2. Background

2.1. This policy refers to the University network, including the “wired” and wireless networking around the University. The University network covers all buildings on the main University campus, most off-campus University locations and University presence in the three University Hospitals of Leicester.

3. Management of the network

3.1. The high level strategy for central IT provision, including data and voice networks, is determined by the Information Communications Technology Committee (ICTC). IT Services is responsible for the campus networks. The IT Operations Team within IT Services has principle day to day accountability for managing and operating the networks.

3.2. IT Services is responsible for administering all network devices such routers, switches, gateways, firewalls, network wall sockets, wireless access points and wall sockets forming the University network infrastructure. The Campus network cabling extends to nearly all University buildings and departments and is also the responsibility of IT Services. Note:
- No unauthorised changes or other interference with these network devices or cabling is permitted.
- Moves, changes and other reconfigurations of cabling and users’ network access points will only be carried out by staff authorised by IT Services according to procedures laid down by them.
- IT Services is responsible for providing the enterprise wireless network service. Departments are prohibited from establishing their own wireless networks and adding wireless access points since these may conflict with the central provision of wireless hotspots.

3.3. The implementation of new equipment or upgraded network software or firmware must be carefully planned tested and managed. Formal change control procedures, with audit trails, shall be used for all changes to critical systems or network components. IT Services reserves the right to make changes to network security as and when necessary. This may be in relation to a security threat or to improve existing arrangements.

3.4. Where there is a risk to the network security, quality of service for network users, or in order to enforce University policy, IT Services is authorised to:
- Impose restrictions on network traffic or use of network applications.
• Refuse connection of devices to the network.
• Remove devices or sub-sections of the network from service.
• Manage network resource allocation (such as bandwidth).

3.5. Control of network address allocation rests with IT Services although this may be delegated to departmental support staff for specific address schemes.

3.6. It is IT Services policy to endeavour, within the networking resources available, to equitably satisfy the legitimate and justified demands of all network users and to meet any relevant service level agreements that might be in place.

3.7. Users of University networks are to be explicitly advised that normal operational network management procedures will include: probing devices to test their security and the monitoring of network traffic to detect operational problems or possible policy violations. See also:

• Institutional IT Usage Monitoring and Access (ISP-I6)

4. Network design and configuration

4.1. The network must be designed and configured to deliver levels of performance, security and reliability suitable for the University’s business needs, whilst providing a high degree of control over access.

4.2. Controls should be used where practical to partition the network into domains on the basis of security requirements. Access controls and routing should be used to prevent unauthorised access to network resources and unnecessary traffic flows between domains. In particular, appropriately configured firewalls should be used to help protect the University’s critical computer systems.

4.3. Networking serving discrete buildings or departments is connected to the campus network only on the understanding that:

• Either, designated departmental network support staff are identified who will work in cooperation with IT Services. (Such staff should be available for consultation during normal working hours. In addition they should be available, with reasonable notice, when out-of-hours development and maintenance is taking place.)

• Or, all rights and responsibilities, including privileged access to any network devices, are ceded to IT Services.

4.4. In principle, permission to use particular protocols, and registration of addressing information, are not necessary for departmental networks that are completely isolated from the campus network, and will never share traffic with it. However, it is very strongly recommended that such networks be managed as though they were part of the campus network, since this will minimize future inconvenience if it is found at a later date that an interconnection is desirable. It will also prevent the problems that might arise if an unplanned connection between networks is made inadvertently.

5. Physical security and resilience

5.1. Reasonable measures based on an assessment of risk, such as fire and water protection, padlocks, secure cabinets etc, must be taken to protect networks and communication equipment against accidental damage, potential security breaches, theft or malicious intent.
5.2. The network should where possible incorporate logical and physical resilience features to help mitigate the impact failure of, or physical damage to, cabling and other network equipment.

5.3. See also:

- **Operations Policy for IT Service Providers (ISP-S6)**
- **Building Security (ISP-I1)**

6. Connecting devices to the network

6.1. Ownership of networked devices

- Only devices owned by the University, or its recognised partner organisations such as the Student’s Union and University Hospitals, may be connected to the “wired” network.
- Privately owned devices may only be connected to the “wired” network in special circumstances approved by the Head of Department. (In such cases approval to connect the device must also be obtained from a Network Authority or Authoriser in the usual way - see below.)
- Privately or University owned laptops/PCs may be connected to the wireless network.
- All devices whether privately owned, or owned by other organisations, must meet the hardware and software requirements, as set out below, and their usage must conform to University policies.
- Regardless of ownership of a device, its connection to University networks is conditional on IT Services having the right to inspect its configuration, test its security and monitor its network traffic in accordance with normal operational network management procedures.

6.2. Administration of networked devices

- Every networked device must be associated with an identifiable and contactable person responsible for its administration. Devices for which the administrator cannot be identified or contacted are liable to be removed from the network.
- Networked devices on the “wired” network may be administered by IT Services, departmental staff or an organisation contracted to undertake their administration.
- It is recommended that where possible administration of networked devices on the “wired” network is restricted to, and undertaken by, computer support specialists. However; departments may choose to delegate administrative privileges for specific devices to other suitably qualified staff, where there are specialised requirements.
- Users of privately owned networked devices are, and will be assumed by IT Services to be, responsible for ensuring that their devices are configured, actively maintained and used in accordance with University policies. Adequate support and maintenance arrangements must be in place for University owned wireless devices.

6.3. Authorisation to connect a device
• Approval must be obtained from a Network Authority or Authoriser before connecting a device to the “wired” network. The request for connection may only be made by a member of staff. (The unauthorised connection of laptops, PCs or other devices to the University “wired” computer network is forbidden for security reasons.)

• Network Authorities and Authorisers must only approve connection of devices to the “wired” network when they are certain that candidate devices meet all relevant requirements set out in the “Connecting devices to the network” section of this document.

• CFS service users and approved visitors are authorised to access the wireless network service.

• Visitors to the University may be granted temporary wireless access to the network by a member of staff with a CFS account.

6.4. Authentication of network users

• Users of University IT facilities must not masquerade as another user or tamper with audit or activity logs.

• It is the responsibility of Network Organisations to manage their computers in a way that ensures that local account users can be identified.

• It should be possible to identify the administrator of each device. Each administrator should be able to identify who is authorised to use any accounts they have created. It is not acceptable for accounts on networked University computers to provide anonymous access or the equivalent of anonymous access.

• Where it is necessary for an account to be shared, the system administrator, or the individual designated as responsible for managing that account, must have full knowledge of the users that have been authorised to share the account.

• In response to security audits or investigations, users and administrators must respond to request for information from IT Services in a timely manner.

6.5. Networked device registration

• Except where IT Services has delegated responsibility for allocating particular groups of addresses to departmental support staff, all devices using the “wired” network must be registered with IT Services.

• Registration of static devices is to be undertaken using the NDOR system.

• The IT Service Desk should be contacted directly about registration of “roaming” devices.

6.6. Hardware and software requirements

• Networked devices must meet current hardware and software requirements, where any such requirements are specified and published by IT Services. At the discretion of IT Services any devices not meeting any such requirements may be denied network access.

• Devices must not be permitted to continue exposing a serious network security vulnerability to the campus network or Internet if there is no imminent prospect of
that vulnerability being removed (whether that be by source code level support, an active program of security patching or firewalling).

- All computer systems providing important University services must be fully supported. That support may be provided by an external supplier or local service provider; however, it must include ongoing remediation of any security vulnerability discovered.
- All networked devices should be maintained so as to be up to date with security patches for both the operating system and any software applications installed.
- Where applicable, networked devices should have current and automatically updated anti-virus software installed.
- Where applicable, networked devices should have correctly configured firewall software installed. As a default all ports should be closed unless specifically opened. Services exposed to the network and the scope of exposure for each service should be the minimum possible.
- Given the variation in software licence agreements, only University-owned machines are considered eligible to become CFS clients.
- Mechanisms intended to ensure University compliance with software licensing restrictions must not be disabled, or their operation interfered with.

7. Management of networked devices

7.1. Those responsible for networked devices must work in cooperation with IT Services such that it can discharge its responsibility for managing the overall network.

7.2. Responsibility for devices must be clear and should fall within the line-management of the University, through Heads of Department.

7.3. Primary control over access to the “wired” network is to be implemented by staff in the Network Authority and Authoriser roles who must:

- Decide whether to approve requests for connection of devices to the “wired” network on the basis of the connection requirements set out in this policy document.
- Be a point of contact with IT Services in relation to the security of the networked devices within their area of responsibility i.e. their Network Organisation.
- Take responsibility for handling security problems that arise in relation to networked devices in a timely manner. Technical support is to be provided to departmental staff by IT Services. Nevertheless, for devices not fully managed by IT Services, ultimate responsibility for ensuring configuration and usage complies with policy rests with departments.
- Where necessary, remove a device from the network to help protect operation or security of the wider network. This should be undertaken in collaboration with IT Services and where possible the person with day-to-day responsibility for the device.

8. Acceptable use of the network

8.1. Connectivity of University networks to the Internet is provided by "JANET" (Joint Academic NETwork) and is subject to compliance with JANET policies. See also:

- Compliance Policy (ISP-S3)
8.2. It is a condition of using University networks that the owners, administrators and users of devices comply with all relevant University policies. In particular, responsibilities and required behaviour of users of University IT systems, including University networks, are described in:

- Use of Computers Policy (ISP-S9).

8.3. All use of the network should be undertaken on the basis of responsible use of a finite shared resource. If there is any doubt as to whether some intended usage of the network is permitted, or could significantly impact performance of the network, then advice should be sought from IT Services before proceeding.

8.4. If some intended use of the network is not explicitly disallowed or controlled it is not necessarily condoned or encouraged.

8.5. Unauthorized eavesdropping will be treated as a serious breach of policy. For the same reason, network monitors and similar devices which allow the inspection of network traffic must not be used without the prior approval of IT Services. See also:

- Institutional IT Usage Monitoring and Access (ISP-I6)

9. Network services and protocols

9.1. Unless there is a compelling reason to do otherwise; existing central or recognised departmental web servers should be used for publishing University generated content.

9.2. Deploying web servers or other types of network servers which do not support recognised University research, teaching or administrative activities is prohibited.

9.3. Only IT services, or Network Organisations with delegated responsibility for management of IP address groups may operate Dynamic Host Configuration Protocol (DHCP) or TCP/IP Bootstrap Protocol (BOOTT) servers.

9.4. IP routing protocols are managed by IT services on routers in the core of the network. Routing protocols, for example RIP, IGRP, BGP etc should not be enabled when setting up IP-connected nodes.

9.5. The use of network management tools that use protocols such as SNMP and CMIP, is restricted to IT Services staff, other than by prior agreement.

9.6. University servers running Domain Name Service (DNS) are managed by IT Services other than by prior agreement.

9.7. University servers running Network Time Protocol (NTP) are managed by IT Services other than by prior agreement.

9.8. Where access credentials, or other confidential information, may otherwise be transmitted on the network in clear text (i.e. unencrypted), use of encrypted network protocols is strongly recommended. See also:

- Information Handling Policy (ISP-S7)
- Outsourcing and Third Party Access Policy (ISP-S4).docx
- Mobile Computing Policy (ISP-S14).docx
- Cryptography Policy (ISP-S16).docx

10. Controlling access to and from other networks

10.1. IT Services is responsible for controlling the network gateway between the University of Leicester networks and the Internet. At this gateway IT Services may exert
control over which incoming or outgoing network connections are permitted. This access control may be used for:

- Limiting the scope of exposure of University network services to the Internet in order to reduce the risk of hacking, denial of service attacks, unauthorised disclosure of information etc.
- Preventing propagation of malware or network traffic associated with malware.
- Applying control consistent with implementing current University IT strategy.

10.2. Exposure of network services to incoming connections from the Internet is not permitted without prior agreement from IT Services. Note:

- “Incoming connections” are those initiated from devices on the Internet.
- All established provision of network services to the Internet may subject to review.
- IT Services’ agreement to permit connections into departmental systems will be consistent firstly with current University IT strategy then secondly with departmental IT strategy.
- These network services include, however, are not limited to: websites, login access for offsite users or automated processes, connection into remote desktop access software etc.

10.3. Access to the University network from the Internet via Virtual Private Network (VPN) connections is not permitted without prior agreement from IT Services.

10.4. Dial up access to a device on the University network using a modem is not permitted without prior agreement from IT Services.

11. Incidents and emergency procedures

11.1. Any incident or emergency relating to the University network should be reported to the Service Desk in IT Services.

11.2. IT Services must ensure that prompt and effective action is taken in response to requests and information from JANET CSIRT (Computer Security and Incident Response Team).

### Failure to comply with University Policy may lead to disciplinary action.

The official version of this document will be maintained on-line. Before referring to any printed copies please ensure that they are up-to-date.