Ulster University Standard Cover Sheet

Document Title	NETWORKS STANDARD 4.5
Custodian	Deputy Director of Finance and Information Services (Information Services)
Approving Committee	ISD Committee
Policy approved date	2017 – 08 – 10
Policy effective from date	2017 – 08 – 10
Policy review date	2018 – 08 – 10

Changes to previous version
Page 1 – “and also” changed to “and”.

INTRODUCTION AND BACKGROUND

The University networks are an essential and integral part of University business processes, and in the delivery of teaching and research. This document outlines the standard for network connections and operation.

Further information on ISD policies, standards and guidelines is available at:

http://www.ulster.ac.uk/isd/policies

RELEVANT LEGISLATION

The University will comply with all legislation and statutory requirements relevant to information and information systems, including:

- Computer Misuse Act 1990;
- Data Protection Act 1998;
- Communications Act 2003;
- Copyright, Designs and Patents Act 1988;
- Freedom of Information Act 2000;
- Human Rights Act 2000;
- Regulation of Investigatory Powers Act 2000;
- Police and Justice Act 2006;
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ('the Lawful Business Regulations')

POLICY STATEMENT

Information Services (ISD) Service Provision

- The ISD infrastructure Networking Team and its contractors are solely responsible for the installation, configuration and the management of all the network active equipment at the core and edge of the University's network.
- Network active equipment is defined as equipment required for connecting and operating the University's data network. Examples are switches, routers, firewalls and wireless access points.
- ISD are responsible for managing the risks of any device connected to the network and implementing any necessary security measures to protect the network. These risks will be minimised by regularly updating firmware and configuration files in firewalls and routers.

Network Infrastructure

- Network equipment and cabling must not be located in public areas. All cabling and equipment must be housed in secure wiring closets. Access must be restricted to prevent interference to the infrastructure or unauthorised patching of cabling services.

- All equipment installed in the edge wiring closets must be of a type specified by ISD and will be managed by ISD.
- ISD are responsible for the connections to this equipment and only ISD staff may connect (or disconnect) them.
- All fibre and UTP cabling must be installed in accordance with the latest ISD cabling specification. ISD must receive test results and certifications prior to use. Only ISD staff and University approved data communications contractors are permitted to modify the cabling infrastructure.
- Users must not disconnect or connect any other device to live network points in Information Services Department (ISD) computer lab facilities. University computers or printers in these areas must not be tampered with.

Departmental Networks

- Departments wishing to install their own networks may do so within their own physical area, however approval must be sought from ISD before their network is connected to the University network infrastructure.
- The department must also appoint a network administrator to act as a contact with ISD.
- All fibre and UTP departmental cabling must be installed in accordance with the latest ISD cabling specification.
- Department network equipment and cabling must not be located in public areas. All cabling and equipment must be housed in secure wiring closets. Access must be restricted to prevent interference to the infrastructure or unauthorised patching of cabling services.

Data Centres and Server Rooms

Host devices like servers and those used for monitoring and other similar operational functions must be sited in a data centre or server room. Host devices like servers used for enterprise functions must be sited in a data centre.

At a minimum, each server room will provide:

- Secure locked environment
- Air conditioning/handling
- Uninterruptible Power Supply (UPS)

Central data centres will provide additional facilities like power generation, fire suppression and additional physical security.

Due to their security and requirements, data centres and server rooms are exempted from University Network Access Control (NAC) and the requirement to periodically authenticate to gain a network connection.

Network Management

- The administrator should ensure the following security guidelines on their network equipment before seeking connection to the University network infrastructure.
    - Change all default passwords
    - Change SNMP community strings from default

    - SNMP write should only be possible via Network Management System
    - Disable unused management access e.g. Web
- And where possible: -
    - Management access should be controlled via access lists to permitted authorised IP addresses only
    - Web interfaces if used should be Secure Sockets Layer (SSL/TLS)
    - Secure Shell (SSH) should be used for access instead of Telnet

Server Connections

- Every computer providing any service must have an identified “system administrator” whose responsibilities include the maintenance of the computer system(s) concerned.
- It is recommended that computers providing services to staff and students should also have at least one identified deputy responsible officer with system knowledge and administration access, so that a contact is available at all times during the normal working week.
- It is the system administrator's duty to ensure that servers are operated in a secure manner and that they are appropriately configured. This entails;
    - Ensuring that the operating system is patched to the latest level
    - All default passwords are changed
    - Unnecessary services are turned off (or preferably not installed)
    - That access to the server is logged appropriately and checked for evidence of misuse
    - Server application software is kept up to date by the application of update patches
    - Every user of the system must have a unique username and password
    - If appropriate install and keep up to date a firewall or intrusion detection system to help protect against unauthorised access or malicious attack
    - If appropriate install and keep up to date antivirus software
    - Keep regular backups of data and services
- Servers must not be located in public areas or offices, but rather in secure server rooms or data centres. Access to physical consoles must be restricted to prevent interference with server configuration or software.
- Remote access to servers for the purposes of system administration must use only approved secure protocols.
- Servers providing access to essential or critical services must be located in a central data centre which provides a safeguarded mains power supply as well as a secure physical environment.
- The University operates a Default Deny Inbound network policy. Servers on campus will not be visible to the Internet unless a service is requested by completion of Server Connection Application Form. System Administrator’s should note;

    - Services must be audited before remote access to the server will be granted.

- Remote access to any server will be immediately withdrawn if it proves impossible to contact the system administrator or any nominated deputy when this is required for any reason during normal working hours.
- Remote access to any server may be withdrawn if routine security auditing of the service reveals it to be insufficiently secure due to the installation of software with known vulnerabilities or configured in a way which permits the service to be compromised.

Staff Connections

- Network points in staff offices are for the connection of staff endpoint devices. No other devices may be connected to the network points without prior approval from ISD.
- Staff members requesting connection of endpoint devices should do so via the ISD helpdesk.
- When a staff endpoint device has been networked, it is the department's responsibility to ensure the computer is secure.
- ISD manages the provision of IP addresses. Any approved University owned device may be connected to the campus network and will be automatically assigned an IP address. Exceptions to the dynamic allocation of IP addresses must be authorised by ISD.
- It should be noted that adding services (e.g. remote access to web, ftp ..etc) to any staff connected computer may turn it into a server and the conditions covered in server connections will apply.

For the purposes of this policy, network connections of endpoint devices by postgraduate students with offices and/or fixed research lab facilities are regarded as staff connections.

Student Connections

- Students wishing to use their own laptops on the University network may only do so in the approved designated open access and wireless areas. A list of these designated areas together with usage instructions is published on the University web.
- It is the responsibility of the student to ensure that all end point devices used on the University network have the latest level of anti-virus software and security patches installed. These must be kept up to date.

Network Access Control (NAC) Exemptions

ISD will authorise exemptions from NAC authentication for specific devices, but only if one of the following conditions are true:

Permanent Exemptions

1. The end-point device is a "headless device". A headless device is a device that lacks a graphical user interface or other means of manually or automatically providing user credentials to the network authentication process. For example, this could be an embedded device that does not include a keyboard and a display screen. The most common examples are IP

phones, WiFi Access points, networked printers, scanners, Building Management System (BMS) sensors, etc.

Temporary Exemptions

1. A work practice has been established that does not conform to University policy, but a fixed period of time will be required to correct the practice.
2. The end-point is experiencing configuration problems with NAC authentication. Exemption may be granted until the configuration problem is corrected.
3. The end-point device could use NAC credential authentication, but it's role requires 24/7 connection for operational purposes, and therefore any scheduled daily or weekly NAC timeout disconnection is unviable. Examples of such devices would include workstations that are used for logging or monitoring. Exemption may be granted until the end-point function is migrated into the appropriate zone in a secure data centre where NAC is not applied. Remote connection to the function may then be implemented.
4. The device is a server or related equipment which does not require daily authentication. Exemption may be granted until the end-point function is migrated into the appropriate zone in a secure data centre where NAC is not applied.

PURPOSE AND SCOPE OF THE POLICY

The data network is now an integral part of University life and indeed a key component of University business. Any changes to it may have serious effects elsewhere on the network. This standard is therefore applied to protect the network from malicious or accidental damage and prevent any unauthorised reconfiguring or change to any part of the network.

The data network is connected to JANET and is therefore bound by the JANET connection and acceptable use policies.

IMPLEMENTATION AND ENFORCEMENT

- Users should be aware that activity on the University network will be monitored and recorded to secure effective operation, and for other lawful purposes.
- ISD reserve the right to refuse to connect to the University network infrastructure, or to disconnect, any departmental network or equipment, which may have an adverse effect on the University network infrastructure.
- ISD reserve the right to disconnect any departmental network or equipment, which does not adhere to the University's Acceptable Use Code of Practice or connection practices.
- ISD reserve the right to remove network privileges from any staff if there is a security risk from their computer or if the user does not adhere to University's Acceptable Use Code of Practice. Staff who are in breach of the University's Acceptable Use Code of Practice may be subject to disciplinary action.

- Students who do not adhere to University's Acceptable Use Code of Practice or tamper with any part of the network in any way, will have their network privileges removed and will be subject to disciplinary action.