



## UU Security Policy

### *Network Connection Policy*

<b>Author:</b>	Harry Young
<b>Approved by:</b>	IICTSC
<b>Version:</b>	2.0
<b>Date:</b>	1 June 2006
<b>Status:</b>	Agreed
<b>Classification:</b>	Public
<b>Enquiry point</b>	Harry Young Network Manager University of Ulster Phone: 028 90366488 Email: <a href="mailto:h.young@ulster.ac.uk">h.young@ulster.ac.uk</a>
<b>Policy effective from:</b>	1 June 2002
<b>Policy review date:</b>	1 May 2007

## Change History

Version	Changes	Date
1.0	Initial document	1/6/02
2.0	Included BS7799 reference Change department name to CIS Updated service provision to include firewalls Updated network infrastructure to include cabling Added Student Connections section	1/6/06

## Contents

UU Security Policy .....	1
Network Connection Policy .....	1
Change History .....	2
Contents .....	2
Network Connection Policy .....	3
Reason for Policy .....	3
Corporate Information Systems (CIS) Service Provision .....	3
Network Infrastructure .....	3
Departmental Networks .....	4
Network Management .....	4
Staff Connections .....	4
Student Connections .....	5
Enforcement .....	5
Further Information .....	5
BS7799 Reference .....	6

## ***Network Connection Policy***

### **Reason for Policy**

The data network is now an integral part of the University life and indeed a key component of University business. Any changes to it may have serious effects elsewhere on the network. This policy 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.

### **Corporate Information Systems (CIS) Service Provision**

- The CIS infrastructure Networking Team is solely responsible for the installation, configuration and the management of all the network active equipment in the core and edge wiring closets.
- Network active equipment are defined as equipment required to connect and operate the University's data network. Examples are switches, routers, firewalls and wireless access points.
- CIS 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 counter measured 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 CIS and will be managed by CIS.
- CIS are responsible for the connections to this equipment and only CIS staff may connect (or disconnect) them.
- All fibre and UTP cabling must be installed in accordance with the latest CIS cabling specification, CIS must receive test results and certifications prior to use. Only CIS staff and University approved data communications contractors are permitted to modify the cabling infrastructure.
- Network points in Information Services Department (ISD) computer labs are for University computers or printers only. Users must not disconnect, tamper with or connect any other devices.

## Departmental Networks

- Departments wishing to install their own networks may do so within their own area, however approval must be sought from CIS before their network is connected to the University network infrastructure.
- The department must also appoint a network administrator to act as a contact to CIS.
- All fibre and UTP departmental cabling must be installed in accordance with the latest CIS 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.

## 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)
  - Secure Shell (SSH) should be used for telnet access

Passwords for these devices must be secure (see Password Policy) and in the event of a violation or suspected violation must be changed immediately. It is suggested that the passwords should be stored in a sealed envelope and stored in a secure place, to be opened only in an emergency by selected personnel if the network administrator is not present, or if there is a change of administrator. Once the envelope has been opened all passwords should be again changed and stored in a sealed envelope.

## Staff Connections

- Network points in staff offices are for the connection of staff computers and printers. No other devices may be connected to the network points without prior approval from CIS.
- Staff members requesting connection of computers or printers should do so via the ISD helpdesk.

- When a staff computer has been networked, it is the user's responsibility to ensure the computer is secure (see Personal Computer Security Advice Note).
- CIS 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 CIS.
- 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 the Server Connection Policy will apply.

### **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 machines used on the University network have the latest level of anti-virus software and security patches installed. These must be kept up to date.

### **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.
- CIS 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.
- CIS reserve the right to disconnect any departmental network or equipment, which does not adhere to the University's Acceptable Use Policy or connection policies.
- CIS 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 Policy. Staff that are in breach of the University's Acceptable Use Policy may be subject to disciplinary action.
- Students who do not adhere to University's Acceptable Use Policy or tamper with any part of the network in any way, will have their network privileges removed and will be subject to disciplinary action.

### **Further Information**

Policy on Acceptable Use of University Computing and Data  
 Personal Computer Security Advice Note  
 Password Policy

<p><b>Ref:</b> UU Security Policy / Network Connection Policy</p>
---

<p><b>Version:</b> 2.0 <b>Status:</b> Agreed</p>
--

<p><b>Classification:</b> Public</p>
--------------------------------------

Page 5 of 6

Server Connection Policy  
Wireless Communications Policy  
Monitoring Policy  
Janet Acceptable Use Policy  
Janet Security Policy  
5.590.2 DGN Structured Cabling Specification

### **BS7799 Reference**

<b>A 3.1.2</b>	<b>Review and evaluation</b>
<b>A 4.1.3</b>	<b>Allocation of information security responsibilities</b>
<b>A 7.2.1</b>	<b>Equipment siting and protection</b>
<b>A 7.2.3</b>	<b>Cabling security</b>
<b>A 7.2.4</b>	<b>Equipment maintenance</b>
<b>A 8.3.1</b>	<b>Controls against malicious software</b>
<b>A 8.5.1</b>	<b>Network controls</b>
<b>A 9.4</b>	<b>Network access control</b>
<b>A 9.5.4</b>	<b>Password management system</b>
<b>A 9.7.1</b>	<b>Event logging</b>
<b>A 9.7.2</b>	<b>Monitoring system use</b>
<b>A 12.2.1</b>	<b>Compliance with security policy</b>