

## Schedule 8: University Permission to Connect to the IT Network Policy

University IT Regulations Section 4 'Integrity of IT facilities' states:

*All connections of equipment to the IT facilities must be conducted in accordance with the University's Permission to Connect policy.*

In order to maintain the integrity and protection of University IT facilities and the information held, the University requires that all equipment which are to be connected to the University IT facilities comply with a set of minimum standards.

### 1. Scope

This policy applies to equipment connected to the University IT facilities.

### 2. Aims and Objectives

The Aim of the Policy is to protect the University Networks in order to maintain integrity and resilience of the IT facilities. Poorly configured, managed or operated equipment may lead to a serious degradation of operation and or a breach in network and systems integrity resulting in

- Disruption to normal business processes.
- Disclosure of sensitive personal, financial or research information.
- System compromise
- Compromise of other network systems

#### 2.1 The Objectives of the Policy are:

- .1 Define minimum requirements for equipment being connected to the University IT networks;
- .2 Define standards of acceptable usage of the University IT facilities including network protocols that may be used on the University IT networks;

### 3 Implementation

#### 3.1 Requirements for connecting equipment to the network

- .1 All hardware and software ('Equipment') which will access the services and facilities afforded by the network must be approved by the Director prior to connection.
- .2 Connection of equipment to certain parts of the network is only available to specified classes of users and equipment given in Appendix 5.
- .3 All devices connected to the network shall first be registered with the University. INSRV will publish the procedure(s) via the Information Services website (Use URL found in **Schedule 3: Guidance Notes for the use of IT Facilities** section S3.2.2)
- .4 Where the registration procedure requires submission of a Permission to Connect (P2C) form Information Services must be informed of any change in use, location or ownership of the equipment; for example a change of operating system, or the addition/removal of a service, requires the submission of an updated P2C form.
- .5 Only Equipment covered by Appendix 1 may be connected to the network.

- .6 Equipment covered by Appendix 2 will NOT be allowed to connect to the network.
- .7 Where a requirement for connection falls outside the permitted list, approval must be sought from the Director before connection to the network.

### 3.2 Conditions of use of the network connect equipment

- .1 Users must accept network names and addresses assigned by INSRV. DHCP (Dynamic Host Configuration Protocol), if possible, must be used to obtain names and addresses.
- .2 Users agree to and will be responsible for ensuring that vendor security and critical system software updates (patches) are applied in a timely fashion and up to date anti-virus software is installed and operational. Failure to carry out these tasks may result in disconnection of the equipment.
- .3 If Schools or Divisions do not integrate their account management with the University Directory system (e.g. via LDAP or Shibboleth), they must maintain records of the accounts they have allocated. The minimum information to be kept is listed in Appendix 3.
- .4 Schools/Divisions must ensure that account holders are aware that whilst logged into a system connected to the network their use is subject to all relevant University Regulations and procedures.
- .5 The University may employ measures (including, but not limited to, remote audit and penetration testing) to ensure compliance with University policies and regulations. By connecting to the network users are deemed to have granted permission for this limited intrusion onto their system.
- .6 The University may suspend access to the Internet, or the network as a whole, whilst complaints are investigated, or to ensure the integrity of the University network.
- .7 Equipment connected to the network may only use the approved protocols and offer those services covered by Appendix 4.

### 3.3 System Purchasers

- .1 This policy must be taken into consideration when specifying and selecting or designing new computer systems and software.
- .2 For new computer systems where the policy specifies a minimum and a recommended the recommended is to be used in specification and selection.

## 4. Contact

For information about this policy or password management in general please contact the Information Services IT Service Desk - [insrvConnect@cardiff.ac.uk](mailto:insrvConnect@cardiff.ac.uk)

### Release History

IT Equipment Network Connection Policy Version 2, draft created by D H J Gulliver 6 March 2007

Re-draft of Permission to Connect statements and minor revision of wording by D H J Gulliver 16 March 2007

## Appendices to the University Permission to Connect to the IT Network Policy

### Appendix 1

Equipment with a University-approved network card that may be connected to the Network:

- Any Windows XP, Vista and 7
- Any Apple Mac
- Any UNIX/Linux workstation
- HP Jet Direct Print Servers (internal and external)
- Novell iPrint compatible printers
- Konica and Canon Multi Function Devices, provided they can be configured by DHCP.

Modem equipment can also be connected, subject to the approval of the Director before connection.

Wireless Access Point (bridge/router) refer to the University Wireless policy, [http://www.cardiff.ac.uk/insrv/resources/regulationsandstrategy/cu\\_wireless\\_policy\\_v2.pdf](http://www.cardiff.ac.uk/insrv/resources/regulationsandstrategy/cu_wireless_policy_v2.pdf)

### Appendix 2

Equipment that users shall **NOT** connect to the network without the permission of the Director

- Bridges and switches
- Routers (including computing systems acting as routers or gateways)
- Repeaters (including hubs)
- Any other device which extends or modifies the network
- Any other device which connects any other network to the University network

### Appendix 3

Other persons may be granted permission to hold an account subject to approval by the Director or relevant Head of School/Division. Each individual School/Division must keep a record of accounts granted to non-University persons. Records must be retained as defined in University Records Retention Schedule, Information and Communications Technology (ICT) Systems Management. As a minimum the following shall be recorded:

- the name and organisation of the person for whom the account(s) is being created;
- the name of the person creating the account;
- the reason the account(s) are required;
- any login name(s) assigned and system(s) on which these login names have been created;
- the date the account(s) were activated;
- and upon expiry, the date when these account(s) were disabled.

### Appendix 4 - Permitted Network Protocols and Services

The following protocols are permitted:

Novell networking

- Must use IPX on Ethernet II frames only
- Must only use NCP over IPX or TCPIP. Use of IPX is deprecated and not supported across the campus backbone

Microsoft networking

- Must only use NBT (no NETBEUI)
- Must seek permission to run WINS server
- Must seek approval for domain names
- Must seek approval for Active Directory Services

TCP/IP

- Users should seek approval for: DNS Server, BOOTP/DHCP server, SLP server, IP V6, IP route serving

Users are required to seek approval for other protocols.

The following services are permitted provided that they are registered with INSRV via a Permission to Connect form. By registering your equipment as a workstation or server and defining any services offered, we can establish normal behaviour for your equipment, and be better able to identify systems which have become compromised. Note that all NCP and NDS servers must be INSRV controlled to protect the integrity of the overall Novell service.

- FTP
- EMAIL
- WEB
- Terminal services
- SMB servers, (Samba and Microsoft File-sharing)
- Database servers
- Peer-to-Peer file sharing protocol

Users must seek approval for all other services.

#### **Appendix 5**

The Cardiff Academic Network (CAN) and those who may apply to connect to it.

- Administration Network: INSRV and Administration staff
- Server Farm Network: INSRV
- RESLAN Network: INSRV, individuals in University Residences
- Research Network (GRID): INSRV and Research staff, including postgraduates with supervisor approval.
- Cathays Wired Network: All Staff, and postgraduates with supervisor approval.
- Heath Wired Network: All Staff, and postgraduates with supervisor approval.
- Staff Wireless Network: Staff
- Student Wireless Network: INSRV and Students.
- Guest Wireless Network: Sponsored by all staff.