University of Salford MANCHESTER

Network Security & Connection Policy

Effective from 17 February 2015

Version Number: 2.0

Author: Network Manager, IT Services

Document Control Information

Status and reason for development

Revised to reflect organisational and technical changes (to be V2.0 when completed)

Revision History

Date	*Author*	*Summary of changes*	*Version*	*Authorised*
Nov 2014	J. Kelly	General update and transfer into policy template	V2.0 Draft	IT Services Associate Director
Jan 2006	D Goodman	Update to section 5.6	V1.1	ISD
Aug 2005	D Goodman	New policy	V1.0	Information Services Division

Policy Management and Responsibilities

Owner:	This Policy is issued by the Director of IT Services, who has the authority to issue and communicate policy on IT Network services and has delegated day to day management and communication of the policy to the Network Manager.
Others with responsibilities (please specify):	All subjects of the Policy will be responsible for engaging with and adhering to this policy.

Assessment	*Cross relevant assessments*	*Cross if not applicable*
Equality Analysis	X	
Legal	☐	X
Information Governance	X	☐
Academic Governance	☐	X

Consultation	*Cross relevant consultations*
Staff Trades Unions via HR	☐
Students via USSU	☐
Any relevant external bodies (please specify) ……..	☐

Authorised by: Associate Director IT Operations, IT Services

Date authorised: 28/01/2015

Effective from: 17/02/2015

Review due: 2 years by February 2017

Document location: University Policy & Procedure Pages
http://www.salford.ac.uk/about-us/corporate-information/governance/policies-and-procedures

Document dissemination and communications plan:
US Online, Student Channel.

1.0 Purpose

IT Services Division (ITS) is responsible for the ownership, development, installation, operation and maintenance of the data communications network on behalf of the University and its members. With this responsibility comes the authority to take action necessary to safeguard the security of the network and minimise and contain potential risks to the University and its members, both operational and legal, from the consequences of network-related security violations and misuse. In this context, the purpose of this policy is to state clearly;

- ITS responsibility and authority for the University's data communications network infrastructure
- ITS responsibility for devices connected to that infrastructure
- End-users' responsibilities in using such devices.

2.0 Scope

2.1 To whom it applies

This policy applies to all Students, Staff and Associates.

2.2 What is covered

The coverage of this policy includes:

1. The University of Salford (UoS) data communications network infrastructure, all devices connected to it and all external network connections to services such as JANET and the Internet (including but not limited to):
    a. University network segments linked directly and indirectly to the UoS data communications network infrastructure
    b. University network segments linked via JANET
    c. University network segments linked via wireless technology.
2. Any and all devices utilising this infrastructure, including those connecting via wireless & mobile technology
3. Protection and detection of threats against University of Salford IT systems (as referenced in the ICT AUP(1): see Related Documentation)
4. Threats from, but excluding risks to:
    i. Devices attempting to connect to the UoS data communications network infrastructure that are not approved for network connection by ITS
    ii. on-campus devices connected both to the UoS data communications network infrastructure and to external network connections
    iii. on-campus networks not installed or approved by ITS
    iv. off-campus networks and devices.

2.3 Out of Scope

This policy does not include guidance on the following aspects as they are covered in specific support and maintenance contracts or ITS procedures:

- External suppliers access to the University network
- Data point activation

2.4 Definitions

Network Devices: active equipment required to interconnect and operate any aspect of a data network; examples include switches, routers, firewalls and wireless access points

Client Devices: equipment generally used by one person at a time. Examples are PCs, laptops, Apple Macs, tablets or smartphones.

Non-Client Devices: equipment which provides a service to one or more users. Examples include (but are not exclusive to) servers, network attached storage, printers.

3.0 Policy Statements

3.1 Users of the Network

Only registered users (i.e. those holding valid UoS usernames and passwords) or those given permission by the CIO (or nominated deputy) are permitted to connect to the University of Salford data communications network.

3.2 Modifiers of the Network

Only relevant ITS staff and University approved data communications contractors are permitted to change, modify or otherwise configure any part of the data communications network.

3.3 Network Devices

Only relevant ITS staff and University approved data communications contractors are permitted to install, configure & connect network devices to the UoS data communications network. All such devices will be solely managed & maintained by ITS.

3.4 Client Devices

3.4.1 University owned or managed client devices

If the client device is owned (or leased) and managed by the University/ITS, network connectivity is achieved by either plugging this equipment directly into an activated data point on the UoS network or via the centrally provided wireless network.

3.4.2 Personally owned client devices

Users wishing to connect their personally owned client devices to the UoS data communications network may do so only by using one of the following methods:

- Connect via the centrally provided wireless network
- Connect via the Halls of Residence clean access service
- Connect (from outside the University) via the Internet to those services explicitly provided by ITS for off-campus use.

Any other method of connection is prohibited unless prior written authorisation has been obtained by ITS. It is the responsibility of the user of any personally owned equipment connected to the network to ensure that the equipment has the latest level of anti-virus software and security patches installed, and that these are kept up to date at all times.

3.5 Non-client Devices

Non-client devices may only be connected to the UoS data communications network if prior written authorisation has been obtained from ITS. Users wishing to connect this type of device must complete a Server Registration Form (See Related Documentation) and submit this to ITS Service Desk. ITS reserve the right to deny this type of request.

3.6 Use of the Network

The University data communications network may only be used for purposes defined in the ICT Acceptable Use Policy (AUP) and for no other purpose.

3.7 ITS Responsibilities

ITS is responsible for:

- managing access to the JANET Network by the University's users
- managing the risks from any device connected to the network and implementing any necessary security measures to protect the network (and other linked networks)
- managing the provision of IP addresses; protection via the network security infrastructure; user registration; authorisation and authentication; and data point activation.
- Installing, connecting and managing networking equipment within the University data communications network e.g. switches, routers and wireless equipment.
- Monitoring and managing the University data communications network for performance issues, abnormal loading, port and IP scanning, and other security threats

4.0 Policy enforcement and sanctions

Any suspected breaches of this policy will be investigated under the terms of the ICT AUP[1].

5.0 Related Documentation

University policies are located here:

http://www.salford.ac.uk/about-us/corporate-information/governance/policies-and-procedures

- ICT Acceptable Use Policy (AUP)
- Information Security Policy
- Mobile Devices Security Policy

Joint Academic Network policies are located here: https://community.ja.net/library/janet-policies

- Janet Connection Policy
- Janet Security Policy
- Janet Acceptable Use Policy

IT Services Server Registration Form: http://www.its.salford.ac.uk/servicedesk/

6.0 Appendices

No Appendices