Network Management Policy

1. Introduction

This policy will define how the university networks are designed and systems are connected to them. It includes appropriate technical and procedural controls to reduce risk and meet the requirements of the Information Handling Policy.

2. Scope

2.1 To define De Montfort University's policy for designing, controlling and managing the university network.
2.2 Enabling the movement of data that supports the university's business and disabling the movement of data that hinders the university's business needs over the networks for which the university is responsible.
2.3 This document includes statements on:
- 2.3.1 Management of the Network
- 2.3.2 Network Architecture
- 2.3.3 Physical Security and Integrity
- 2.3.4 Controlling Access

3. Definitions

3.1 End User Network Device – any network enabled device which is the initial source or ultimate destination in a data network.
3.2 Network Device – a device such as a switch or router through which data passes on its journey to or from an End User Network Device.
3.3 Network Interface – part of a network device or end user network device that enables it to communicate via a network, there may be more than one interface on a device.
3.4 Local Area Network (LAN) – a computer network than spans a relatively small area, such as a building.
3.5 Network Manager – The person appointed by the Chief Information Officer as the person responsible for the management of the University network.
3.6 System Owner – The manager of individual systems or services such as email or websites can include PC labs or LAN partitions.

4. Management of the Network

4.1 De Montfort University's network shall be managed by suitably authorised and qualified staff appointed by the network manager to oversee its day to day running and to preserve its security and integrity in collaboration with nominated individual system owners.
4.2 Planned reconfiguration of the network will use formal, auditable change control procedures and appropriate risk management.
4.3 Where there is a risk to the security or quality of service to the network, the Network Manager is authorised to make emergency changes to restore service.
4.4 The overall control of the IP address scheme is managed by the Network Manager, although this may be delegated to nominated system owners for limited IP address management.

4.5 Users of the network are advised that network management procedures may include procedures such as:
  4.5.1 Probing devices to test security.
  4.5.2 Monitoring of network traffic to detect operational issues.
  4.5.3 Recording of network traffic to detect possible policy violations.
  4.5.4 Validation that data travelling across the network is legitimate and does not have virus content, is not of an offensive nature, and cannot be detrimental to performance or management of any device or end user device on the network.

5. Network Architecture

5.1 The network must be designed and configured to deliver performance, reliability and security suitable for the requirements of the university.
5.2 The network shall be segregated into separate logical domains on the basis of security requirements. These domains will have controls to prevent unauthorised access to the university's critical business systems.
5.3 LANs in individual buildings or departments should normally be designed and installed by the network management team. In other cases the Network Manager reserves the right to check the installation before connecting it to the DMU network.
5.4 No changes to the network infrastructure, such as the introduction of a router, switch or wireless access point, is permitted without prior approval from the Network Manager.
5.5 Records of all active and inactive network device locations and configurations shall be maintained.

6. Physical Security and Integrity

6.1 Reasonable measures based on a risk assessment, and regulatory compliance must be taken to protect rooms containing servers, active network devices and patching panels from threats such as fire, water, accidental damage, security breaches and theft.
6.2 Physical access to rooms containing servers, active network devices and patching panels shall be restricted to:
  6.2.1 A list of authorised staff maintained by the relevant system or network manager.
  6.2.2 Other individuals providing that their entry has been approved by the relevant system or network manager.
6.3 Any device that is running a service that conflicts with centrally managed services such as OSPF, DHCP, RIP, BOOTP etc. must not be connected to the network without prior agreement with the Network Manager.

7. Controlling Access

7.1 Access control procedures must provide adequate safeguards through robust identification and authentication techniques.
7.2 Only devices owned by the university or recognised partner organisations may be connected to the wired network, except under special circumstances, approved by the Network Manager.
7.3 Personal devices may be used on the wireless network only after registration and authentication.
7.4 All devices connecting to the university network both wired and wireless must conform to university policies.
7.5 Remote administrative connection to the university network and resources will only be permitted from authorised users and devices over suitably secured connections.

8. Document Approval

Approved by: Kathryn Arnold CIO
Approved Date: 5th October 2012
Review Date: 5th October 2013
Reviewer: IT Governance Manager

9. Document History

9.1 1st October 2010 – Draft 1 Neil Faver
9.2 5th October 2010 – Draft 2 Neil Faver
9.3 9th October 2010 – Draft 3 Neil Faver
9.4 3rd November 2010 – Draft 4 – Document re-formatted Neil Faver
9.5 21st February 2011 – Draft 5 – Neil Faver
9.6 3rd March 2011 – Draft 6 Neil Faver
9.7 24th May 2011 – Draft 7 Neil Faver
9.8 13th June - Draft 8 Neil Faver
9.9 2nd August 2011 – Draft 9 Logo updated, Section 3.1 and 5 amended. – Neil Faver
9.10 22nd March 2012 – Draft 10 Neil Faver
9.11 5th October 2012 – Version 1 Neil Faver