Network Management Policy

1. Introduction

This policy will define the design, management, operation and use of the university data networks. It is a sub-document of the Principal Information Security Policy.

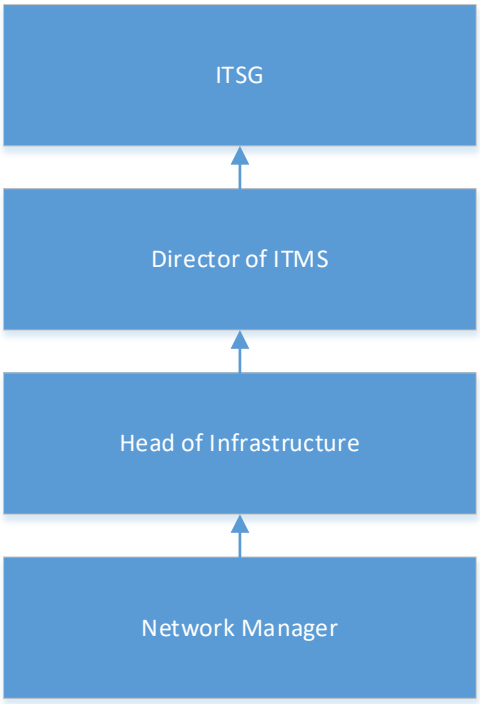
2. Scope

2.1 All of the university's data communications networks, whether wired or wireless are in scope, irrespective of the nature of the traffic carried over those networks.
2.2 This document includes statements on:
- 2.2.1 Definitions
- 2.2.2 Management of the Network
- 2.2.3 Monitoring of the Network
- 2.2.4 Network Design and Architecture
- 2.2.5 Physical Security and Integrity
- 2.2.6 Controlling Access
- 2.2.7 Configuration Management
- 2.2.8 Capacity Management

3. Definitions

3.1 End User Device – any network enabled device which is the initial source or ultimate destination in a data network.
3.2 Personal Device – any network enabled device not owned or managed by the university.
3.3 Network Device – a device such as a switch or router through which data passes on its journey to or from an End User Device.
3.4 Network Interface – part of a network device or end user device that enables it to communicate via a network, there may be more than one interface on a device.
3.5 Data Network – A communication network that is devoted to carrying information. It consists of a number of nodes connected by various communication network devices.
3.6 System Owner – The accountable person of individual systems or services such as email or websites can include PC labs or LAN partitions.
3.7 Pre-approved standard changes – These are Business as Usual changes to the network that have already been passed Changes by the ITMS Change Advisory Board.
3.8 ITMS – Information Technology and Media Services
3.9 ITSG – Information Technology Strategy Group
3.10 Data Integrity - Data integrity is the assurance that digital information is uncorrupted and can only be accessed or modified by those authorized to do so.
3.11 CAB – IT Change Advisory Board
3.12 Resilience - Resilience is the ability of a server, network, storage system, or an entire data centre, to recover quickly and continue operating even when there has been an equipment failure, power outage or other disruption.
3.13 Confidentiality – Information defined in the Information Handling Policy as personal, sensitive personal and confidential must only be accessible to authorised users.
3.14 Availability – Ensuring timely and reliable access to and use of information.

4. Management of the Network



The high level strategy for the provision of the Data Network at the university is determined by ITSG.

The Director of ITMS is responsible for the implementation of the strategy and management of the networks.

The Head of Infrastructure is responsible for translating the strategy into implementation plans

The Network Manager is responsible for the management of the network

4.1 The university's networks 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, integrity and resilience.

4.2 Planned reconfiguration of the networks will comply with the university's 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 required to convene an Emergency CAB to implement emergency changes.

4.4 The overall control of the IP address scheme is managed by the Network Manager, although this may be delegated to nominated trained staff..

5. Monitoring of the Network

5.1 De Montfort University respects the privacy and academic freedom of staff. The university logs the use and operation of ICT systems to assure system performance and integrity. These logs are monitored but not routinely inspected. Within the terms of the Janet Acceptable Use Policy, the Use of Computers Policy and the Email, Internet and Social Media Policy the university has the right to access communications and data within its ICT systems for the purposes of:

5.1.1 Detecting, investigating or preventing misuse of the facilities or breaches of the university's regulations.

5.1.2 Monitoring the effective function of the network to enable:

5.1.2.1 Capacity Management

5.1.2.2 Alerts in the event of network issues

5.1.2.3 Prevention, detection and remediation of Cyber Attacks

5.1.2.4 Detection and removal of unauthorised network devices that connect to the network.

5.1.3 Investigation of alleged misconduct in breach of the university's IT or other policies.

5.1.4 To comply with lawful requests for information from law enforcement and government agencies for the purposes of detecting, investigating or preventing crime, and ensuring national security.

5.2 Any monitoring or investigation that may, whether deliberately or accidentally, reveal the content of packets or messages will also be subject to the relevant legislation listed section 2 of the Principal Information Security Policy

6. Network Design and Architecture

6.1 The network must be designed and configured to deliver high performance, reliability, resilience and security suitable for the requirements of the university. The following will therefore apply:

6.1.1 The network shall be segregated into logical domains on the basis of access requirements. These will include but not be limited to separate domains for the following:

6.1.1.1 Staff
6.1.1.2 Students
6.1.1.3 Wireless
6.1.1.4 De-Militarised Zone
6.1.1.5 Data Storage
6.1.1.6 Visitors

6.1.2 Access for users to specific domains will be restricted by authentication to the network.

6.1.3 Access to services within each domain will be managed by firewall technology.

6.1.4 No unauthorised equipment shall connect to the network that prevents it functioning correctly.

6.1.5 Approval must be gained from the Network Manager before any configuration changes are made on the networks who will conduct a risk assessment to consider the potential risk to the university network prior to approval.

6.1.6 Cabling of the networks can only be carried out by authorised, accredited personnel. This can be broken down to:

6.1.6.1 Patching – ITMS personnel and ITMS approved 3rd party contractors
6.1.6.2 Structured cabling – ITMS personnel and ITMS approved 3rd party contractors

7. Physical Security and Integrity

7.1 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.

7.2 Essential network services and devices shall be protected from power failures and other disruptions caused by failures in supporting utilities. These utilities need to be monitored and alerts automatically sent in the event of failure.

7.3 Equipment shall be correctly maintained to ensure its continued availability and integrity.

7.4 Physical access to rooms containing servers, active network devices and patching panels shall be restricted to:

7.4.1 A list of authorised staff maintained by the ITMS Technical Architect or the ITMS Network Manager.

7.4.2 Other individuals providing that their entry has been approved by the following:

7.4.2.1 ITMS Director
7.4.2.2 ITMS Head of Infrastructure
7.4.2.3 Network Manager
7.4.2.4 Technical Architect

8. Controlling Access

ITMS is responsible for the management of the university data network devices that link multiple buildings and data centres together and ultimately to the internet. It is imperative that access to these devices must be controlled to prevent unauthorised access in order to reduce the risks to the university from cyber-attacks.

8.1 Access to the university network devices must be strictly controlled and will only be permitted from authorised users and devices over suitably secured connections.

9. Configuration Management

9.1 A record of the configuration of all network devices will be kept.

9.2 Any changes to the network device configuration will be recorded with a record of prior and post configurations kept.

9.3 A risk assessment of any changes to the networks that are not 'Business as Usual' must be performed and documented prior to any changes being carried out and the results presented to the ITMS Change Advisory Board for their response to the risk.

9.4 Prior to implementation of changes to any network device that are not 'Business as Usual' the configuration changes must be tested before introduction into the live environment.

9.5 Restoration testing must be carried out on a regular basis that will be set by the Network Manager.

9.6 All network devices must have a secure version of software loaded.

10. Capacity Management

The data network must deliver high performance, reliability, resilience and security suitable for the requirements of the university. To maintain this network devices must perform at optimal levels.

10.1 The Network Manager and Head of Infrastructure will agree on optimal levels of performance of the following:

10.1.1 Network traffic capacity

10.1.2 Network devices

10.1.3 Physical connections

10.2 The Network Manager or their nominated deputies will monitor and record levels of network traffic capacity throughout the networks and report any existing or potential degradation to the ITMS Head of Infrastructure.

10.3 The Network Manager or their nominated deputies will monitor and record the performance capacity of all network devices and report any existing or potential degradation to the ITMS Head of Infrastructure.

10.4 The Network Manager or their nominated deputies will monitor and record the physical connection capacity of the networks devices and report any existing or potential degradation to the ITMS Head of Infrastructure.

10.5 The Network Manager shall produce a review on a six monthly basis highlighting any areas of future concern to the Head of Infrastructure.

11. Document Approval

Approved by: Head of the Information Governance Board
Approved Date: December 2019
Review Date: December 2020
Reviewer: Interim IT Governance and Security Manager

12. Document History

12.1 5th October 2012 – Version 1 Neil Faver
12.2 18th August 2014 – Version 1.3 Neil Faver
12.3 21st September 2014 – Version 1.4 Neil Faver
12.4 12th January 2016 – Version 1.6 Neil Faver
12.5 2nd October 2018 – Version 1.7 Neil Faver