Network Security Policy

De Montfort University

January 2006

Contents

6 SECURITY ADMINISTRATION

1 Introduction

1.1 Background

1.1.1 De Montfort University is one of the largest universities in the UK. Its activities are supported by an extensive network infrastructure.

1.1.2 The University has a number of faculties as well as corporate services which need to be accessed from all sites. A single university-wide network has been developed.

1.1.3 The De Montfort University Network will continue to be developed to support the University's evolving requirements.

1.1.4 The security policies relating to the De Montfort University Network are defined in two documents:

a) Community Security Policy (Reference 1)

b) Network Security Policy (this document).

1.1.5 Significant changes in the network may necessitate review and re-approval of these policy documents.

1.1.6 In addition to the security policies, usage of the University's networks and systems is governed by the JANET Acceptable Use Policy and De Montfort University IT use regulations.

1.2 Purpose and Scope

1.2.1 The purpose of this document is to define De Montfort University's policy for controlling access to electronic information using network features. Systems, and PCs are outside the scope of this document.

1.2.2 This policy does not cover threats against risks to the buildings such as fire and breaches of the external perimeter of the University buildings.

1.3 Validity

1.3.1 This Network Security Policy is approved and issued by Director of Information Systems and Services. Approval is indicated by signature on the master hard copy and by its availability in the advertised location on the network.

1.3.2 This is the first issue and does not supersede any other document.

1.3.3 The policy contained in this document remains extant until a subsequent version is approved.

1.4 Assumptions

1.4.1 It is assumed that UK Government Protectively Marked Information will not be carried over the University Network, nor will it be stored or processed by systems or client devices attached to it. Should this occur or become a requirement, the security measures and connectivity will require review and approval by the relevant authorities.

1.5 Definitions

1.5.1 The definitions on which this security policy is based are contained in Reference 5.

1.6 References

1) Community Security Policy
2) Information Management Requirements
3) JANET Acceptable Use Policy, current issue
4) Regulations for the use of De Montfort University IT facilities
5) IT Security Definitions.

2 Information and Access

2.1 Overview

2.1.1 The University's requirements for the management of information defines three levels of sensitivity, termed Low, Medium and High, with corresponding protection measures within the Network, Systems, and Applications.

2.1.2 The network infrastructure is able to mediate access only on the basis of attributes known to it. The potential attributes are:

a) physical location as identified by a knowledge of cable endpoints and patching, and the use of shared or dedicated media

b) MAC address identified by analysis of the frame content of the network data link layer communications protocol

c) IP address or IP sub-net identified by datagram content although this could be impeded by use of DHCP

d) VLAN membership

e) authentication within application proxies in a firewall

f) protocol type analyses within a firewall

g) dial back to known numbers for remote access.

2.1.3 Where information needs to be protected beyond the capability of network measures, the necessary levels of protection need to be built into the systems and/or applications.

2.2 Protection Afforded by the Network

2.2.1 It is desirable that, where practicable and cost effective, protection measures are built into the network infrastructure in order to keep potential crackers away from the systems themselves. It is also desirable that multiple layers are used where practicable and cost effective in order to reduce further the risk of compromise of information.

2.2.2 The management of the network and systems to provide security will inevitably introduce overheads in terms of performance, administration costs and user restrictions or extra authentication. These overheads should be viewed in the light of the potential costs of the consequences of information loss. Similarly, for users, there will be overheads and/or constraints on their mode of operation.

2.3 Network Users

The Information model divided users into three levels of known trustworthiness for the purposes of the network architecture:

a) staff

b) students

c) external user.

2.4 Secure Enclaves

Additionally, information identified as having a very high degree of sensitivity and a narrowly restricted set of users should be protected as an attached secure enclave.

3 Security Threats

The Information Management Requirements (Reference 2) identified the types of information to be carried over the network, and by implication, what benefit might be gained from access to the information, and thus likely attack by crackers. The perceived types of attack relevant to the network are:

a) access to information

   i) cracking authentication and/or access controls to obtain information
   ii) cracking authentication and/or access controls to corrupt or delete information
   iii) recording network traffic either for the information itself or to mount another attack
   iv) infiltration of De Montfort University (e.g. becoming a network or system administrator) to obtain information
   v) oversight of screens while working (see Note below)

b) denial of service by attacking network devices or systems

   i) malicious software
   ii) system corruption
   iii) mail flooding
   iv) packet flooding.

Notes:

Oversight of screens is relevant to the network since network controls are applied on the basis of location.

Although the attack of systems located on the Internet from the University Network is not a threat to De Montfort University per se, subject to specific needs, restrictions on actions which could allow attacks will be restricted (for example ping and finger might be disallowed other than by network administration staff).

Although outgoing viruses are not a threat to De Montfort University, virus checking shall be performed by the network on all incoming and outgoing mail through the firewall.

4 De Montfort University Network

4.1 Network Overview

4.1.1 De Montfort University's network provides access to administrative and academic systems..

4.1.2 The University Network service will need to evolve over time but must facilitate:

a) Access by External Users to open access material via the Internet

b) Access by students:

from Student Terminals and from remote locations from student owned devices to:

- their own (low sensitivity) served file space and mailbox
- learning resources
- open access material
- course material (access controlled at system or application level)
- the Internet
- administrative information
- personal information

c) Access by De Montfort University Members, excluding students, and Approved Visitors:

i) from staff offices to:

- served file space (including low sensitivity area if allocated) and mailbox
- learning resources
- course materials
- open access material
- administrative systems
- the Internet

ii) from student terminals to:

- low sensitivity served file space
- learning resources
- course materials
- open access material
- the Internet

iii) remotely, using dial-in or the Internet to:

- served file space (including low sensitivity area if allocated) and mailbox
- learning resources
- course materials
- open access material
- administrative systems

d) Access to defined secure enclaves from defined locations on De Montfort University campuses and from remote locations

e) Transfer of e-mail between De Montfort University Members, Approved Visitors and External Users

f) Transfer of information by the owner/custodian, or those authorised by the owner/custodian, to areas for replication to Internet-accessible servers.

4.1.3 Virus checking and countermeasures will be performed at system and application level.

4.2 Network Description

4.2.1 De Montfort University Network services may be provided to any building or room which is under the control of De Montfort University and is either left locked or has access controls such as a security reception desk or ID card controlled turnstile. Buildings are inter-linked by means of De Montfort University-owned cabling or WAN services. The network will span multiple De Montfort University sites.

4.2.2 Associate colleges which comply with the Community Security Policy (Reference 1) and this Network Security Policy may be connected as part of the De Montfort University Network. Otherwise they shall be treated as any other form of Internet access and traverse the secure network boundary. Users at franchise colleges and in student residences shall traverse the secure network boundary.

4.2.3 The University Network is focused on the Leicester City campus with connections radiating to the other sites.

4.2.4 The University Network is required to support the University's staff and students.

4.2.5 External network connections include Internet access via JANET and dial-up access to various locations.

4.3 Connected Systems

4.3.1 Central systems are managed by Information Services and Systems while others are managed by individual faculties or departments.

4.3.2 All connected hosts and servers will be located in secure areas with controlled access.

4.3.3 Client devices may be owned and configured on a central or a devolved basis and use a diverse set of hardware platforms and operating systems as:

a) some faculties have particular client requirements (e.g. Apple Mac's and UNIX workstations)

b) usage of portable computers is likely to increase and the network is required to support their use

c) individuals are be allowed to connect their own portable computers

d) no assumptions can be made about devices accessing the University Network via the Internet.

5 Security Measures

5.1 Introduction

5.1.1 The integrated network requires the implementation of security measures to contribute to the overall protection afforded to the University systems and information.

5.1.2 As a point of good practice, if particular equipment allows additional controls to be applied without significant administrative overhead, without unduly restricting user services, and in an easily maintainable manner, the implementation of these controls should be considered.

5.2 Architecture

5.2.1 The De Montfort University network shall have a defined secure boundary. Access shall be controlled across the boundary using:

a) a firewall (protected by a screening router) with authentication in an application proxy

b) dial-in using encryption to an authenticating server

c) dial-back to pre-defined PSTN numbers (providing that the line is dropped between dial-in and dial-back), additionally using encryption if access by means of a mobile telephone.

5.2.2 As detailed in Reference 2, access to information internally shall be based on the location of the dient device (see Table 5.1 below). Knowledge of this location may be derived from:

a) the fact that a cable is known to terminate in a particular location

b) the fact that ports, MAC addresses or IP addresses are associated with particular cable runs and may potentially be configured into a VLAN

c) the fact that a trusted user authenticates to a suitable network device implicitly confirming that the user is in a particular type of location.

5.2.3 Hosts and servers shall also be located on the network in a manner corresponding to their sensitivity and the measures in place to control client access (i.e. Member of VLAN or protected by a firewall). The relevant System Manager shall review the means of connection with the IT Security Officer and the Network Manager to ensure that the system is connected appropriately.

5.2.4 Highly sensitive information shall be located within networks which are:

a) restricted to personnel trusted for accidental access to the information

b) separated from the rest of the De Montfort University network by means of a firewall or other gateway requiring authentication for incoming access.

5.2.5 Information for dissemination to External Users shall be stored on servers outside the secure boundary.

Location	Highest Sensitivity	Other controls
Student Computer Laboratory, Library	Low	Packet scrambling for packets not addressed to the particular MAC address (auto-learn of MAC addresses is permissible)
Electronic kiosks	Medium	Client functionality limited to that needed for the function, system controls to ensure that personal information is only released for the currently authenticated user, access only possible to a copy (not the master) of any information of Medium sensitivity
Enclaves	High	Firewall requiring authentication when access is across the University Network, network access only possible from specifically defined locations, no unencrypted access across the Internet
Other staff offices	Medium	

Table 5.1 - Location-based Access Controls

5.2.6 Figure 5.1 illustrates the permitted information flows and the logical location of the security measures described in this document and in the Community Security Policy (Reference 1).

5.2.7 Authentication details shall not traverse the Internet unencrypted.

5.2.8 Highly sensitive information shall not traverse the Internet unencrypted.

5.3 Staff Controls

5.3.1 The Network Manager shall assure that Network Administration staff are sufficiently trustworthy for the potential access that could be gained to information on the network.

5.3.2 The Network Manager shall vet all requests for non-Network Administration staff to have access to controlled network areas (as described in Section 5.5), equipment or configuration details.

5.4 Building Access Controls and Authentication

Access to each building to which University Network services (inside the Internet firewalls) are provided shall require either the display or use of a De Montfort University identity card to gain entry or the registration and authentication of the person as a valid visitor.

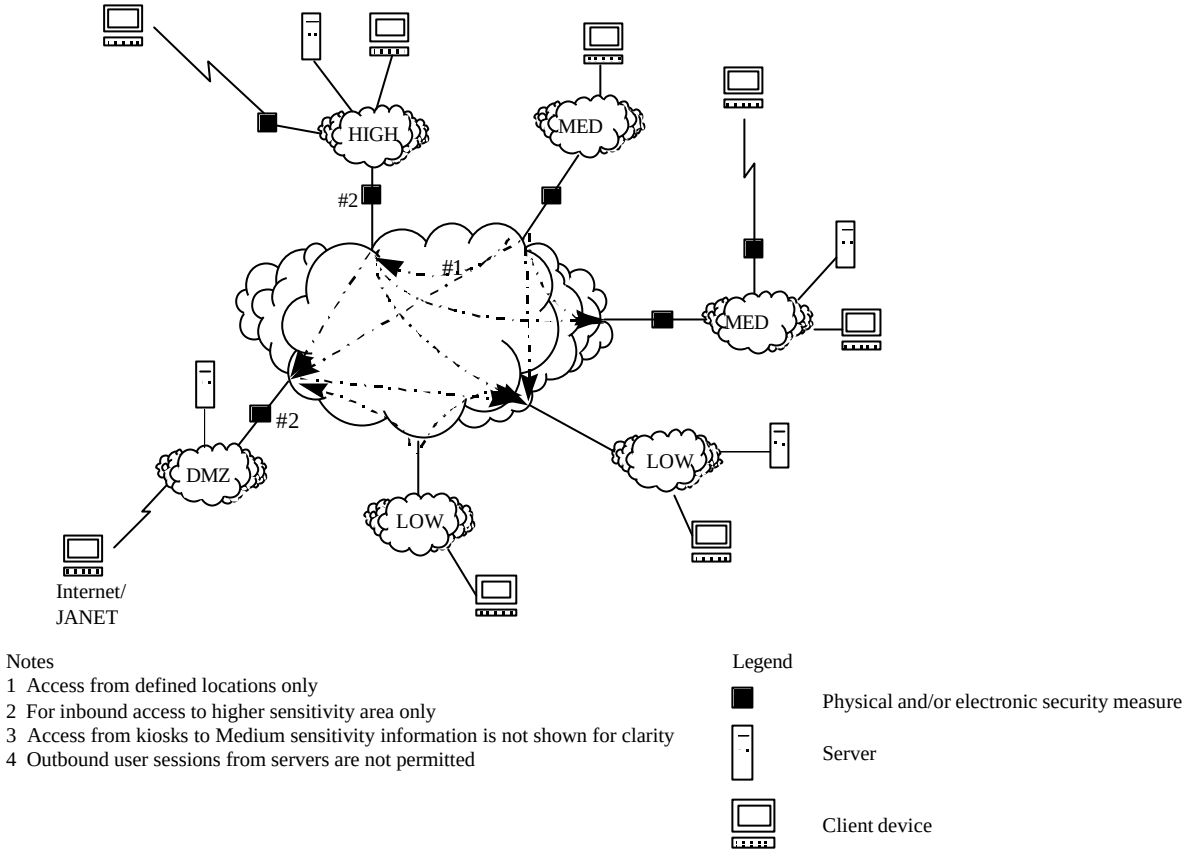

Figure 5.1 - Illustration of Security Architecture

5.5 Host/Server and Network Physical Access Controls

5.5.1 Physical access to rooms containing servers providing network services, active network devices and patching shall be restricted to:

a) authorised staff

b) other individuals provided that their entry has been approved by the relevant system or network manager and that they are escorted by authorised individuals.

5.5.2 The owner of each room shall maintain a list of authorised staff.

5.5.3 Rooms containing servers providing network services, active network devices and patching shall be locked at all times when not occupied and access to the keys controlled

5.5.4 Where key-pad locks are used, the codes shall be changed on a 3 monthly basis or if compromised. Out of hours, key-pad locks shall be supplemented by means of a key lock.

5.5.5 Communications cabinets shall be left locked to discourage tampering.

5.5.6 Physical access to the Network Management System shall be restricted to:

a) authorised network administration staff

b) other individuals provided that their access has been approved by the Network Manager and that they are escorted by authorised individuals.

5.5.7 Physical access to backbone cabling by unauthorised individuals shall be prevented by such measures as robust trunking, burial, etc.

5.6 Location Restrictions

5.6.1 Access to Highly sensitive information stored within enclaves shall be allowed from only defined locations (including remote locations and suitable staff offices away from the enclave) which are suitable for processing that information.

5.6.2 Access to information which has greater than Low sensitivity shall be prohibited from locations used by students.

5.6.3 Remote access shall be permitted by any of the following mechanisms (subject to the system and application level controls):

a) via the Internet Firewall using authentication in an application proxy

b) using dial-back to an approved non-mobile telephone number

c) using encrypted circuits.

5.6.4 Servers holding sensitive information shall be connected to the network such that the client access restrictions are enforced as described in Section 5.2.2.

5.7 Access to Network Device Configuration

5.7.1 Access to network device configuration details and software on all network devices, including servers providing network services, shall be as restricted as much as possible consistent with delivery of the user services or network administration functions.

5.7.2 Network devices shall provide at least basic electronic access controls (e.g. community string) prior to allowing any extraction or modification of device configuration whether in-band over the network or by use of local terminal or front panel.

5.7.3 Access to network device configurations over the network shall be restricted to access from the Network Management System (NMS) on the basis of its (static) IP address.

5.7.4 Firewalls shall be managed using secure connections (e.g. from a LAN dedicated to firewall management, directly connected consoles, or encrypted sessions over the LAN). This LAN shall be physically accessible only from locations restricted to authorised network and system administration staff or by means of PSTN circuits using encryption or dial-back.

5.7.5 Access to and authentication controls on the NMS shall be consistent with the operational need, e.g. to have a continuous display of the network status.

5.8 Configuration and Change Management

5.8.1 All proposed changes to the architecture of the network shall be approved by the IT Security Manager prior to their implementation.

5.8.2 Prior to implementation of any new service or use of new type of component, the effectiveness of security measures shall be tested, see Reference 1, to demonstrate that the proposed change achieves the desired effect, is secure in itself, and does not introduce new weaknesses. The results of the tests shall be

reviewed by the Network Manager and the IT Security Manager as part of the approval process.

5.9 Records of Device Configuration

5.9.1 Records of the location and configuration of the network and network devices shall be maintained in order to:

a) allow the audit of actual configurations

b) investigate the scope of any potential weaknesses discovered.

5.9.2 Records of the configuration of network devices shall be disclosed only to staff authorised by the Network Manager.

5.10 Internet Access

5.10.1 Internet access circuits shall be connected to routers, acting as screening routers, with direct connections only to those circuits and application level gateway firewalls (hereafter referred to as Internet Firewall(s)). Screening routers shall be configured to prevent external users pretending to be accessing the network internally.

5.10.2 All access to and from the Internet shall be mediated by appropriately configured application level gateway firewalls with 3 network interfaces connected to:

a) the Internet access circuit

b) a network (De-Militarised Zone (DMZ)) hosting servers containing open access information

c) the De Montfort University Network.

5.10.3 Access to the De Montfort University Network from the Internet shall require authentication by an application proxy on the Internet Firewall and/or tunnelling using an encrypted session between De Montfort University and another secure and defined location.

5.10.4 Remote access to information of sensitivity greater than Low shall be prevented across the Internet other than by means of tunnelling (see 5.10.3); instead such access shall typically be facilitated by suitably protected dial-in access (see 5.2.1).

5.10.5 Open access information to be distributed via the Internet shall be placed on a reference server on the De Montfort University side of the Internet Firewall and information shall be copied to expendable hosts in the DMZ.

5.10.6 Internal IP addresses shall not be visible to External Users or Internal Users accessing the University Network via the Internet.

5.10.7 The Internet Firewall shall implement restrictions on out-going traffic as follows:

a) any network traffic other than that used for information access (e.g. ping, finger) shall be barred unless from the NMS or other authorised IP addresses

b) remote logon (rlogon) shall be prevented other than from authorised IP addresses.

5.11 Authentication

5.11.1 The Network Management System, and all firewalls and servers providing network services shall ensure that users are authenticated by means of user identity and password prior to granting access.

5.11.2 The Network Manager shall maintain a record of those persons having electronic access to the systems maintaining network configuration details.

5.11.3 Passwords (including SNMP community strings) used in the network shall be subject to the following constraints:

a) minimum length - 6 characters where practicable on the equipment in use and preferably longer, especially if the device does not support automatic lockout after a limited number of incorrect attempts

b) passwords shall not be words, names, car registration numbers or similar, or simple variations on those themes

c) passwords shall be different for each device under a user's control (however it is acceptable for passwords on network devices to use coded variations; e.g. based on location)

d) passwords shall be changed every 12 months and if compromised.

5.11.4 A record of changes made to passwords on active network equipment and servers providing network services (e.g. DHCP) and to those who know passwords shall be maintained by the Network Manager.

5.11.5 Passwords shall not be disclosed deliberately or inadvertently to any person. If a password is disclosed, the disclosure shall be logged and the password changed immediately disclosure is discovered.

5.11.6 If supported by the system/equipment, logon failures against the user identity shall be reported at the next successful logon by that user to the system.

5.11.7 The NMS, firewalls and any servers providing network functionality shall implement automatic lockout after, at most, 5 invalid attempts to log on using a particular user identity.

5.12 Encryption

If information of greater than Low sensitivity is to be sent over the Internet, encryption shall be applied between the end-system or the network inside the Internet Firewall and the remote end. The encryption algorithm to be used shall be subject to approval by the IT Security Manager.

5.13 Accounting and Audit

5.13.1 The following accounting and audit logs shall be maintained:

a) network and device configuration (possibly by off-line storage of NMS data)

b) firewall configurations

c) network configuration changes

d) firewall configuration changes

e) authentication of users by firewall proxies

f) log of persons allowed access to controlled network locations.

5.13.2 Accounting logs and audit trails shall be protected from modification.

5.13.3 The following audit tasks shall be performed:

a) Annually - Checking the list of those persons allowed access to controlled network locations

b) 6 monthly - Audit of Internet firewall configuration

c) Annually - Sample audit of network configuration

d) Monthly - Check audit logs compiled by Internet firewalls

e) Annually, on a random basis, and on detection of a potential security weakness - conduct penetration tests of the security features.

5.14 Prevention of Interception

Where network outlets are in areas not supervised by members of staff, the network shall implement measures to ensure that only traffic addressed to the relevant MAC address is transmitted to that outlet. Automatic learning of connected MAC addresses shall be permitted to limit the administrative overhead.

5.15 Packet and Mail Filtering

5.15.1 Should attempts be detected to flood the University Network with email messages or IP datagrams, appropriate filters shall be configured on the routers or mail servers as appropriate.

5.15.2 Mail servers shall be configured with a maximum message size as a constraint on mail flood attacks.

5.16 Virus Checking

5.16.1 Virus checking shall be performed on all incoming and outgoing mail.

5.17 Investigation of Security-Related Incidents

5.17.1 All potentially security-related incidents shall be reported to the Network Manager who shall arrange for their investigation. These incidents shall be logged and the investigations and outcomes shall be reviewed on a regular basis with the IT Security Manager.

5.17.2 The IT Security Manager shall comply with the prevailing JANET Computer Emergency Response Team (CERT) procedures.

5.18 Security Management

5.18.1 The Network Management Team shall keep up to date with developments in network security features and attacks.

5.18.2 The Network Management Team shall review developments in threats and counter-measures with the IT Security Manager on an annual basis for their relevance to the University Network.

6 Security Administration

6.1 Organisational Structure

6.1.1 The IT Security Manager has overall responsibility for the security of De Montfort University IT resources. The IT Security Manager is responsible for the Network Security Policy document and subordinate security documentation.

6.1.2 The Head of the Communications and Networking Group is the Network Manager. Network Administrators report to the Network Manager.

6.1.3 Management of connected systems shall be performed in accordance with the Community Security Policy (Reference 1).