Network Security Policy v1.0

Organisation	Oxford Brookes University
Title	Network Security Policy
Creator	Gareth Packham - Head of Information Management
Approvals Required	1. Information Security Working Group 2. CIO 3. Executive Board
Version	Version 1.0
Owner	Chief Information Officer
Subject	The formal, approved, network security policy of Oxford Brookes University
Review date and responsibility	Annually by Head of Information Management

Revision History			
Date	Author	Version Number	Comments
20/09/16	Gareth Packham	0.1 (draft)	Original draft
14/09/16	Gareth Packham	0.2 (draft)	Minor revisions only; clarification of “network” and “network systems”
17/03/17	Gareth Packham	1.0 (live)	Minor revisions only

1. Introduction and Policy Aim

1.1 This document defines the Network Security Policy for Oxford Brookes University (OBU). The Network Security Policy applies to all network hardware, services on the network and network attached systems.

1.2 For the purpose of this policy a network is defined as Oxford Brookes University's connected (physically and wirelessly) data network that allows computing devices (including phones) to exchange data.

1.3 The aim of this policy is to ensure the security of the network. To facilitate this, the university shall:

- Protect assets against unauthorised access or disclosure **(Confidentiality)**
- Protect the network from unauthorized or accidental modification and ensure the accuracy and completeness of data assets **(Integrity)**
- Ensure the network is accessible how and when users need it **(Availability)**

2. Policy Objectives

2.1 To protect all hardware, software and information assets under its control. This will be achieved by implementing a set of well-balanced technical and non-technical measures.

2.2 To provide effective protection that is commensurate with the risks to OBU network assets.

2.3 To implement the policy and associated procedures in a consistent, timely and cost-effective manner.

2.4 To ensure OBU is compliant with all relevant legislation, including (but not limited to:

- The Data Protection Act 1998
- Computer Misuse Act 1990
- Human Rights Act 1998
- Freedom of Information Act 2000
- Electronics Communications Act 2000
- Copyright, Designs & Patents Act 1988

3. Physical & Environmental Security

3.1 Network equipment (principally routers, switches and servers) shall be housed in a controlled and secure environment. Critical or sensitive network equipment will be housed in an environment that is monitored for temperature, humidity and power supply quality.

3.2 Critical or sensitive network equipment will be housed in secure areas, protected by a secure perimeter, with appropriate security barriers and entry controls.

3.3 Critical or sensitive network equipment will be protected from power supply failures and protected by intruder alarms and fire suppression systems.

3.4 Smoking, eating and drinking is forbidden in areas housing critical or sensitive network equipment.

3.5 All visitors to secure network areas must be authorised by an appropriate manager.

3.6 All visitors to secure network areas must be made aware of network security requirements.

3.7 The movement of visitors to secure network areas must be recorded. The log will contain name, organisation, purpose of visit, date, and time in and out.

3.8 The Network Manager, or appropriate deputy, shall ensure that all relevant staff are made aware of procedures for visitors and that visitors are escorted when necessary.

4. Access Control to the Network

4.1 Access to limited-access network services shall be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access. Remote access to the network will be via the University's remote access software.

4.2 Departmental business managers will approve user access to systems including network access via standard staff joiner/leaver processes.

4.3 Access rights to network services will be allocated on the requirements of the user's role, rather than on a status basis.

4.4 All users users of network services will have their own individual user identification and password.

4.5 Users are responsible for ensuring their password is kept secret (please see OBU's Password Policy for further details).

4.6 User access rights shall be removed or reviewed for those users who have left the

University or changed roles as soon practically possible.

5. Third Party Access Control to the Network

5.1 Third party access to network systems, services, hardware and network attached systems shall be based on a formal contract that satisfies all necessary security conditions.

5.2 All third party access to network systems, services, hardware and network attached systems must be logged.

5.3 For further information please refer to the University Third Party & Supply Chain Management Policy

6. Maintenance and Fault Management

6.1 The Network Manager will ensure that adequate maintenance contracts are maintained and periodically reviewed for all network equipment.

6.2 The Network Manager is responsible for ensuring that a log of all faults on network systems and equipment is maintained and reviewed.

6.3 OBU shall ensure that timely information regarding the technical vulnerabilities of information systems is obtained. Any vulnerability will be assessed and any risks will be appropriately controlled.

6.4 The use of privileged utility programs that may be capable of overriding system and application controls shall be controlled and restricted.

6.5 Operational software shall only be installed by authorised system administrators and authorised third-parties (see section 5).

7. Network Operating Procedures

7.1 Documented operating procedures should be prepared for the operation of network services and systems, to ensure their correct, secure operation.

7.2 Changes to operating procedures must be authorised by the Network Manager.

8. Data Backup and Restoration

8.1 The Network Manager is responsible for ensuring that backup copies of network

configuration data are taken regularly.

8.2 Documented procedures for backup processes and storage will be produced and communicated to all relevant staff.

9. User Responsibilities, Awareness and Training

9.1 The University will ensure that all users of network systems, services, hardware and network attached systems are provided with the necessary security guidance, awareness and where appropriate training to discharge their security responsibilities.

9.2 All users of network services and systems must be made aware of the contents and implications of the Network Security Policy.

9.3 All users must ensure that they protect the network from unauthorised access. They must log off the network when finished working.

9.4 Irresponsible or improper actions by users may result in disciplinary action

10. Protection against Malware

10.1 Software to protect against malware should be installed on all client devices including mobile computing assets.

10.2 Software used to protect University systems against malware shall be regularly reviewed and updated.

10.3 Procedures on dealing with malware protection and attacks shall be developed and documented together with appropriate business continuity plans.

11. Clock Synchronisation

11.1 All network systems and services shall be synchronised using ntp.brookes.ac.uk

12. Logging & Monitoring

12.1 Adequate event logs recording network activity, exceptions, faults and information security events shall be produced, kept and regularly reviewed.

12.2 Logging facilities and log information shall be protected against tampering and unauthorised access.

12.3 The activity of privileged users shall be logged and the logs protected and regularly reviewed.