Information Security Policy

Network Management

1 Introduction

1.1 Connections to the University's Information and Communication Technology [IT] networks (including remote access, whether through VPNs or direct service connection) have to be properly managed to ensure that only authorised devices/persons are allowed to connect. Availability, security and integrity of information require appropriate planning and configuration of the University's networks.

2 Purpose

2.1 This policy defines requirements for the management and operation of IT networks.

3 Scope

3.1 This policy applies to those responsible for the provision and management of IT networks owned by or operated on behalf of the University.

4 Policy

4.1 The University's network shall be managed by suitably authorised and qualified staff to oversee its day to day running and to preserve its security and integrity in collaboration with individual system owners. All network management staff shall be given relevant training in Information Security issues.

4.2 The network must be designed and configured to deliver high performance and reliability to meet the University's needs whilst providing a high degree of access control and a range of privilege restrictions.

4.3 The network must be segregated into separate logical domains with routing and access controls operating between the domains. The levels of control must be commensurate with the access policy requirements of the domains being interconnected. For example, appropriately configured firewalls shall be used to protect the domains containing especially sensitive information or particularly vulnerable equipment, such as the University's business systems.

4.4 Separate domains must exist to gather together computing resources which pose higher risks to the operation of the University's business

systems in order that appropriate access controls can be applied. For example, public workstations ("student clusters") will be treated differently from servers and from staff workstations; staff and student personal workstations are different again; computing resources on the Internet in general are treated differently from those on campus in general.

4.5 Access to the resources on the network must be strictly controlled to prevent unauthorised access, and access control procedures must provide adequate safeguards through robust identification and authentication techniques. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorised.

4.6 Interception of traffic and recording of communications data will only be carried out by staff authorised so to do by IT Services, and will be in accordance with the University's Policy for Institutional Access to information within University IT Accounts, Equipment and Networks.

4.7 Remote access to the network will be subject to robust authentication and VPN connections to the network are only permitted for authorised users ensuring that use is authenticated and data is encrypted during transit across the network.

4.8 The implementation of new or upgraded software or firmware must be carefully planned and managed. Formal change control procedures shall be used for all changes to critical systems or network components. All changes must be properly tested and authorised before moving to the live environment.

4.9 Moves, changes and other reconfigurations of users' network access points will only be carried out by staff authorised by IT Services according to procedures laid down by them.

4.10 Networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorised intrusion.

Ownership:

Owner	Department/Team
Director ITS	ITS

Authors:

Author(s)	Department/Team
Jeremy Maris	Client Services

Contributors and Reviewers:

Contributor/Reviewer	Department/Team
Matthew Trump	Information Service Assurance Manager

Revision History:

Version Number	Status D/R/A/I[1]	Date Issued	Reason for Issue	Issued by
1.0	D			JM
1.1	I	27/05/09		Iain Stinson
1.2	I	3/3/15	Updated and Approved by ISC for Issue	PD
1.2	D	6/2015	Reformatted. Add Policy control page	SR
1.3	I	20 June 2017	Minor Amendments	MT

[1] D = Draft; R= Ready for approval; A = Approved for issue; I = Issued