Information Security Policy

Systems Management

1 Introduction

1.1 This Policy sets out the responsibilities and required behaviour of those managing University Information systems.

2 Objectives

2.1 To ensure the availability of systems.

2.2 To protect the integrity of systems and information from malicious software and people with malicious intent.

2.3 To prevent unauthorised access to systems.

2.4 To detect unauthorised activities.

3 Scope

3.1 This policy applies to managers with responsibility for the provision of information and business systems and the staff who manage their day-to-day operations.

3.2 Information systems should be understood to mean the critical information systems that serve the core purpose of the University e.g. Library systems, Financial systems, Student systems, E-learning systems, Email, Web servers etc.

4 Policy

4.1 The University's information systems shall be managed by suitably trained and qualified staff with relevant training in Information Security issues. In collaboration with those responsible for its business purpose they will oversee the day to day running of the system to preserve confidentiality, availability and integrity.

4.2 Access controls shall be maintained at appropriate levels for all systems by proactive management. Changes in access permissions to systems or applications must be authorised by the manager responsible for the service.

A record of access permissions granted or revoked must be maintained.

4.3 Access to all information services must be via an appropriately secure log on process in accord with the Account Management and Password Policy.

4.4 Active connections to the University's business systems must not be left unattended and shall time-out or require re-authentication after a defined period of inactivity to limit access by unauthorised persons.

4.5 Access to commands and functions that control the operation of the system must be restricted to those persons who are authorised to perform systems administration or management functions. Where appropriate, use of such commands should be logged and monitored.

4.6 For internally operated systems, the implementation of new or upgraded software must be carefully planned and managed in accord with the Software Management Policy. Formal change control procedures, with audit trails, shall be used for all changes to internally operated business systems. Where systems are provided by external service providers, the service and business owners shall ensure that the service provider implements and maintains acceptable change management and change control procedures.

4.7 Capacity demands of internally operated systems supporting business processes shall be monitored and projections of future capacity requirements made to enable adequate processing power, storage and network capacity for planning purposes. For externally operated systems, the service and business owners shall ensure that appropriate capacity management arrangements are implemented and maintained.

4.8 Security event logs, operational audit logs and error logs must be properly and regularly reviewed.

4.9 System clocks must be synchronised against the University's network time servers, or ultimately against a time source against which the University's network time servers are themselves synchronised.

4.10 Information systems operated by the University must use appropriately supported operating software maintained by the application of relevant security updates. For externally operated systems, the service owner shall ensure that appropriate arrangements for updating underlying software and infrastructure are implemented and maintained. Exclusions to this must be approved by the IT Services Director.

4.11 Internally operated systems must be regularly checked to ensure that they comply with the University's Information Security Policy. For externally operated systems, the service and business owners shall ensure that appropriate arrangements are in place to ensure ongoing compliance of the service with the agreed information security measures.

5 Related Policies

5.1 System administrators should abide by the Systems Administrators Charter which provides additional guidance.

5.2 This policy should be read alongside the Third Party Access Policy, Software Management Policy and System Operations Policy.

Ownership:

Owner	Department/Team
Director ITS	ITS

Authors:

Author(s)	Department/Team
Jerry Niman	Consultant

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
1.2	R	23/02/2015	Issued to ISC	PD
1.3	I	3/3/15	Approved by ISC for Issue	PD
1.4	I	20 June 2017	Minor Amendments	MT

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