Software Management Policy

1 Introduction

1.1 This Policy sets out how the software that runs on the University's information systems shall be managed. The policy includes controls on the installation and use of software, the features provided and the granting of access to software packages. In addition, it covers the maintenance of software, with appropriate procedures for upgrades, to minimise risks associated with Information and Communication Technology systems.

2 Objective

2.1 To ensure that information security controls are applied to the procurement, implementation, management and maintenance of business critical software.

2.2 To reduce the risk of failure of critical information systems.

2.3 To reduce the risk of compromise to the integrity and confidentiality of business data.

3 Scope

3.1 The policy applies to all staff involved in the specification, installation and maintenance of software.

3.2 Business software should be understood to mean the software component of 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 business applications are to be managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity in collaboration with nominated individual application owners. All business application developer, specifying and management staff shall be given relevant training in information security issues.

4.2 The procurement or implementation of new, or upgraded, software must be carefully planned and managed. Any software development undertaken for or by the University must follow a formalised development process or methodology appropriate for the type of development being undertaken. Information security risks associated with such projects must be assessed and mitigated.

4.3 Business requirements for new software or enhancement of existing software shall specify the requirements for information security controls.

4.4 Formal change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to business software operated by the University. All such changes must be properly authorised and all software, including that which interacts with the amended software, must be tested and satisfactory for the purpose before changes are moved to the live environment.

4.5 Modifications to commercially supplied software shall be allowed only when essential to the business purpose. The risk of invalidating support contracts shall been measured and accepted by the service and business owners. Modifications to Open Source software shall be strictly controlled and essential to the business purpose; wherever possible these changes shall be managed through the formal channels utilised in the development of the software and the risk shall be assessed and must be accepted by the service and business owners.

4.6 The implementation or modification of software on the University's business critical systems and operated by the University shall be controlled. All software operated by the University shall be tested before implementation to ensure that it meets the business purpose and that information security controls are adequate.

4.7 Where business critical systems, or infrastructure that they depend on, are provided by external service providers, the service and business owners shall ensure that the service provider implements and maintains adequate change management and change control procedures.

5 Related Policies

5.1 This policy should be read alongside the Systems Management Policy, the System Operations Policy and the Third Party Access 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
1.0	R	25/01/2010	Final version to ISWG	
1.1	D	8/1/2015	Excluded externally hosted services from 4.4 and 4.6. Added 4.7. Added Outsourcing Policy to 5.1	JN
1.2	R	25/2/2015	Reformatted and updated references to IS policies. Issued for ISC Approval	PD
1.3	I	3/3/15	Approved by ISC for issue	PD
1.4	!	20 June 217	Minor Amendments	MT

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