Policy for the Operation of Information and Communications Technology Systems

1 Introduction

1.1 This Policy defines information security controls relevant to the operation of the University's information and Communications Technology (ICT) systems. It includes standard procedures and responsibilities for the operation of information systems and the need for fault and incident reporting and review.

2 Objectives

2.1 To assess Information security risks and adopt an appropriate operations procedure that reduces the risk of damage from security incidents and malfunctions. To monitor and learn from such incidents.

2.2 To prevent unauthorised physical access, damage and interference to business premises and information systems.

2.3 To ensure the correct and secure operation of information processing facilities.

3 Scope

3.1 This policy applies to managers with responsibility for the operation of information processing activities.

4 Policy

4.1 Areas and offices where sensitive or critical information is processed shall be given an appropriate level of physical security and access control. Staff with authorisation to enter such areas are to be provided with information on the potential security risks and the measures used to control them.

4.2 Procedures for the operation and administration of the University's business systems and activities shall be documented and regularly reviewed.

4.3 Duties and areas of responsibility shall be segregated to reduce the risk and consequential impact of information security incidents that might result in financial or other material damage to the University. For example creating suppliers, raising invoices and approving invoices must not be undertaken by a single role.

4.4 Procedures will be established and widely communicated for the reporting of security incidents and suspected security weaknesses in the University's business operations and information systems. Mechanisms shall be in place to monitor and learn from those incidents.

4.5 Procedures will be established for the reporting of software malfunctions and faults in the University's information systems. Faults and malfunctions shall be logged and monitored and timely corrective action taken.

4.6 Changes to operational procedures must be controlled to ensure ongoing compliance with the requirements of information security and must have management approval.

4.7 Development and testing facilities for business critical systems shall be separated from operational facilities and the migration of software from development to operational status shall be subject to formal change control procedures.

4.8 Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to migration to operational status. Tests involving live data or periods of parallel running shall only be permitted where adequate controls for the security of the data are in place.

4.9 Procedures shall be established to control the development or implementation of all operational software. All systems developed for or within the University must follow a formalised development process

5 Related Policies

5.1 This policy should be read alongside the Software Management Policy, System Management Policy and the Policy for Outsourcing or Granting Third party access to University Information Systems.

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
2.0	A and I	09/10/2014	Approved by ISC	PD
2.1	I	01/06/2015	Reformatted, Policy control page added Header and footer added	SR
2.2	I	20 June 2017	Minor Amendments	MT

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