GISP9. Change management

Date:	5 October 2017
Version:	2.0
Authors:	Raymond Scott
Quality Assurance:	Information Strategy and Services Committee (ISSC)

Version control

Revision	Date	Revision Description
1.0	8/11/12	Approved by ISSC
1.1	5/10/17	Reviewed and updated
2.0	20/10/17	Approved by ISSC

Policy

Security Control	All University IT and computing facilities/services to be maintained in a secure state irrespective of any changes to infrastructure or business processes.
Objective	To ensure that security matters are considered as an integral part of any change process where IT and computing facilities, or information processing is involved.
Policy	9.1. Security issues must be seriously considered in any process or project where the IT and computing infrastructure may be changed, or the manner in which information is processed is likely to change. Where a project is particularly reliant on IT and computing facilities/services, security should be addressed under a specific heading within the project plan. 9.2. Where IT and computing facilities/services are subject to change compliance with relevant legislation should also be reviewed (see GISP16). 9.3. System planning processes should explicitly define and document the legal obligations arising from the operation of the proposed system. There is a named individual responsible for updating that information. 9.4. Changes to operational procedures must be controlled to ensure on-going compliance with the requirements of information security and must have management approval. 9.5. Formal change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to business software. All changes must be properly authorised and all software, including that which interacts with the amended software, must be tested before changes are moved to the live environment.
Responsibility	• ITCS will advise on best practice. • Project managers are responsible for ensuring that security matters are seriously considered in projects involving IT and computing facilities, or information processing. • Service owners are responsible for ensuring on-going security compliance when undertaking any change.

Incident Management	If IT facilities/services are discovered to be insecure, this should be reported to ITCS, who will investigate and address matters with relevant project managers and stakeholders.
Implementation	• ITCS will define a process and develop templates to manage and record changes to services accounting for the impact on information security.