GISP12. Secure areas

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	Access to secure areas must be strictly controlled and monitored.
Objective	To ensure that access to computer and telecommunications systems in secure areas/buildings is strictly controlled and monitored with only authorised individuals having access.
Policy	12.1. All secure areas must comply with University building security recommendations. 12.2. Documented authorisation and authentication procedures and mechanisms must be implemented for every secure area to ensure that only authorised individuals can access the area. 12.3. Where sensitive data is stored in secure areas, network access to that data must be carefully controlled and monitored following documented procedures. 12.4. Sensitive data supplied by third parties must be stored in secure areas in compliance with the agreement with the third party. 12.5. Each secure area must have a designated individual responsible for day to day security of that area.
Responsibility	• University Security is responsible for overall building security on campus. • The manager of a secure area within a building is responsible for the security of that area.
Incident Management	• Breaches of building security should be reported immediately to University Security. • For secure areas within buildings, breaches of security should be reported to the manager for the area in question.
Incident management	Where IT security of a secure area is found/judged to be inadequate, this should be reported immediately to the manager for that area.

	Where IT security mechanisms are discovered to have been breached, the manager of the area should liaise with ITCS and other University agencies as appropriate and take the necessary action to remove/reduce any security threats. Details of the incident should be recorded, including times/dates, relevant system logs and actions taken. If the breach is considered to have been a major one, with significant impact on data and services, a full report should be submitted to Faculty management or ITCS Divisional Directors as appropriate. The Security Risk log should also be reviewed in light of such incidents.
Audit and accountability	Managers of the secure areas should audit IT security of the areas on a regular basis (at least annually), taking remedial action as appropriate. Outstanding issues and deviation from these controls should be recorded in the annual Security Policies Implementation Issues Log which is collated by ITCS and submitted to ISSC for review.
Implementation	• A manager of the secure area should be nominated and they will be responsible for all aspects of the area's security (physical and IT security) • Physical security controls should be applied – see GISP3. • Data associated with the secure area should be stored and handled in accordance with security controls/ policies detailed in the Information Classification and Data Management Policy. • There may also be additional data controls/policies as applied by a funding agency that must be abided by. • Only secure encrypted data channels should be used to connect to systems and data, except where insecure data protocols are implicit within the service, e.g. HTTP for web services. • It should be ensured that the necessary University Firewall policies are in place to protect against unauthorised external access to systems, see GISP8. • It should be ensured that all systems operated from, or stored within the secure area are appropriately protected against unauthorised user access by complying with policies and security controls as listed below: GISP4. Identification, authentication and authorisation GISP5. Use of passwords • It should be ensured that the segment of network used for the secure area is appropriately protected against unauthorised access via the University network. Where appropriate this may mean a separate subnet being used for the secure area and/or use of the University Firewall policies to mediate access. The appropriate mechanisms should be determined by agreement with ITCS Network Services. • All network connected equipment used within the secure area, or used to connect to the secure area, should comply with University equipment registration security controls and policies. • A Security Risk Log for services/systems operating from the secure area should be created and reviewed on a regular basis (at least annually).