GISP3. Physical and environmental security

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	Physical access to computer and telecommunication systems proportionate to the sensitivity of the data held on those systems will be managed to restrict access to authorised users only.
Objective	• To ensure that only those authorised to do so can physically access computer and telecommunication systems. • To prevent theft and unauthorised tampering with information assets • To prevent theft and unauthorised tampering with computer resources
Policy	3.1 All computer systems must be located in an environment which is secure against theft and complies with University building security recommendations. 3.2 Screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons. 3.3 Computer servers and telecommunications equipment should be housed in especially secure areas to which physical access is controlled with only authorised users being allowed access.
Responsibility	• For centrally managed services, physical access to computer servers will be the responsibility of ITCS. • Departments are responsible for the physical security of their servers located in their building. Where department servers are located in ITCS's computer suites, their physical security will be the responsibility of ITCS. • For computers located in staff offices it is the responsibility of the occupier to ensure that their office is locked when no one is there.
Incident Management	Breaches of physical security will be investigated by the manager responsible for security of the area concerned. The investigating manager is responsible for assessing the impact of any unauthorised data access and this should be reported to the IT Service Desk or, if of a sensitive nature, reported to Assistant Director Strategy, Policy and Compliance, or in their absence the Director of IT.

	In the case of break-ins/theft these should be reported to the University Security Office who will liaise with the Police.
Audit and accountability	IT Support Managers and relevant managers in ITCS should audit physical security of systems in their charge 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 Issues Log which is collated by ITCS and submitted to ISSC for review.
Implementation	**IT areas** In open access areas such as student IT areas: • Systems should be secured to the desk to guard against theft. • Systems should be configured to automatically logout after 30 minutes of non-use. • Students should be warned (e.g. by notices) that they should not leave an unattended system logged in. **Staff offices** Key owners/occupants of staff offices are responsible for ensuring overall room security, but should in respect of IT systems in their offices adhere to the following practices: • When absent from the office and no one else is in it, ensure that the office is locked and secure. • When absent from the office, ensure that mobile devices and laptop computers are locked away wherever practical. • Blinds should be drawn on office windows overnight to guard against external viewing of IT equipment. • Confidentiality/privacy should be maintained on systems by automatically locking the system when unattended after 15 minutes. This is particularly important in shared offices where confidential information may be viewed on the screen. • All PCs should be logged out and powered off at the end of the working day. • All sensitive information should be secured from unauthorised accessed at the end of the working day, a clear desk policy should be considered. **Servers and telecommunications equipment** • Servers and telecommunications equipment should be secured in special purpose rooms which are secured against unauthorised access and theft by University approved door access control mechanisms. Such access control mechanisms should record who has been authorised to access the area and who has entered an area at a particular point in time. Procedures should be in place to ensure that when a person ceases employment with the University, or their role changes to one without access rights to the area, their access rights are changed accordingly on the system. • Where it is necessary to locate telecommunications equipment in multiple locations across campus (e.g. network switches), the equipment should be locked away to safe guard against unauthorised access and tampering. Key holders should be recorded and strictly controlled.

	• Server backups should be stored in a fire safe to which access is restricted to authorised individuals and for which records are kept of transferrals to/from the fire safe. Where disaster recovery policies/procedures require so, backups should be housed away from the server area, or off-site.