GISP13. Business continuity and disaster recovery

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	A Disaster Recovery Plan will be in place to protect the University's business processes and information assets from loss or failure of IT or telecommunications services.
Objective	• To ensure that in the case of a failure or disaster affecting University IT services or telecommunications, a plan for service recovery exists. • To ensure that in the case of a major failure or disaster affecting University IT services or telecommunications, a plan for continuing to deliver business processes exists and is aligned to recovery times. • To ensure that University information assets are stored securely and can be recovered in the event of loss.
Policy	13.1. A Disaster Recovery Plan (including system backup and restoration facilities as appropriate) which supports the University's Business Continuity Plan will exist for all IT and computing services and telecommunication systems. 13.2. The Disaster Recovery Plan will be reviewed annually and disaster recovery plans for any new systems will be tested before those systems go live. 13.3. All staff must be made aware of the business continuity plan and their own respective roles. 13.4. Information owners must ensure that appropriate backup and system recovery procedures are in place. 13.5. Management must ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of data files; especially where such files may replace more recent files. 13.6. Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.

	13.7. All users of information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files. The degree to which software techniques and disciplined user procedures are necessary should be applied by management and determined by the classification of the information in question. 13.8. Highly sensitive or critical documents should not rely upon the availability or integrity of (external) data files over which the author may have no control. Key documents and reports should normally be self-contained and contain all the necessary information.
Responsibility	ITCS is responsible for maintaining and reviewing a Disaster Recovery Plan. ITCS is responsible for establishing and running backup regimes which allow for recovery of systems in line with the Disaster Recovery Plan.
Incident Management	In the event of a major catastrophe affecting IT or telecommunication systems, the Disaster Recovery Plan will be consulted and appropriate action taken.
Audit and accountability	Managers of the systems should audit disaster recovery plans 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	**Minimum requirements for safe/secure data storage** • All University owned computer systems should be secure against unauthorised access to data stored on them and compliant with the University's Information Security Policy. • Data should be copied/backed up at least once every 24hrs to a safe and secure location/media away from the desktop. • Exception is data generated temporarily during local processing operations. • The backing up of data from computers should be independent of end-user action and mechanisms should be in place to enable automated synchronisation of stored data with the backup copy. • University owned laptops when connected to campus network should operate under the same policies as for static desktop systems, but the backing up of data from such systems may require end-user action. • All data backups should be secure against fire, theft, flood and unauthorised access, and compliant with the University's Information Security Policy. • Any data utilised, or generated by strategic corporate information systems (e.g. finance and personnel systems) should be stored only on the centrally provided storage associated with those systems.

	• Exception is where centrally provided corporate systems cannot provide all reports required to comply with funding and regulatory bodies, or for University management purposes, it may be necessary to process and store some data on the desktop. This data should be backed up to a secure location/media. • If data is to be shared with other individuals/groups the data should be shared from another secure location such as central filestore or Office 365 so that data access is not compromised due to the desktop system being out of service. All such shared resources should have appropriate security measures in place to prevent unauthorised access to data and comply with the University Information Security Policy. • Anonymous FTP should not be used to share desktop computer data. **Central provision for storage of desktop data** • ITCS will provide safe, secure and backed up central filestore with individual quotas for staff and students to store their work data. This filestore will have no single point of failure and hence will be highly available. • Filestore quota will be "fit for purpose" and sufficient for the storage of work data for the majority of staff and students. • Exception is where a researcher requires large amounts of storage the central filestore quota may be insufficient and additional arrangements as defined will have to be made. • Staff and student quotas will be published on ITCS's web pages. These quotas will be reviewed annually in consultation with Faculties/Schools/Units with the aim of ensuring that quotas keep pace with the demand. However, it should be realised that the quotas offered may be constrained by the level of available funding. • Mechanisms will be provided for individuals, working groups and Schools/Units to purchase or rent additional storage on the central filestore system. These mechanisms will be published on ITCS's web pages. • All desktop data stored on central filestore will be backed up to a secure location on a 24hr basis. Backups will be retained for a guaranteed period. • Where data is required to be kept for a prolonged period of time, the user should consider long-term archive arrangements. • Files will be available from backup for restore to a user's central filestore. Arrangements and procedures for restoring files will be documented on ITCS's web pages. • ITCS will provide mechanisms to allow PC, Mac, UNIX and Linux desktop systems to connect to central filestore in such a manner that the filestore appears as a 'native' drive or folder on that system. • ITCS developed Standard Staff and Student Desktops will provide an automatic connection to the user's central filestore and synchronisation at regular intervals between locally cached data and the central copy, including at logon and logoff.

	• Provision will be made for sharing of centrally stored data between individuals and groups connected to the campus network. Such provision will allow for fine control of access down to the user and file level.