# St George's, University of London

# Data Backup Policy

## 1. Scope

**1.1.** SGUL's backup service is designed and implemented with disaster recovery/business continuity (i.e. the ability to recover recent live data in the event of a partial or total loss of data) as the primary objective. It is not therefore designed as a method of archiving material for extended periods of time, nor as a safety net for users inadvertently deleting data.

**1.2.** "Backups" cover all systems managed by the IT department, however, there are 2 types of backup, targeted at different systems. File Level backups are targeted at physical hardware, and Snapshot backups are targeted at Virtual Machines. Occasionally, where appropriate, a system may utilize both types.

**1.3.** Data held and managed locally in departments and desktop devices is excluded unless departments have entered specific arrangements with IT.

**1.4.** All staff are reminded that they are individually responsible for data held locally on their desktop or laptop computer and all critical data must be stored on the network drives provided or central email services.

## 2. Backup Policy

**2.1.** General

2.1.1. Backups are stored in secure locations. A limited number of authorised personnel have access to the backup application and media copies.

2.1.2. Requests for backup data from 3rd parties must be approved by the SIRO

2.1.3. Direct backup of data held within Database Systems are excluded. Database administrators are expected to export the data to be backed up to the local service file system in line with the timings of the backup for their system.

2.1.4. Virtual Servers (vmware) are backed up by a rolling monthly snapshot of the system to a separate data store. 2 copies are kept for business continuity. This data store is remote from the source.

2.1.5. A daily backup report is produced for each system being backed up. Both physical and virtual.

2.1.6. It is the role of SGUL's systems administrators to review these reports each working day, and deal with any issues.

2.1.7. The backup schedule is available for each system on request via ITAV@sgul.ac.uk

**2.2. Full Backups**

**2.3.** Full backups of all SGUL managed physical servers are performed on a monthly rotation. That is to say that not all full backups are run on a given day; systems are backed up throughout the month.

**2.4.** Full backups are retained for 1 months before being overwritten.

**2.5.** Full backups for some file servers take several days. Where this is the case, incremental backups will be skipped during the full backup process.

**2.6.** Upon completion of a full backup backups, media copies are moved automatically to a secure remote site for disaster recovery purposes.

## 3. Incremental backups

**3.1.** Incremental backups of all SGUL physical servers are performed daily.

**3.2.** Incremental backups are retained for 1 month before being overwritten.

**3.3.** Where possible incremental backups are run overnight and are time to be completed before 8am on working days.

## 4. Backup procedure

4.1. The IT Backup systems have been designed to ensure that routine backup operations require no manual intervention.

4.2. The IT department monitor backup operations and the status for backup jobs is checked each morning during the working week.

4.3. Any failed backups are re-run immediately the next working day.

4.4. Backups can be excluded by users by placing a file called ".nobackup" in the directory to be excluded. This, and any sub directories will be excluded from subsequent backups.

4.5. Nominated systems administrators can use the backup software

## 5. Restore procedure

5.1. Data is available for restore within a few minutes of a backup job completing on the daily Schedule, except when there is a full backup in progress.

5.2. Data will be available during the retention policy of each backup job – which is currently defined as 1 month.

5.3. Recent data is available from this system on completion of the daily backup jobs, which means that there is potential data loss during a working day on some systems. The IT systems at SGUL have been specified to minimise data loss between backup windows by having elements of system redundancy.

5.4. Requests for data recovery should be submitted to ITAV@sgul.ac.uk

5.5. Only nominated systems administrators are permitted to perform a restore.

5.6. The restore of data is only permitted when requested by the data owner, their nominated proxy, or the SIRO.

5.7. Systems administrators must confirm the identify of the requestor, and files required before restoring.

## 6. Policy Review and Maintenance

6.1. The Policy will be reviewed and updated to ensure that the policy remains aligned with changes to relevant laws, contractually obligations and best practice.

6.2. For advice, queries can be emailed to itav@sgul.ac.uk