STU-SOP-IT-003 – Standard Operating Procedure on IT Management

1. Purpose

This Standard Operating Procedure (SOP) describes the procedure of Information Technology (IT) Management used by Swansea Trials Unit (STU).

2. Background

Many IT systems utilised by STU are provided by bodies outside STU such as Swansea University (SU) Information Systems and Services (ISS). In those cases, this SOP shall apply only to the extent applicable within the policies and best practice of those organisations. Details are available in STU IT policy (STU-POL-002)

There is always a risk of disaster or malicious intent beyond that which can be reasonably predicted. Therefore, the emphasis is on taking appropriate precautions that are in proportion with the anticipated risk.

3. Roles and Responsibilities

The **STU IT Officer** (or delegate) shall have responsibility for logical access to systems (where not directly arranged by SU ISS), and for overseeing server management. Also, for maintaining oversight of trial databases and mailboxes and management of clinical trial systems hosted in ISS data centres. Also, for maintaining and updating trials data systems as required.

SU ISS supply the virtual servers on which STU's systems are hosted and manage these within their data centres. Provision of and regular updates to the operating systems of these virtual servers are carried out by SU ISS, as well as routine backups and clones of these servers as part of SU ISS's normal data centre management operations.

The **Trial Manager (TM),** on behalf of a trial **Chief Investigator (CI),** is responsible for determining which users should be given access to their trial on STU trial systems.
Examples of systems which are provided and managed by SU ISS are those which are common to Swansea University, e.g. email, word processing, spreadsheets etc.

Examples of systems: specific to clinical trials and managed by the STU IT Officer include REDCap, Q-Pulse, Randomisation applications, STU-specific SharePoint sites and the STU website.

External use of SOP: this SOP and Associated Documents (AD) may be used for research projects not adopted by STU where Swansea University (SU) staff and associated NHS organisations require guidance. In such instances, oversight responsibility for any associated tasks will not be the responsibility of STU.

4. Procedure

4.1 Logical Access

Logical Access is the set of safeguards put in place to ensure that only authorised users can gain access to information stored on STU-related IT infrastructure and/or services.

The IT Officer will, as and when necessary, extract from any relevant systems an up-to-date list of users for each system or coordinate such work with ISS where the system in question is managed by them.

Where a system doesn't provide a mechanism for contacting users directly, these user lists will provide contact information to inform users in the event of planned system downtime. In the event of unplanned downtime (e.g. a system crash), priority will be given to getting the system back up, and users will be informed once normal functioning has been restored. Notification templates for such scenarios are also shared with the STU team via an internal drive.

4.1.1 Granting access to Systems

STU staff members will have standard computer functionalities such as a university email account arranged by SU ISS.

Access to STU-specific infrastructure/services shall be arranged by the STU IT Officer as detailed below.

Users outside STU will not normally be given access to STU shared drives/folders (an exception is made for audit or inspection purposes). If it is necessary to share data with external users, it should be transferred according to the principles set out in the 2018 Data Protection Act (see references).

Access to other STU systems will be arranged by the STU IT Officer and granted on a 'need to' basis.

For all users, before granting access to STU infrastructure/services, the IT Officer will first ensure it:

- has been requested (using the account form (STU-AD-FRM-024)) by a suitable person, such as the user's line manager or the TM of the relevant study
- is appropriate, and in line with the responsibilities of the person being granted access. They will then carry out any appropriate action to grant access and inform the user and requester of the result. Access privileges shall be minimised in all cases and restricted to those aspects directly relating to the user's needs. Details of all users will be held in a user account list.

4.1.2 Approval for user access

For user access requests relating to specific research projects, approval can be granted by the TM on behalf of the CI.

The TM requests the STU IT Officer to grant access to the systems, specifying the type of access required.

The STU IT Officer enables the required access, setting the roles and privileges for the user in question to meet the request.

For some systems, the TM may be granted administrative rights by the STU IT Officer to allow them to set up the access privileges themselves for specified research projects.

For access to STU systems or shared drives, not directly related to research project activities, approval will be granted by a member of the STU Executive Team.

4.1.3 Revoking user access

To ensure auditability, users cannot be entirely deleted from the data record of any system:

- In cases where a given system retains an audit trail of a user's activities even when their account has been deleted, an account may be removed from that system when a user's access is finally revoked.

- In cases where a given system does not permit removal of an account without violating either data referential integrity or an audit trail, access will be revoked in such a way as to inactivate the account (i.e. to deny login) but retaining the account for data integrity and audit.

The exact mechanism for each approach will depend on the system in question. The minimum action for revoking access will be to disable login for an individual user account.

When a member of staff leaves STU, relevant emails/files not available in the project inbox should be stored in an accessible location to provide business continuity and audit accountability. Care should be taken that this access does not adversely impact on-going work (e.g. potentially unblinding a project).

4.2 Helpdesks from service providers

STU staff will usually report issues with STU IT systems directly to the STU IT Officer who will assist in finding a solution or contacting ISS.

There may be instances when STU staff need to report directly to ISS. The IT officer will advise of such instances and should be copied into relevant communication.

For issues with ISS managed processes/systems, these will be reported through the LanDesk helpdesk service via the SU website or Zendesk application manager.

4.3 Business Continuity & Disaster Recovery

In the event of system(s) or database(s) failure, affected users will be notified as soon as possible and provided with an estimate of when normal service will resume.

For each STU-related IT system either ISS or the STU IT Officer are responsible for function checks:

ISS:

- Normal system functioning is checked daily during the working week, by checking that the application indicates it is functioning normally, and by checking that the servers for that application show no fault indications.
- A regular automated back-up process is in place, running every 6 hours. This is automatically monitored by ISS to ensure it is running, with alerts triggered to the ISS Infrastructure Team if it fails.

- In addition to automated 'traditional' database backups, full virtual machine clones run every 6 hours. This process is automatically monitored to ensure it's running, with alerts triggered to the ISS Infrastructure Team if it fails.
- Complete datacentre failover between their two geographically separate datacentres is carried out regularly by ISS under their disaster recovery plan.
- For management of virtual servers and data centre operation, ISS have teams of multiple individuals with overlapping knowledge and training.
- Catastrophic events will be managed outside office hours as required.

STU IT Officer:

- Checks daily during the working week that the backups and clones ran as expected for the past 24 hours, raising fault cases with ISS If the backup/clone hasn't run (whether they're already taking action, or not). In the event of database/system corruption, these traditional backups and virtual machine clones allow rapid restoration of a logically consistent dataset or complete machines to a point not more than 6 hours old.
- Database restores can be carried out by the STU IT Officer but would in practice be done in conjunction with ISS to ensure the root cause for the corruption is fully understood and corrected before dataset restoration.
- Database 'restore' processes are tested regularly by loading a recent backup from a live system into a test database.
- A system restore depends on the infrastructure provider (i.e. ISS) or the IT Officer to contact the relevant bodies to request a system restore. A list of contacts for all systems will be kept in a log (detailed below) by the IT Officer.
- At least two STU IT users must have administration rights, business continuity training, and access to documentation for every system.
- Catastrophic events will be managed outside office hours as required.

The STU IT Officer's credentials for all STU-related IT systems are stored in a secure digital password management system, with its underlying, encrypted database stored on a restricted area of a drive managed by relevant ISS staff. A hard copy pack, consisting of how to access this digital password safe and the database's master access credentials, is printed out and stored in a safe location agreed with the Operational Lead. This pack shall be used in exceptional circumstances to gain access to the password safe in case of the sudden and unexpected absence of both the STU IT Officer and relevant ISS staff.

4.4 Server Management

The STU IT Officer will maintain documentation including a list detailing which applications are hosted on all STU-related servers and services, and where the corresponding service agreement can be found. They will also be responsible for reviewing IT agreements, ensuring that a suitable back-up/restore policy is in place, and that servers have sufficient capacity.

4.5 Systems Maintenance and Updates

The STU IT Officer will carry out periodic maintenance and updates as required to trials data management systems, for example to keep them up to date as new functionality is offered, and also secure as bugs and security issues are identified and fixed. As part of these systems maintenance and update responsibilities, the STU IT Officer will carry out a functional change analysis of any new system version, to identify functional changes which might impact existing studies. The STU IT Officer will then use the resulting change analysis to carry out testing as required to establish the impact of any functional changes, and train STU staff as required in any functional differences which a new version of any trials data management software will bring.

4.6 Electronic Data Archive

The STU IT Officer will set up and manage an electronic data archive, suitable for preservation of project data for future use after the active trial phase of a project has finished. This archive will be based on a centralised data storage method, providing high protection against data loss, but also data separation between interested parties to preserve data blinding. The IT Officer will not act as STU Archivist, but will facilitate the Archivist's access to the electronic data archive as necessary, and ensure the storage medium and access control facilities fulfil all projects' data security and data separation requirements.

5. References

- Swansea University IT Services: http://www.swansea.ac.uk/itservices/
- Data Protection Act (2018): Data Protection Act 2018 (legislation.gov.uk)
- Computerised Systems Validation In Clinical Research, A Practical Guide, 2nd Edition, CR-CSV Working Party, 2004
- Requirements for Certification of ECRIN Data Centres, Version 3.1, European Clinical Research Infrastructure Network, January 2016 http://www.ecrin.org/activities/datacentre-certification

It is assumed that by referencing the principal regulations that all subsequent amendments are included in this citation.

6. Associated Documents

Number	Title	Location
STU-AD-FRM-024	STU System Account Form	Q-Pulse

7. Abbreviations

List of Abbreviations	
BCP	Business Continuity Plan
ISS	Information Systems and Services
IT	Information Technology
SOP	Standard Operating Procedure
STU	Swansea Trials Unit
SU	Swansea University

8. Appendices

Appendix 1: Document History

Version No:	5	Effective Date:	20-Jun-2024
Description of changes:	Content reviewed and updated		