STU-SOP-IT-001 – Standard Operating Procedure on Validation of Computerised Systems

1. Purpose and Definitions

This Standard Operating Procedure (SOP) describes the procedure of validating STU-specific computerised systems.

Definitions	
Computerised systems	Software that accumulates data in an electronic format and involves creating, modifying, maintaining, archiving retrieving or transmitting that data.

2. Background

System validation is the documented process of testing a computerised system to ensure it is suitable for use, functions as intended in a consistent and reproducible manner, and is usable by a typical end-user. All such systems, be they commercial/off-the-shelf systems, bespoke/in-house systems or otherwise, should be appropriately validated before use.

Validation is an ongoing process; a system that is deemed suitable at one point in time may not remain so due to a changing user base, evolving requirements, or alternative systems becoming available. All validation must be subject to review.

A documented validation review process provides assurance that the system remains fit for purpose and meets the requirements of Good Clinical Practice (GCP).

3. Roles and Responsibilities

The **STU IT Manager** has responsibility for system validation. This includes coordinating and ensuring validation for specific systems, liaison with IT service providers, keeping a validation log, identifying validators (one of whom may be the IT Manager), and approving the validation plan.

Validators share responsibility with the IT Manager for devising and implementing the Validation Plan. They must be appropriately qualified by education, training, or experience to do this for the system undergoing validation.

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 Identify Validators

It is desirable that more than one validator should be identified for the system undergoing validation.

4.2 Write Validation Plan

The Validation Plan Template (STU-AD-TMP-031) should be adapted as necessary for the system undergoing validation. The sections listed below are for guidance only.

All validators should agree the plan, which should be proportionate to the current status of the system requiring validation.

4.2.1 Estimate the Risk associated with system failure

This will include both the likelihood and impact of any potential failure. Systems with a high risk may need a more comprehensive validation plan, or multiple rounds of validation, while low risk systems may only justify a more cursory validation.

4.2.2 Determine System Requirements

This will include identifying the purpose of the system and the requirements for its correct operation.

4.2.3 Installation Qualification

This will include confirmation that the system (including any dependencies) has been set up correctly and must be carried out by someone with appropriate permissions. Vendor assessment may be required for externally hosted systems.

4.2.4 Operational Qualification

This will include confirmation that the system operates as expected and is usable by typical end-users. If there are several user groups with different responsibilities /access levels, all such groups should be considered individually.

4.2.5 Performance Qualification

If the anticipated load is predicted to be high, a stress-test (including review of current configuration, including number of licences held) should be carried out.

4.2.6 Catastrophic Failure & Recovery

Recovery of the system after various failure modes should be considered. These will include at least failure or corruption of the database, partial failure of infrastructure at the facility where the system is hosted, and catastrophic failure of the hosting facility. Plans for coping with these scenarios should be assessed, and tests carried out to check that these plans work as expected. It may be impractical to test some of the anticipated failure modes directly (e.g. you can’t realistically bring down a datacentre just to test one system’s recovery plan), but validation should include a test of these plans at some stage of the system’s lifecycle. For example, a test of hot standby failover of an entire datacentre would normally be tested at some stage as part of that datacentre’s operational management, which would then be considered a valid test for this system’s validation once it has been carried out.

4.3 Validate the system

The validation plan will be implemented, and associated documentation completed. When completed, a signed and dated copy of the system validation plan, including any findings and the final recommendation of the system’s suitability for use should be stored with the System Validation Log (STU-AD-TMP-032) maintained by the STU IT Manager.

4.4 On-going system review

The extent and frequency of review will vary from system to system. The introduction of an updated version of a system may merit a review even where one is not otherwise planned.

There will be a formal process to manage any changes that arise in the system to provide a complete system history.

4.5 Decommissioning the system

A decommissioning plan will be implemented and associated documentation completed.

The plan will include details to ensure that archived databased can be accessed if required.

5. References

- 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/data-centre-certification
- UKCRC Guidance for CTUs http://www.ukcrc-ctu.org.uk/page/Guidance

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-TMP-031	Validation Plan Template	Q-Pulse
STU-AD-TMP-032	System Validation Log	Q-Pulse

7. Abbreviations

List of Abbreviations	
GCP	Good Clinical Practice
IT	Information Technology
SOP	Standard Operating Procedure
STU	Swansea Trials Unit
GCP	Good Clinical Practice
IT	Information Technology
SOP	Standard Operating Procedure
STU	Swansea Trials Unit

8. Appendices

Appendix 1: Document History

Version No:	4	**Effective Date:**	22-Apr-2024
Description of changes:	Updated onto SOP Template v5		