Labstep

Labstep for GLP Compliance

This document summarizes how the Labstep platform enables compliance with the requirements of the OECD Series on Principles of Good Laboratory Practice (GLP) and Compliance Monitoring. As a quality assurance system, the GLP Principles have been introduced by the Organisation for Economic Co-operation and Development (OECD) with the intention to promote data quality and guarantee data integrity. Apart from other guidelines regarding quality research, the GLP Principles can be found in the member countries of the OECD (except the USA and Japan) for non-clinical, chemical and agrochemical research testing studies.

In particular, the GLP principles intend to provide a secure research environment that protects raw data from manipulation during and after testing procedures and incorporates all organizational structures of research procedures. Therefore GLP not only regulates the personnel working in a laboratory or other research facility, but also applies to computerized systems and their device-specific requirements used for research purposes.

As a result, computerized systems like Labstep have to provide validated services to ensure accuracy, reliability and consistent intended performance, including the ability to ensure data quality and integrity, protecting stored records against manipulation or loss.

This document summarizes the Labstep implementation to meet the technical requirements of the OECD Series on Principles of Good Laboratory Practice (GLP) and Compliance Monitoring regulations which are relevant to electronic systems like Labstep. In addition to the selected GLP Principles, there are several sections of the GLP regulations that do not apply (test sites and physical archives only) to the system and services provided by Labstep.

This document does not give detailed information on GLP, nor does it provide legal advice for full compliance. The full text of GLP can be found on the OECD website at: **http://www.oecd.org/env/ehs/testing/oecdseriesonprinciplesofgoodlaboratorypracticeglpandcompliancemonitoring.htm**

Overview of Labstep's Compliance with the GLP Principles

Labstep is a research management platform, used for the electronic analysis and management of research data across scientific disciplines. For a computerized system with

integrated archive facilities like Labstep, the provision of services that are compliant with the GLP Principles is of utmost importance.

The Labstep system has considered the GLP Principles during its development phase and continues to incorporate the regulations within its system life cycle to ensure continuous quality, integrity and security of research data stored in the electronic archive facilities. **Since the compliant adherence to GLP is not exclusively based on the software system itself but also depends on procedural controls (such as SOPs, well trained personnel, physical conditions of research facilities) within a laboratory or other research organizations using electronic management systems for research purposes, a software system cannot be certified to be compliant (and any software vendor claiming GLP-compliance is incorrect!).**

However, software vendors can offer a system which meets the technical requirements for computerized systems and the management of electronic records set by the OECD in a compliant set-up.

The following section below gives a brief summary on how the Labstep system complies with selected GLP Principles that are relevant for software systems used in laboratories or other research institutions. The Labstep system provides a secure, GLP-compliant environment for research data by employing the following features:

Security

Labstep incorporates state of the art enterprise security - both logical and physical - to protect research data, including:

- Access control: Password complexity requirements
- Back-up power: Daily back-ups of records
- High-security data center: Offsite back-ups on redundant servers in SOC-compliant data centers.
- End-to-end encryption: Storage encryption, encrypted communication and encryption during uploads and downloads
- System check-ups: System scanning and monitoring routines
- IT updates: Regular security and functionality updates
- Business infrastructure: Validation plan and continuity and disaster recovery procedures
- Physical protection programme: Secure data centre with regular stress testing of the infrastructure, climate protection procedures (e.g fire. water or other natural disasters), the provision of redundancies and emergency management

Confidentiality

The Labstep system employs procedures that keep all stored records protected from disclosure to unauthorized parties, including:

- Admission control: Limited access to data only for account owner and authorised persons
- Data encryption: Encryption for identifiable data during uploads/downloads, transfer and storage
- Secure storage: Separate security locations on redundant servers with various security procedures in place (both physical and logical)
- Safe disposal: of data and media
- Confidentiality agreement: Records Management Section for staff working with sensitive research data, well trained personnel and internal security training

Authenticity

Labstep guarantees the reliability of data transfers and the information exchange within research networks through:

- Multi-level authentication processes: Login/password combination and access rights management
- Secure user identification: Identification needed to access and to manage data
- Electronic signatures: Sign and witness functions for digital data
- Migration plan: Secure data transfer with encrypted coding

Integrity

Labstep provides comprehensive protection of research data from unauthorised access and changes through:

- Access control: Restricted management rights to ensure data quality in a regulated environment
- Authority checks: Limited access to authorized individuals only
- Full audit trail: All activities within the system will be recorded
- Version control. Recording and monitoring of all activities, including IT related processes
- Logged data: Uploads and downloads are logged and “hashed” to verify data integrity
- Timestamps: Records and changes are provided with a system-created timestamp, recording person, date and time
- Electronic signatures: Option to sign and witness electronic documents
- Secure data transfer: Migration plan with encrypted coding
- Data retention: Long term retention of electronic records. No records can ever be hard-deleted on the platform and are always retrievable even when deleted by the account owner.
- Data availability: Stored records are available for collection, inspection and review by the agency/reviewing body
- Data deletion: Deletion of records can be controlled and prohibited by organizational policy through roles and permissions.
- Standard Operating Procedures: SOPs to ensure optimal system performance and uninterrupted services, including validation, operation and maintenance