5.10 Control of Data and Information Management

5.10.1 General Policy

The **..... NAME OF LAB.....** ensures that all data and information—whether recorded on paper or in electronic format—are managed to guarantee integrity, confidentiality, and ready accessibility to authorized users. The Laboratory Director assumes ultimate responsibility for the management of these systems. Documentation for the operation and maintenance of all information systems is readily available to all authorized staff.

5.10.2 Management of Physical (Paper-Based) Data

- **Recording & Integrity:** Data shall be recorded legibly in permanent ink. All original observations must be retained to allow for the reconstruction of the examination process.
- **Corrections:** Any alterations to manual records must be made by crossing out the original entry with a single line (ensuring the original remains readable), signing, and dating the change.
- **Storage:** Physical records are stored in a secure, controlled environment to prevent damage from moisture, fire, or unauthorized access.

5.10.3 Control of Electronic Data (Non-LIMS/Standalone PCs)

- **Access Control:** All computers are password-protected with unique user accounts.
- **Data Integrity:** Master templates for reports and worksheets are "Read-Only" to prevent unauthorized changes to formulas.
- **Backup Protocol:** Regular backups of electronic data are performed on encrypted external media or secure server space.

5.10.4 Laboratory Information Management System (LIMS)

For laboratories utilizing a dedicated, centralized software system, the following controls apply:

- **7.6.4.1 System Validation and Verification:** Before routine use, the LIMS shall be validated by the supplier and verified by the laboratory to ensure it meets the specific requirements of the microbiology workflow (e.g., handling of culture results, antibiotic sensitivity patterns). Any changes to the software must be authorized, documented, and verified before implementation.

- **7.6.4.2 User Access and Permissions:** A formal hierarchy of access is maintained. Permissions to "Enter," "Modify," "Authorize," or "Delete" data are strictly assigned based on staff competency and job role. Generic or shared accounts are prohibited.
- **7.6.4.3 Audit Trail Management:** The system is configured to automatically maintain a permanent audit trail. This includes the original value, the modified value, the identity of the person making the change, and the date/time stamp.
- **7.6.4.4 Cybersecurity and Data Protection:** The LIMS is protected against malware and unauthorized external access via firewalls and updated antivirus software. Data transmitted electronically (e.g., to ward terminals or via email) is encrypted to maintain patient confidentiality.
- **7.6.4.5 Automated Data Processing:** Interfaces between laboratory instruments (e.g., Blood Culture systems, VITEK) and the LIMS are verified daily for error-free transfer of results. The system is programmed to flag critical results for immediate notification.

5.10.5 Verification of Data Transfers and Calculations

The laboratory periodically verifies that:

- Data transfers between different systems (e.g., from a manual worksheet to a computer or from an instrument to a report) occur without corruption.
- Calculations, such as unit conversions or measurement uncertainty, are verified by a second staff member or a validated software process.

5.10.6 Information Security and Confidentiality

- Digital firewalls and physical locks prevent unauthorized access.
- Procedures prevent unauthorized disclosure (e.g., automatic screen locks).
- Off-site or cloud-based information providers must provide evidence of compliance with international data security standards (e.g., ISO 27001).

5.10.7 Contingency and Disaster Recovery

The laboratory maintains a documented **Disaster Recovery Plan** to ensure continuity of service during system failures (e.g., power outages or cyber incidents). This includes:

- A manual backup system for sample tracking and reporting.
- Defined procedures for data restoration and "catch-up" data entry once the system is restored.
- Verification of data integrity following any system restoration.

Reference Documents:

- **QSP for Information Management** (..... NAME OF LAB...../QSP/5.10/IM)
- **LIMS User Access Matrix** (..... NAME OF LAB...../SD/09)
- **Disaster Recovery & Contingency Plan** (..... NAME OF LAB...../SD/08)
- **Verification Records for Data Transfer** (..... NAME OF LAB...../REC/5.10/VAL)