DATA INTEGRITY POLICY

Document ID:	SOP-DI-001
Revision:	1.0
Effective Date:	*[DD.MM.YYYY]*
Review Date:	*[DD.MM.YYYY + max. 2 Years; frequency should be risk-based per ICH Q10]*
Owner:	Quality Assurance
Approved by:	*[Name], Head of Quality*

Revision History

Rev	Date	Author	Description
1.0	*[DD.MM.YYYY]*	*[Name]*	Initial Release

1. Purpose and Scope

1.1 Purpose

This Standard Operating Procedure establishes the requirements and controls for ensuring data integrity throughout the organization. It defines the principles, responsibilities, and processes to maintain the integrity of GxP-relevant data in compliance with regulatory requirements.

1.2 Scope

This SOP applies to:

- All GxP-relevant data generated, processed, reported, stored, or archived
- All computerized systems used to create, modify, store, or transmit GxP data
- All paper-based and hybrid documentation systems
- All personnel who create, process, review, or approve GxP data
- Contract laboratories, contract manufacturers, and other service providers handling GxP data

1.3 Regulatory References

- FDA 21 CFR Part 11 - Electronic Records; Electronic Signatures
- EU GMP Annex 11 - Computerised Systems
- PIC/S PI 041-1 (2021) - Good Practices for Data Management and Integrity
- WHO TRS 1033 Annex 4 - Guideline on Data Integrity
- ICH Q10 - Pharmaceutical Quality System
- GAMP 5 - Good Automated Manufacturing Practice

2. Definitions

Term	Definition
ALCOA+	Attributable, Legible, Contemporaneous, Original, Accurate + Complete, Consistent, Enduring, Available
Audit Trail	A secure, computer-generated, time-stamped electronic record that allows reconstruction of the course of events relating to creation, modification, or deletion of an electronic record.
Data Integrity	The degree to which data is complete, consistent, accurate, trustworthy, and reliable throughout its lifecycle.
Electronic Record	Any combination of text, graphics, data, audio, or other information represented in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.
Metadata	Data that describe the attributes of other data, providing context and meaning (e.g., audit trails, date/time stamps, operator ID).
Raw Data	Original records and documentation, retained in the format in which they were originally generated.
True Copy	A copy of original data that has been verified and certified to have the same information as the original.

3. Roles and Responsibilities

3.1 Senior Management

- Establish and maintain a quality culture that supports data integrity
- Provide adequate resources for data integrity controls
- Ensure appropriate escalation of data integrity issues

3.2 Data Integrity Officer / Coordinator

- Oversee implementation of this policy across all departments
- Conduct periodic data integrity risk assessments
- Coordinate data integrity training programs
- Track and trend data integrity metrics
- Report data integrity status to Senior Management

3.3 Quality Assurance

- Review and approve this policy and related procedures
- Conduct periodic audit trail reviews
- Investigate data integrity deviations
- Ensure data integrity requirements are included in supplier qualification

3.4 System Owners

- Ensure systems under their control comply with data integrity requirements
- Maintain system validation status
- Manage user access and periodic access reviews
- Ensure audit trails are enabled, protected, and regularly reviewed

3.5 All Employees

- Follow Good Documentation Practices (GDP)
- Report data integrity concerns immediately
- Protect login credentials - never share passwords
- Complete required data integrity training

4. Data Integrity Principles (ALCOA+)

All GxP data must comply with the ALCOA+ principles throughout its entire lifecycle:

Principle	Requirement
Attributable	Data must identify WHO performed an action and WHEN. Use individual user accounts - generic logins are prohibited.
Legible	Data must be readable, permanent, and retrievable throughout its retention period.
Contemporaneous	Data must be recorded at the time the activity is performed. Backdating is prohibited.
Original	The original record or a certified true copy must be retained.
Accurate	Data must be free from errors, complete, and reflect the actual observation or activity.

+Complete	ALL data must be present, including failed tests, repeat analyses, and deleted records.
+Consistent	Data must use consistent formats, timestamps, and sequences with no unexplained gaps.
+Enduring	Data must be protected and maintained for the required retention period.
+Available	Data must be accessible and retrievable when needed, including during inspections.

5. Requirements for Electronic Systems

5.1 Audit Trail Requirements

- Audit trails SHALL be enabled for all GxP-critical systems
- Audit trails SHALL be protected from modification or deletion
- Audit trails SHALL capture: User ID, date/time, old value, new value, reason for change
- Audit trails SHALL be reviewed as part of batch release and periodically
- Disabling of audit trails requires documented justification and QA approval

5.2 Access Control

- Each user SHALL have a unique user ID - shared/generic accounts are PROHIBITED
- Passwords SHALL meet complexity requirements and be changed periodically
- User access SHALL be based on job function (principle of least privilege)
- Access rights SHALL be reviewed at least annually
- Failed login attempts SHALL be logged and monitored
- User accounts SHALL be deactivated promptly upon termination or role change

5.3 System Validation

- All GxP computerized systems SHALL be validated according to GAMP 5 principles
- Validation documentation SHALL include data integrity considerations
- System changes SHALL follow change control procedures
- Periodic review SHALL confirm continued validated state

5.4 Backup and Recovery

- Regular backups SHALL be performed and documented
- Backup restoration SHALL be tested periodically
- Disaster recovery procedures SHALL be documented and tested
- Backup media SHALL be stored securely, preferably off-site

5.5 Spreadsheet Controls

- GxP-critical spreadsheets SHALL be validated
- Formulas and calculations SHALL be protected from modification
- Version control SHALL be maintained
- Access controls SHALL prevent unauthorized changes
- Use of personal copies on local drives is PROHIBITED for GxP data

6. Requirements for Paper-Based Systems

- Entries SHALL be made in permanent, indelible ink (blue or black)
- Corrections SHALL use single line strikethrough with initials, date, and reason
- White-out, erasure, or overwriting is PROHIBITED
- Blank spaces SHALL be lined through to prevent later entries
- Pages SHALL be numbered and bound where possible
- Blank forms SHALL be controlled and accounted for
- Original records SHALL be stored securely with controlled access

7. Hybrid Systems

When both electronic and paper records exist for the same activity:

- The relationship between paper and electronic records SHALL be clearly defined
- The designated original record SHALL be identified
- True copy requirements SHALL be documented
- Data flow between systems SHALL be validated
- Controls SHALL prevent duplicate or conflicting data

8. Periodic Review and Self-Inspection

8.1 Data Integrity Assessment

- A comprehensive data integrity assessment SHALL be performed at least annually. The frequency should be determined based on risk assessment considering system criticality, previous findings, and regulatory requirements (per ICH Q10 Section 4.1)
- Assessment SHALL cover all GxP-relevant systems using ALCOA+ criteria
- Findings SHALL be documented and addressed through CAPA
- Results SHALL be reported to Senior Management

8.2 Audit Trail Review

- Audit trails SHALL be reviewed as part of batch release
- Periodic audit trail reviews SHALL be performed monthly or quarterly
- For-cause reviews SHALL be performed when anomalies are suspected
- Review findings SHALL be documented

9. Training Requirements

- All personnel handling GxP data SHALL receive initial data integrity training
- Training SHALL cover ALCOA+ principles and this policy
- Role-specific training SHALL be provided for system users and administrators
- Refresher training SHALL be conducted annually
- Training records SHALL be maintained

10. Handling of Data Integrity Findings

10.1 Classification

Level	Description	Action Required
Critical	Intentional falsification, fraud, or systematic data manipulation	Immediate escalation to Senior Management; potential regulatory notification; formal investigation
Major	Significant gaps in controls; unintentional but widespread issues	Investigation within 5 days; CAPA required; Management notification
Minor	Isolated incidents with limited impact; documentation errors	Document and address; include in trending; CAPA if recurring

10.2 Investigation

- All data integrity findings SHALL be investigated

- Root cause analysis SHALL be performed
- Impact assessment SHALL evaluate affected batches and data
- CAPA SHALL address both immediate correction and systemic prevention

10.3 Escalation

- Critical findings SHALL be escalated immediately to Senior Management
- Regulatory notification SHALL be evaluated for significant findings
- Confidential reporting mechanisms SHALL be available for employees

---

Compliant with FDA 21 CFR Part 11, EU GMP Annex 11, PIC/S PI 041-1, and WHO TRS 1033