GRRMDP

Global Regulatory requirements for Good Manufacturing and Distribution practices in Pharmaceutical /Biopharma industries

1 PROCEDURE:

1.1 EXPECTATION AND REQUIREMENTS TO PREVENT DATA INTEGRITY

1.1.1 Data may be generated by

- Recording on paper, a paper-based record of a manual observation or of an activity
- Electronically, using equipment that range from simple machines through to complex highly configurable computerized systems.
- By using a hybrid system where both paper-based and electronic records constitute the original record.
- By other means such as photography, imagery, chromatography plates, etc.

1.1.2 Data Must Be

- A - Attributable to the person generating the data
- L – Legible and permanent
- C – Contemporaneous- Activities be documented at the time of performance
- Original (or 'true copy') (un-tampered)
- A – Accurate

Data governance measures should also ensure that data is complete, consistent, enduring and available throughout the lifecycle, where;

- Complete – the data must be whole; a complete set
- Consistent - the data must be self-consistent
- Enduring – durable; lasting throughout the data lifecycle
- Available – readily available for review or inspection purposes

1.1.3 Person shall not engage in any unethical practices with respect to data integrity, and will report the supervisor about inappropriate behavior and violations if any are observed or suspected.

1.1.4 Accessibility of records at locations where activities take place so that informal data recording and later

	transcription to official records does not occur.
1.1.5	Reconciliation of controlled print-outs.
1.1.6	Sufficient training in data integrity principles shall be provided to all appropriate staff (including senior management) and Counsel fellow employees when it appears that they are intending of violating the practices.
1.1.7	All personnel shall participate in ethics and data integrity training at the time of joining and then after periodically. This training shall cover organizational mission, how and when to report data integrity issues, record keeping practices and data integrity procedure documentation.
1.1.8	Inclusion of subject matter experts in the data integrity risk assessment process.
1.1.9	Remain attentive and sensitive to situations that could result in actions that are improper, unethical, or otherwise in violation of the data recording practices.
1.1.10	Conduct all data recording practises with integrity and in an ethical manner; will be responsible and accountable for the integrity and validity of the own work.
1.1.11	Data transfer should be validated. The data should not be altered during or after it is transferred to the worksheet or other application. There should be an audit trail for this process. Appropriate Quality procedures should be followed if the data transfer during the operation has not occurred correctly. Any changes in the validated software should be managed through appropriate Quality Management Systems.
1.1.12	Electronic worksheets used in automation like paper documentation should be version controlled and any changes in the worksheet should be documented/ verified appropriately.
1.1.13	There should be adequate traceability of any user-defined parameters used within data processing activities to the raw data, including attribution to who performed the activity.
1.1.14	Audit trails and retained records should allow

reconstruction of all data processing activities regardless of whether the output of that processing is subsequently reported or otherwise used for regulatory or business purposes.

1.1.15 If data processing has been repeated with progressive modification of processing parameters this should be visible to ensure that the processing parameters are not being manipulated to achieve a more desirable result.

1.1.16 Shall be honest about the mistakes made *(Covering up the mistake may take it from mistake to fraud)*

1.1.17 The Expectation / guidance (where relevant) standard format is provided in **Annexure I.**

1.2 DEFINITION:

1.2.1 **Data**: Information which is derived or obtained from raw data. (eg. A reported analytical result)

1.2.2 **Data Integrity:** The extent to which all data are complete, consistent and accurate throughout the data lifecycle. Data integrity is the assurance that data records are accurate, complete, intact and maintained within their original context, including their relationship to other data records.

1.2.3 **Data Governance:** The sum total of arrangements to ensure that data, irrespective of the format in which it is generated, is recorded, processed, retained and used to ensure a complete, consistent and accurate record throughout the data lifecycle.

1.2.4 **Data Life Cycle:** All phases in the life of the data (including raw data) from initial generation and recording through processing (including transformation or migration), use, data retention, archive / retrieval and destruction**.**

1.2.5 **Raw Data:** Original records and documentation, retained in the format in which they were originally generated (i.e. paper or electronic), Raw data must be contemporaneously and accurately recorded by permanent means. In the case of basic electronic equipment which does not store electronic data, or provides only a printed data output (e.g. balance or

pH meter), the printout constitutes the raw data**.**

1.2.6 **Original Record:** Data as the file or format in which it was originally generated, preserving the integrity (accuracy, completeness, content and meaning) of the record, e.g. original paper record of manual observation, or electronic raw data file from a computerized system.

1.2.7 **True Copy:** An exact copy of an original record, which may be retained in the same or different format in which it was originally generated, e.g. a paper copy of a paper record, an electronic scan of a paper record, or a paper record of electronically generated data.

1.2.8 **Attributable:** Data record linked to name of person or the source from where data was acquired, who performed any action on or with the data.

1.2.9 **Legible:** Paper based data should be in handwriting that is readable.

1.2.10 **Contemporaneous:** Data should be recorded at the time of data capture or when work is performed and date/time should follow in order.

1.2.11 **Original:** Data should be recorded on the original sheet or the database/table. Also signifies the importance of maintaining raw data and metadata.

1.2.12 **Accurate:** The data contains correct value. Accurate data not only adheres to integrity constraints and measurement rules but is data that reflect actuality.

1.2.13 **Paper Generated Data**: Data generated manually on paper may require independent verification if deemed necessary from the data integrity risk assessment or by another requirement. Consideration should be given to risk-reducing supervisory measures.

1.2.14 **Electronic Generated Data:** The inherent risks to data integrity relating to equipment and computerized systems may differ depending upon the degree to which the system generating or using the data can be configured, and the potential for manipulation of data during transfer between computerized systems during the data lifecycle.

1.2.15 **Audit trail:** Audit trail means a secure, computer-generated, time stamped electronic record that allows for reconstruction of the course of events relating to the creation, modification or deletion of an electronic record. An audit trail is a chronology of the 'who, what, when and why' of a record.

1.3 PREAMBLE:

1.3.1 Data integrity is a prerequisite for the regulated healthcare industry as decisions on product quality, safety and efficacy & compliance with the applicable regulatory requirements are made based on data and Data Integrity Policy provided in **Annexure II.**

1.3.2 Data integrity is a part of quality system and every employee has a duty to perform their GxP functions in an ethical manner that meet company requirements and industry standards as articulated in the company requirements, ad in accordance with all relevant laws, regulations and legislative directives of regulatory authorities.

1.3.3 Data integrity requirements apply equally to manual (paper) and electronic data.

1.3.4 Data generated, used to make manufacturing and quality decisions shall be trustworthy and reliable. For example: all weights, Analytical report numbers (A.R. number), time and temperature factors which are treated as important or critical in manufacturing activities are double checked during documentation.

1.3.5 All pH, weights are recorded as a printed matter for reference in respective protocol. Employees must sign or initial on original records with date and time in a contemporaneous manner

1.3.6 Breaches in data integrity can have negative consequences and may lead to patient injury, or even death.

1.3.7 The inability to detect and prevent breaches in integrity of data warrants serious concerns about the reliability and effectiveness of the quality system.

1.3.8 The integrity of the data generated by any means is a prime factor in determining the credibility between

Regulatory and Management.

1.3.9 All SOPs are followed exactly as per the procedure designed. If any employee finds any difficulty in this regard should bring it to notice of seniors. Established quality systems and procedures should be followed thoroughly to minimize the potential risk to data integrity. The integrity of the data generated by any means is a prime factor in determining the credibility between Regulatory and Management.

1.3.10 Data Reliability Policy is provided as **Annexure III**

1.4 INTRODUCTION TO DATA INTEGRITY:

1.4.1 The term 'Data' denotes the information which is derived or obtained from raw data. (e g. A reported analytical result).

1.4.2 Data are factual information used as a basis for reasoning, discussion or calculation.

1.4.3 Examples

- Hand written entries on log books / records /registers/ laboratory note books, etc.
- Recording of critical process parameters in Batch manufacturing record.
- Worksheets
- Electronic files (Word Documents and E-Mails)
- Printed reports
- Any other form of information used for later reference

1.5 DATA INTEGRITY

1.5.1 Data integrity is the assurance that data records are accurate, complete, intact and maintained within their original context, including their relationship to other data records.

1.5.2 Each and every information should get recorded in issued formats like batch manufacturing record, dispensing sheets, protocols etc.

1.5.3 Ensuring of data integrity shall include protecting original data from accidental or intentional modification, falsification or even deletion.

1.5.4 All data's generated shall be documented and maintained in an appropriate manner.

1.5.6 Approved procedures should be followed to document the results of each activities and to maintain the integrity of the record throughout the retention period of the document. (Refer SOP for documentation control (_____) and SOP for data backup (_____)

1.5.7 Data integrity refers to maintaining and assuring the accuracy and consistency of the data throughout the life cycle of document.

1.5.8 Records /Data generated should be accurate, truthful / authentic and complete.

1.6 REGULATORY AGENCIES EXPECTATIONS OVER DATA INTEGRITY:

1.6.1 Information / data derived or obtained from the raw data shall be **ALCOA Plus:**

Some key concepts of GdocPs are summarized by the acronym ALCOA: Attributable, Legible, Contemporaneous, Original and Accurate. The following attributes can be added to the table: Complete, Consistent, Enduring and Available (ALCOA+). Together, these expectations ensure that events are properly documented and the data can be used to support informed decisions. Data Integrity Checklist **Annexure IV**

1.6.2 Data are intended to ensure that products meet pre-established specifications, such as yield, purity, potency, efficacy and stability of its intended purpose.

1.6.3 **The regulatory requirements for data integrity**

Requirements with respect to data integrity include:

- "Backup data are exact and complete", and "secure from alteration, inadvertent erasures, or loss"
- Data be "stored to prevent deterioration or loss"
- Certain activities be "documented at the time of performance" and that laboratory controls be "scientifically sound"
- records be retained as "original records", "true copies", or other "accurate reproductions of the original records"

- "Complete information", "complete data derived from all tests", "complete record of all data", and "complete records of all t performed"

1.6.4 Maintaining data integrity is a critical aspect of pharmaceutical operations. With strict regulations and the need for accurate and reliable data, having a standardized operating procedure (SOP) is essential.
SOP should be designed to:

- Establish clear guidelines and protocols for data integrity
- Ensure compliance with regulatory requirements
- Streamline data management processes to minimize errors and inconsistencies

1.6.5 **Benefits of Data Integrity SOP**
Data integrity is crucial to maintain the highest standards of quality and ensure compliance.
Some of the benefits include:

- Ensuring accurate and reliable data throughout the entire pharmaceutical manufacturing process
- Mitigating the risk of data manipulation or unauthorized changes
- Facilitating compliance with regulatory requirements, such as FDA guidelines
- Enhancing transparency and traceability of data for audits and inspections

Promoting a culture of data integrity and accountability within the organization

1.6.6 **Best Practices for Achieving Data Integrity**
Impart Training, create awareness
Personnel in every process on the manufacturing floor must be trained in proper data management. The training must go beyond good document practices. It should cover why the process are conducted the way they are. To enhance the training, include:

- Consequences of poor handling for any given process
- How the smallest of mistakes evolve into serious problems
- Why validations are important
- Why protocols should be followed

1.6.7 **Set Controls on Human errors Procedures, and technology**

- Have SOPs that are well-defined, clear, and simple. Train staff adequately on them.
- Keep audit trials in order to clearly show who accesses a given system, which login credentials were used and the date and time it was accessed. This will help investigate issues and address root cause.
- Regularly review audit trials
- Keep records of audits at handy to show investigators that reviews are being conducted routinely by trained professionals
- Ensure your SOPS offer a process for escalating issues to management should they be discovered
- Simplify SOPs, train staff on all directives, and monitor the effectiveness of these efforts

1.6.8 **Set Procedural controls**

Embed procedural and administrative controls in your core business activity. It should consist of a suit of documents that include written directives, training programs, record and review management, audits and self-inspections of governing processes.

1.6.9 **Set Technical controls**

Set controls to protect information systems such as passwords, access controls for operating systems or application software programs, network protocols, firewalls and intrusion detection systems, encryption technology, network traffic flow regulators, etc.

- Set appropriate technical controls into products for all three stages namely a) data at rest b) data in motion c) data in use.
- Create a culture of integrity
- Recognize the contributions of employees and encourage them to be critical, and divergent thinkers.

1.6.10 **Set Document controls**

Data must not be recorded in unofficial forms, writing pads, and uncontrolled media. This policy must be stated in the SOPs for good documentation practices.

- Lab notebooks, worksheets should be issued by the quality unit.
- System user accounts especially those with data alteration abilities should not be shared
- Limit duplication risks such as duplicate

copies of paper records, multiple copies of databases/spreadsheets and so on by maintaining a centralized library

- Audit electronic systems, ensure verifying controls are in place and functioning
- Ensure that archiving processes maintain and protect data loss
- Backup electronic data regularly, maintain as per procedural GMP requirements.
- Draw a single line through the erroneous entry. Record correct entry, initial and date providing reason for the correction. Justify and document any data discarding.
- Perform data entry accurately, truthfully and completely
- Store data, documents and backups securely during their retention periods. Limit access and use fireproof storage as necessary

1.7 DATA INTEGRITY REQUIREMENTS

1.7.1 All raw data should be legible and accessible throughout the data life cycle. Ensure that printed matter is clearly legible and second or third copy of documents is clearly readable.

1.7.2 Data governance should address data ownership throughout the lifecycle, and consider the design, operation and monitoring of processes / systems in order to comply with the principles of data integrity including control over intentional and unintentional changes to information. While preparing any master documents like protocol or batch manufacturing record, the preparer should make provision for all required information so as not to loose any information or data for future reference. (SOP for preparation of specification, method of analysis and protocol (_____))

1.8 Breaches to Data Integrity (but not limited to) / Unethical conduct and data integrity issue

1.8.1 **Breaches to Data Integrity (but not limited to)**

1.8.1.1 Falsification of data**.**

1.8.1.2 Alteration of data and events.

1.8.1.3 Misleading information, statements or facts.

1.8.1.4 Misrepresentation of what really happened.
1.8.1.5 Untruthful statements.
1.8.1.6 Forgery.
1.8.1.7 Questionable information, statements, events or facts.
1.8.1.8 Misreporting or selective reporting information.
1.8.1.9 Not recording activities contemporaneously.
1.8.1.10 Backdating.
1.8.1.11 Copying existing data as new data
1.8.1.12 Releasing failing product.
1.8.1.13 The above mentioned should be avoided by every individual.

1.8.2 **Unethical conduct and data integrity issue**

1.8.2.1 Human errors: when willful- Faking data (falsification or fraud with the intent to deceive).
1.8.2.2 Selection of good or passing results to the exclusion of those that is poor or failing (fabricating data).
1.8.2.3 Unauthorized changes to data made post-acquisition.
1.8.2.4 Errors that occur when data is transmitted from one system to another.
1.8.2.5 Changes to data through software bugs or malware of which the user is not aware.
1.8.2.6 Hardware malfunctions, such as disk crashes.
1.8.2.7 Changes in technology, where one document/record is replaced when it becomes obsolete or no longer supported, make old records unreadable or inaccessible.
1.8.2.8 Substituting data (like copying over data points from successful batch record into a failed batch record).
1.8.2.9 Intentionally omitting negative data (like OOS or, in trending graphs, eliminating outliers).
1.8.2.10 Hiding or obscuring SOP or protocol deviations.
1.8.2.11 Not recording activities contemporaneously.
1.8.2.12 Backdating.
1.8.2.13 Signing of record in place of other person.
1.8.2.14 Copying existing data as new data.
1.8.2.15 Re-running (reanalyzing) samples without a valid reason.
1.8.2.16 Discarding data without justification.

	1.8.2.17	Management oversight of quality metrics relevant to data governance.
1.9		**DETECTING & PREVENTING BREACHES TO DATA INTEGRITY**
	1.9.1	Quality Risk Management (QRM) approaches shall be implemented, wherever applicable to detect, control and prevent potential risk.
	1.9.2	Ensure the data generated is reliable, trustworthy verifiable.
	1.9.3	Ensure GMP is followed during processing and analyzing of raw material, packaging material, key star material, intermediates, APIs.
	1.9.4	Ensure the datas are traceable and/or referenced to original raw data and reviewed by an appropriate quality personnel. No column should be left unfilled and wherever not applicable to write NA provision should be made. Presence of unfilled column or block is also a point of data integrity.
	1.9.5	Ensure datas generated is authentic and retrievable.
	1.9.6	Ensure additional check on the accuracy of the entry for the data being entered manually.
	1.9.7	Laboratory control records should include complete data derived from all tests conducted to ensure compliance with established specifications and standards, including examinations of assays.
1.10		**DATA REVIEW AND APPROVAL- FOR ISSUES IDENTIFICATION**
	1.10.1	The approach of reviewing specific record content, such as critical data and metadata, cross outs (paper records) and audit trails (electronic records) should meet all applicable regulatory requirements and shall be risk-based.
	1.10.2	There should be a procedure that describes the process for review and approval of data. Data review should also include a risk-based review of relevant metadata, including relevant audit trails records.
	1.10.3	Data review should be documented and the record should include a positive statement regarding issues, it shall also include the date on which review was

performed and the signature of the reviewer.

1.10.4 A procedure should describe the actions to be taken if data review identifies an error or omission. This procedure should enable data corrections or clarifications to provide visibility of the original record, and traceability of the correction, using ALCOA Plus principles as per GDP SOP

1.10.5 Periodic audit of the data generated (encompassing both a review of electronically generated data and the broader organisational review) might verify the effectiveness of existing control measures and consider the possibility of unauthorised activity at all interfaces, e.g. have there been IT requests to amend any data post review? Have there been any system maintenance activities and has the impact of that activity been assessed?

1.11 CONTROLS OVER BREACHES TO DATA INTEGRITY

1.11.1 **Culture In Built**

1.11.1.1 Policy on data integrity and declaration stating that 'No breaches to data's' signed from all the Employees is in place and provided in **Annexure III.**

1.11.1.2 Awareness on data integrity policy will be given during induction program (for new joiners) and through regular GMP training. (for all employees)

1.11.1.3 It is the right of all individuals to report actual or suspected wrongdoing or violations of laws, rules, regulations, company/ ethical standards, or any other irregularities to management via Department Head.

1.11.2 **Data errors and loss of integrity shall be prevented by**

1.11.2.1 Maintaining quality of correctness, completeness, wholeness, soundness and compliance with the intention of the creators of the data.

1.11.2.2 It is achieved by preventing accidental or deliberate but unauthorized insertion, modification or destruction of data in a database.

1.11.2.3 Avoiding Human errors like:

- Data is entered by mistake & unawareness (not

being aware of regulatory requirements due to poor training).
- Document or Communicate problems immediately.
- Take time to do it right and avoiding short cuts.
- Follow the SOP and Methods strictly.

1.11.2.4 Systems shall be designed in a way that encourages compliance with the principles of data integrity. Examples include but not limited to:
- Access to clocks for recording timed events
- Accessibility of batch records at locations where activities take place
- Control over blank paper templates for data recording
- User access rights which prevent (or audit trail) data amendments
- Automated data capture or printers attached to equipment such as balances (Proximity of printers to relevant activities)
- Access to sampling points (e.g. for water systems).
- Access to raw data for staff performing data checking activities.

1.11.3 **Knowledge management program**

1.11.3.1 Regular scheduled trainings will be conducted on data integrity & GMP. The quality assurance and department heads in coordination with admin are responsible for conducting the training programs with simplified and understandable matter.

1.11.4 **Monitoring Mechanism**

1.11.4.1 Doer and checker system is available for critical activities which will impact the quality of raw material, packaging material, key starting material, intermediates, APIs.

1.11.4.2 Risk based approach followed for the compliance of all non-conformances

1.11.5 **System Control**

1.11.5.1 Guidelines, SOPs and protocols are available.

1.11.5.2 Scheduled self-inspection by Quality Assurance and

cross functional team is in place (SOP for Self Inspection SQA/O/008).

1.11.5.3 The Self Audit SOP _____ shall have DI checklist (**Annexure IV**) and format scheduled for DI inspection twice a year by DI trained technical staff (Schedule for DI Audit – **Annexure V**)

1.12 MANAGEMENT RESPONSIBILITY

1.12.1 Awareness on company's commitment on data integrity should be made to each employee at the time of induction.

1.12.2 Regular trainings on professional ethics, data integrity and Good Manufacturing Practices shall be conducted to all the employees.

1.12.3 Accordingly P&A and QA shall prepare policies such as Data Integrity policy (Annexure II ____), Responsibilities of employee related to data Reliability (Annexure I ____) and Pledge code for ethical Quality product (Annexure No I.: _____)

1.12.4 All above policies training shall be given to the all employees.

1.12.5 If any breaches to data integrity are identified, appropriate action (retraining, warning, and dismissal) shall be taken based on the severity of the issue. Based on the investigation findings to the particular breaches, appropriate corrective action shall be taken to prevent the recurrence of the same.

1.12.6 Customer shall be notified for negatively impacted data, wherever applicable

1.12.7 Data Integrity Policy as per **Annexure II**

1.13 ISSUANCE AND NUMBERING SYSTEM OF DATA INTEGRITY REPORT:

1.13.1 If data integrity observed then concerned department shall take issued format for Data integrity report (Format No. _____).

1.13.2 Enter the Data Integrity report number in format and take entry in register as Data Integrity Log (Format No. _____)

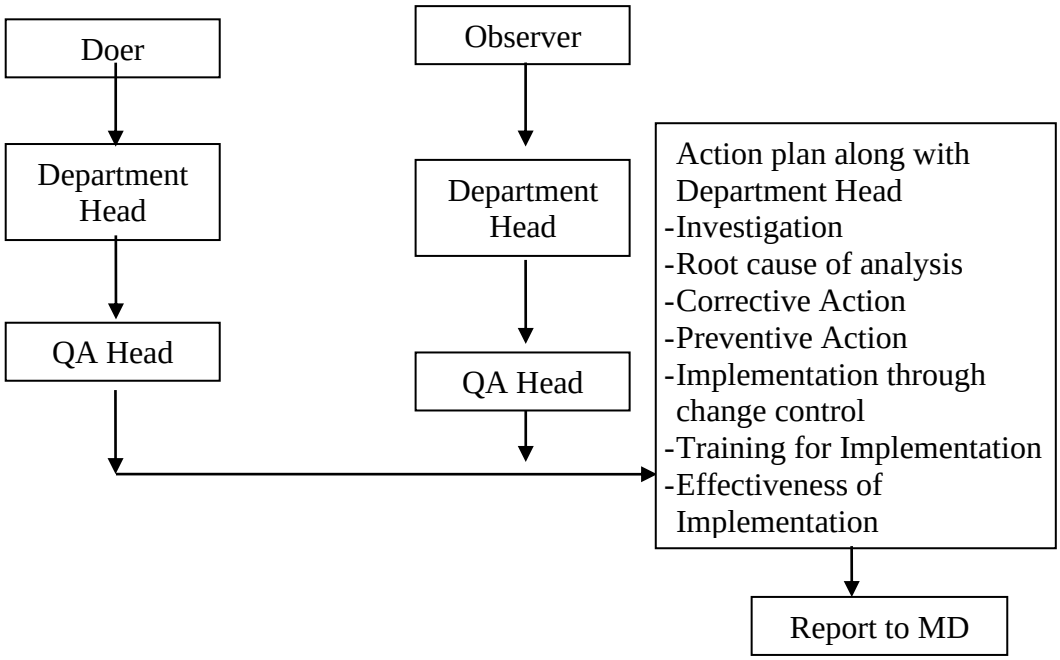
1.13.3 Numbering system of Data Integrity as follows "DI/XXX-YY".

Where 'DI' Stands for 'Data Integrity',
'XXX' stands for 'Serial Number' of Data Integrity,
'YY' Stands for 'Last Two Digits of the Calendar Year

1.13.4 According to format and procedure given below it will be investigated.

1.14 REPORTING STRUCTURE:

If Data Integrity observed, then it will be reporte per following structure



1.15 INCIDENT REPORTING FOR DATA INTEGRITY:

1.15.1 Observed Data Integrity should be reported by using format for Data integrity report (Format No. _____).

1.15.2 Based on outcome of investigation, re-training, re-qualification or disciplinary action will be taken depending on severity

1.16 INVESTIGATION:

Data Integrity to be investigated as per SOP Investigation.

1.16.1 **Data Review and Approval- for Issues**

Identification

1.16.1.1 The approach of reviewing specific record content, such as critical data and metadata, cross outs (paper records) and audit trails (electronic records) should meet all applicable regulatory requirements and shall be risk-based.

1.16.1.2 There should be a procedure that describes the process for review and approval of data. Data review should also include a risk-based review of relevant metadata, including relevant audit trails records.

1.16.1.3 Data review should be documented and the record should include a positive statement regarding issues, it shall also include the date on which review was performed and the signature of the reviewer.

1.16.1.4 A procedure should describe the actions to be taken if data review identifies an error or omission. This procedure should enable data corrections or clarifications to provide visibility of the original record, and traceability of the correction, using ALCOA Plus principles as per GDP SOP_____

1.16.1.5 Periodic audit of the data generated (encompassing both a review of electronically generated data and the broader organisational review) might verify the effectiveness of existing control measures and consider the possibility of unauthorised activity at all interfaces, e.g. have there been IT requests to amend any data post review? Have there been any system maintenance activities and has the impact of that activity been assessed?

1.16.2 **Route cause analysis:**

For observed data Integrity, action plan to be prepared, investigation will be done along with route cause analysis as per SOP for Investigation.

1.16.3 **Corrective and Preventive Action:**

After investigation and root cause of analysis, corrective action and preventive action shall be planned by Head QA along with department Head by following SOP for Corrective action and Preventive action (_____).

1.16.4 **Implementation of CAPA along with change control and training**

Planned corrective action and preventive action will be implemented through change control (_____), before implementation training shall be imparted to all concerns as per SOP for training (_____).

1.16.5 **Post Implementation Review**

Post Implementation shall be review within 30 days as per SOP for change control (_____) and recorded in change control form.

1.16.6 **Continuous Review and Improvement**

Every month corrective and preventive action shall be review for its effectiveness and improvement till three months. If continuously observed then review effectiveness and control within six months.

2 REFERENCES

U.S. Food and Drug Administration, Data Integrity and Compliance With Drug CGMP: Questions and Answers; Guidance for Industry, FDA-2018-D-3984, 2018, https://www.fda.gov/media/119267/download.

Pharmaceutical Inspection Convention/Pharmaceutical Inspection Cooperation Scheme, Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments Draft (PI-041), 2021, https://picscheme.org/docview/4234.

European Medicines Agency, EMA Draft Guideline on Computerized Systems and Electronic Data in Clinical Trials, 2021, https://www.ema.europa.eu/en/documents/regulatory-procedural-guideline/guideline-computerised-systems-electronic-data-clinical-trials_en.pdf.

Standard format	Annexure	Format No.	SOP Reference
Expectation / guidance (where relevant)	**Annexure I**		
Data Integrity Policy	**Annexure II**		
Data Reliability Policy	**Annexure III**		
Data Integrity Checklist	**Annexure IV**		
Data Integrity Schedule vs Executed	**Annexure V**		
Data Integrity Log (Issuance / Numbering System of DI	**Annexure VI**		

Template for Standard Operation Procedure (SOP) - Data Integrity (Optional)

Table of Contents

GRRMDP

Global Regulatory requirements for Good Manufacturing and Distribution practices in Pharmaceutical /Biopharma industries

1. Introduction

1.1 Background

- Provide context about the organization's reliance on accurate and trustworthy data for operational success.
- Emphasize the significance of data integrity in maintaining the organization's reputation and compliance with regulations.

1.2 Purpose of the SOP

- Clearly state the purpose of the SOP which is to establish guidelines and procedures for ensuring data integrity throughout the organization.

2. Scope

2.1 Inclusions

- Specify the types of data (e.g., customer records, research findings, relevant documents) covered by this SOP.
- Identify the departments or processes where data integrity measures apply.

2.2 Exclusions

- Define any data types or processes that are not encompassed by this SOP and the rationale behind their exclusion.

3. Definitions

3.1 Data Integrity

- Provide a concise and precise definition of data integrity, highlighting its role in maintaining accurate, consistent, and unaltered data.

3.2 Data Lifecycle

- Explain the stages of the data lifecycle, from creation and entry to storage, processing, and archiving.

4. Roles and Responsibilities

4.1 Data Owners

- Describe the responsibilities of individuals or departments designated as data owners.
- Highlight their role in ensuring data accuracy, accessibility, and security.

4.2 Data Custodians

- Define the responsibilities of data custodians who handle and manage data on a day-to-day basis.
- Explain their role in data entry, maintenance, and the safe custody, transport, storage of the data.

4.3 Data Integrity Officers

- List the duties of data integrity officers who oversee and enforce data integrity practices across the organization.

5. Data Integrity Measures

5.1 Data Entry and Collection

- Outline procedures for accurate data entry, including validation checks and standardized formats.
- Address data source verification and proper documentation.

5.2 Data Storage and Access

- Describe guidelines for secured data storage, including access controls, encryption, and backups.
- Emphasize the importance of data segregation and appropriate user permissions.

5.3 Data Processing and Manipulation

- Explain procedures for data manipulation, transformation, and calculations to ensure accuracy and consistency.
- Highlight audit trails and version control mechanisms.

5.4 Data Review and Approval

- Describe the process of data review and approval, involving relevant stakeholders to verify accuracy and completeness.

6. Data Auditing and Monitoring

6.1 Regular Audits

- Describe the schedule and process for conducting routine data audits to identify and rectify discrepancies.

6.2 Data Monitoring

- Explain how ongoing data monitoring helps detect anomalies, errors, or unauthorized changes in real-time.

7. Data Integrity Incidents

7.1 Reporting Incidents

- Provide guidelines for reporting and documenting data integrity incidents or breaches.

7.2 Incident Resolution

- Describe the steps to be taken while addressing data integrity incidents including investigation, containment and corrective actions.

8. Training and Awareness

8.1 Training Programs

- Explain the training initiatives to educate employees about data integrity best practices.
- Highlight the importance of continuous training to keep up with evolving threats and technologies.

9. Documentation

9.1 Data Integrity Policy

- Summarize the key points of the organization's data integrity policy which supports this SOP.

9.2 Data Integrity Procedures

- List and explain the detailed procedures for ensuring data integrity at each stage of the data lifecycle.

10. Annexures

- Attach any relevant templates, forms, or additional resources to assist in implementing the data integrity measures.

  Note: Customize the SOP to match the organization's specific needs and practices.