PHARMA DEVILS

QUALITY ASSURANCE DEPARTMENT

STANDARD OPERATING PROCEDURE

Department: Quality Assurance	**SOP No.:**
Title: Data Integrity	**Effective Date:**
Supersedes: Nil	**Review Date:**
Issue Date:	**Page No.:**

1.0 PURPOSE

To define a procedure for control of data integrity issues at manufacturing location.

2.0 SCOPE

2.1 This procedure applies to all the employees working in all the departments and applicable to all GMP documents throughout its lifecycle, of ……………..

3.0 REFERENCE(S) & ATTACHMENTS

3.1 References

3.1.1 MHRA GMP Data Integrity Definitions and Guidance for Industry March 2015.

3.1.2 ICH Q9 guideline: Quality Risk management.

3.2 Attachments

3.2.1 Nil

4.0 DEFINITION & ABBREVIATION(S)

4.1 Definitions

4.1.1 **Data Integrity:** The extent to which all data are complete, consistent and accurate throughout the data lifecycle.

4.1.2 **Raw data:** Original records and documentation, retained in the format in which they were originally generated (i.e. paper or electronic), or as a ‘true copy’.

4.1.3 **Metadata:** Metadata is data that describe the attributes of other data, and provide context and meaning. Typically, these are data that describe the structure, data elements, inter-relationships and other characteristics of data. It also permits data to be attributable to an individual. Metadata forms an integral part of the original record. Without metadata, the data has no meaning.

4.1.4 **Data Lifecycle:** 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.

4.1.5 **Audit Trail:** GMP audit trails are metadata that are a record of GMP critical information (for example the change or deletion of GMP relevant data), which permit the reconstruction of GMP activities.

4.2 Abbreviations

4.2.1 GMP: Good manufacturing practices

4.2.2 SOP: Standard Operating Procedures

4.2.3 ID: Identity

4.2.4 E.g.: Example gratia

5.0 RESPONSIBILITY:

5.1 All staff:

5.1.1 To follow the procedure as described in the SOP.

5.2 All Departments Heads:

5.2.1 To ensure that all the persons working in department are following the procedure.

5.3 Quality Assurance Head:

5.3.1 To ensure implementation of the defined procedure.

5.4 Plant Head:

5.2.1 To ensure implementation of the defined procedure.

6.0 Distribution:

I. Quality Assurance

II. Quality Control

III. Production

IV. Ware house

V. Engineering

VI. Human resource and Administration

VII. Environment, Health and safety

7.0 PROCEDURE:

7.1 Data Integrity:

7.1.1 Data integrity arrangements must ensure that the accuracy, completeness, content and meaning of data is retained throughout the data lifecycle.

7.1.2 Data must be:

A– Attributable to the person generating the data

L– Legible and permanent

C– Contemporaneous

O– Original record (or 'true copy')

A– Accurate

7.1.3 Raw data must:

• Be legible and accessible throughout the data lifecycle**.**

• Permit the full reconstruction of the activities resulting in the generation of the data.

7.1.4 Where computerised systems are used to capture, process, report or store raw data electronically, system design shall always provide for the retention of full audit trails to show all changes to the data while retaining previous and original data. It shall be possible to associate all changes to data with the persons making those changes, and changes shall be time stamped and a reason given. Users shall not have the ability to amend or switch off the audit trail.

7.1.5 There shall be a procedure which describes the process for the review and approval of data, including raw data. Data review must also include a review of relevant metadata, including audit trail.

7.1.6 A procedure shall describe the actions to be taken if data review identifies an error or omission. This procedure shall enable data corrections or clarifications to be made in a GMP compliant manner, providing visibility of the original record, and audit trailed traceability of the correction.

7.1.7 The archive arrangements must be designed to permit recovery and readability of the data and metadata throughout the required retention period.

7.1.8 Backup and recovery processes must be validated. The backup file shall contain the data (which includes associated metadata) and shall be in the original format or in a format compatible with the original format.

7.1.9 Computerised systems shall comply with the requirements regulatory guidelines and be validated for their intended purpose.

7.1.10 Original records and true copies must preserve the integrity (accuracy, completeness, content and meaning) of the record. Exact (true) copies of original records may be retained in place of the original record (e.g. scan of a paper record), provided that a documented system is in place to verify and record the integrity of the copy.

7.1.11 User login ID's and passwords shall not be shared and shall be kept confidential.

7.1.12 The individual shall log in using the account with the appropriate access rights for the given task e.g. a laboratory manager performing data checking shall not log in as system administrator where a more appropriate level of access exists for that task.

7.1.13 Data and document retention arrangements shall ensure the protection of records from deliberate or inadvertent alteration or loss. Secure controls must be in place to ensure the data Integrity of the record throughout the retention period, and validated where appropriate.

7.1.14 Senior management is responsible for the implementation of systems and procedures to minimise the potential risk to data integrity, and for identifying the residual risk, using the principles of ICH Q9 guideline (Quality risk management).

8.0 REVISION HISTORY

Version No.	00	Effective Date	
Details of revision: New SOP Prepared			