

MASTER COPY

For Restricted Circulation only

 SHAKAMBHARI GROUP # SteelWithin	SHAKAMBHARI ISPAT & POWER LTD. (Formerly known as Ess Dee Aluminium Ltd.)		
STANDARD OPERATING PROCEDURE			
Title: SOP for Data Integrity			
Page No. 1 of 6			
SOP No.	Version No.	Effective Date	Next review date
SIPL/QAS/030	00	07.07.2026	06.07.2028

1.0 PURPOSE

- 1.1 To define a documented procedure that ensures all data — whether paper-based (manual records) or electronic — generated, recorded, processed, reported, retained, retrieved and reviewed across the plant is Attributable, Legible, Contemporaneous, Original and Accurate (ALCOA), and is Complete, Consistent, Enduring and Available (ALCOA+), throughout its life cycle.
- 1.2 To establish a Data Integrity governance framework and the controls, behaviours and responsibilities required to prevent, detect and correct data integrity failures at Shakambhari Ispat & Power Ltd.

2.0 SCOPE

- 2.1 This SOP is applicable to all data and records — manual / paper, electronic, hybrid, photographic, imaging and printed — generated at all functions of the plant engaged in the conversion of aluminium foil for pharmaceutical primary packaging, including but not limited to:
 - 2.1.1 Foil rolling mill (thickness, tension, spool / coil data).
 - 2.1.2 Annealing / degreasing furnace records.
 - 2.1.3 Lacquer coating & polyethylene lamination (coater-laminator: coating weight / GSM, oven temperatures, line speed).
 - 2.1.4 Gravure printing press (colour, print registration, artwork / specimen approval, cylinder records).
 - 2.1.5 Slitting & rewinding (width, core, roll length, joint records).
 - 2.1.6 Quality Control laboratory instruments and testing records (GSM, thickness, COF, adhesion, migration / food-contact test data, bond strength).
 - 2.1.7 Warehouse, dispatch, and pre-dispatch inspection records.
 - 2.1.8 Engineering, calibration, preventive maintenance and utility (compressed air, water, HVAC) records.
- 2.2 This SOP applies to all employees, contract staff, trainees and third parties who create, handle, review, approve, store or retrieve data on behalf of SIPL.

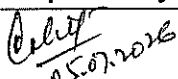
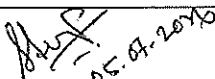
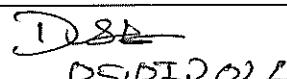
3.0 REFERENCE(S) & ATTACHMENTS

3.1 References

- 3.1.1 ISO 15378:2017 - 4.2.4, 4.2.5, 7.5.
- 3.1.2 ISO 9001:2015, Clause 7.5.
- 3.1.3 ICH Q10.

3.2 Attachments

- 3.2.1 Attachment-I : Data Integrity Risk Assessment Format - SIPL/QAS/030/F01/00
- 3.2.2 Attachment-II : Audit Trail Review Record - SIPL/QAS/030/F02/00
- 3.2.3 Attachment-III : Data Integrity Undertaking / Declaration - SIPL/QAS/030/F03/00
- 3.2.4 Attachment-IV : User Access & Privilege Control Record - SIPL/QAS/030/F04/00

Prepared By:	Checked By:	Approved By:
 05.07.2026	 05.07.2026	 05.07.2026

For Restricted Circulation only

 SHAKAMBHARI GROUP # SteelWithin		SHAKAMBHARI ISPAT & POWER LTD. (Formerly known as Ess Dee Aluminium Ltd.)	
STANDARD OPERATING PROCEDURE			
Title: SOP for Data Integrity			Page No. 2 of 6
SOP No.	Version No.	Effective Date	Next review date
SIPL/QAS/030	00	07.07.2026	06.07.2028

3.2.5 Attachment-V : Data Integrity Breach / Incident Reporting Form -
SIPL/QAS/030/F05/00

4.0 RESPONSIBILITY

4.1 All Employees / Data Originators

- 4.1.1 To record data accurately, contemporaneously and legibly at the time the activity is performed.
- 4.1.2 To never falsify, back-date, pre-date, fabricate, delete, obscure or share personal login credentials.
- 4.1.3 To report any suspected or actual data integrity breach to their department head / QA.

4.2 Department Heads (Rolling, Coating-Lamination, Printing, Slitting, QC, Stores, Engineering, HR)

- 4.2.1 To ensure adequate resources, trained personnel and controlled formats are available for correct data recording.
- 4.2.2 To perform / assign first-level review of records and audit trails within their department.
- 4.2.3 To foster an open culture where errors can be reported without fear (no-blame reporting).

4.3 Quality Assurance Person

- 4.3.1 To issue, control and retrieve SOPs, formats and logbooks and maintain their record.
- 4.3.2 To maintain the master list of computerised systems, user access records and the audit trail review schedule.
- 4.3.3 To conduct periodic data integrity risk assessments and verification checks.

4.4 IT / Engineering (System Administrator)

- 4.4.1 To configure user access levels, enable audit trails, maintain data back-up and restoration, and ensure server date / time synchronisation and control.

4.5 QA Head

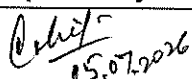
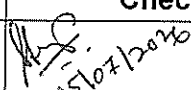
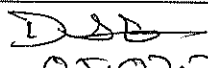
- 4.5.1 To approve this SOP and the data integrity governance framework.
- 4.5.2 To ensure investigation of data integrity breaches through incident management & CAPA.

4.6 Plant Head / Top Management

- 4.6.1 To provide leadership commitment, allocate resources and set the 'tone at the top' for a strong data integrity culture.
- 4.6.2 To approve this SOP and review data integrity status during Management Review.

5.0 DISTRIBUTION

- 5.1 Quality Assurance
- 5.2 Quality Control
- 5.3 Production (Rolling / Coating-Lamination / Printing / Slitting)
- 5.4 Store / Warehouse

Prepared By:	Checked By:	Approved By:
 05.07.2026	 05.07.2026	 05.07.2026

For Restricted Circulation only

 SHAKAMBHARI GROUP # SteelWithin		SHAKAMBHARI ISPAT & POWER LTD. (Formerly known as Ess Dee Aluminium Ltd.)	
STANDARD OPERATING PROCEDURE			
Title: SOP for Data Integrity			Page No. 3 of 6
SOP No.	Version No.	Effective Date	Next review date
SIPL/QAS/030	00	07.07.2026	06.07.2028

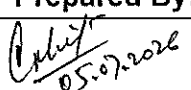
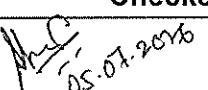
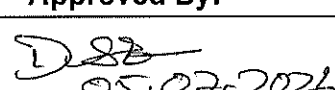
- 5.5 Engineering / IT
 5.6 Human Resource and Administration

6.0 DEFINITION(S) & ABBREVIATION(S)**6.1 Definitions**

- 6.1.1 **Data Integrity:** The degree to which data is complete, consistent, accurate, trustworthy and reliable, and these characteristics are maintained throughout the data life cycle.
- 6.1.2 **ALCOA+:** A framework for data quality — Attributable, Legible, Contemporaneous, Original, Accurate, plus Complete, Consistent, Enduring and Available.
- 6.1.3 **Raw Data:** Original records and documentation, retained in the format in which they were originally generated (paper or electronic), that permit the full reconstruction of the activity — e.g. the printed strip-chart of a coating oven, the balance printout for GSM, the original entry in the printing logbook.
- 6.1.4 **Metadata:** Data that describe the attributes of other data and provide context and meaning — e.g. the time stamp, user ID, instrument ID and units associated with a QC test result.
- 6.1.5 **Audit Trail:** A secure, computer-generated, time-stamped electronic record that allows reconstruction of the course of events relating to the creation, modification or deletion of a record, including the 'who, what, when and why'.
- 6.1.6 **Dynamic Record:** Records with an interactive interface where the format may be changed and data re-processed.
- 6.1.7 **Hybrid System:** A system combining paper and electronic records — e.g. an electronic balance whose printout is manually pasted into a QC worksheet.
- 6.1.8 **Data Life Cycle:** All phases of data from initial generation and recording, through processing, use, retention, archival and retrieval, to destruction.
- 6.1.9 **Good Documentation Practice (GDP):** Practices that ensure records are recorded accurately, contemporaneously and legibly, as defined in SIPL/QAS/017.

6.2 Abbreviations

- 6.2.1 ALCOA+ : Attributable, Legible, Contemporaneous, Original, Accurate (+ Complete, Consistent, Enduring, Available)
- 6.2.2 CAPA : Corrective Action and Preventive Action
- 6.2.3 DI : Data Integrity
- 6.2.4 GDP : Good Documentation Practice
- 6.2.5 QA : Quality Assurance
- 6.2.6 QC : Quality Control
- 6.2.7 SOP : Standard Operating Procedure
- 6.2.8 IT : Information Technology
- 6.2.9 ID : Identification

Prepared By:	Checked By:	Approved By:
 05.07.2026	 05.07.2026	 05.07.2026

For Restricted Circulation only

 SHAKAMBHARI GROUP # SteelWithin		SHAKAMBHARI ISPAT & POWER LTD. (Formerly known as Ess Dee Aluminium Ltd.)	
STANDARD OPERATING PROCEDURE			
Title: SOP for Data Integrity			Page No. 4 of 6
SOP No.	Version No.	Effective Date	Next review date
SIPL/QAS/030	00	07.07.2026	06.07.2028

7.0 PROCEDURE

7.1 Data Integrity Principles – ALCOA+

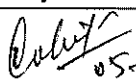
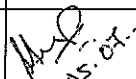
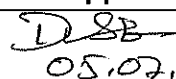
- 7.1.1 All data at SIPL, whether paper or electronic, shall comply with the following principles:
- 7.1.1.1 **Attributable:** Every record shall clearly identify who performed the activity and when. Sign / initial and date every entry; every electronic action shall be traceable to a unique named user.
 - 7.1.1.2 **Legible:** Records shall be readable and permanent. Use indelible blue / black ink; never use pencil, correction fluid, or overwriting. Corrections as per GDP (single-line cross-out, initial, date, reason).
 - 7.1.1.3 **Contemporaneous:** Data shall be recorded at the time the activity is performed — e.g. the coating-oven temperature is logged as it is read, not reconstructed at end of shift.
 - 7.1.1.4 **Original:** The first / source record (or a certified true copy) shall be retained — e.g. the original balance printout for GSM, the original in-process check sheet on the slitter.
 - 7.1.1.5 **Accurate:** Data shall be correct, truthful and free from errors; instruments shall be calibrated and within validity before use.
 - 7.1.1.6 **Complete:** All data, including repeat / re-tests, out-of-specification results and associated metadata / audit trails, shall be retained. Nothing shall be selectively deleted.
 - 7.1.1.7 **Consistent:** Data shall be recorded in the expected sequence with correct, synchronised date / time stamps.
 - 7.1.1.8 **Enduring:** Records shall be recorded on controlled, durable media (issued formats / logbooks, validated electronic storage), not on loose scraps, hands or Post-it notes.
 - 7.1.1.9 **Available:** Records shall be retrievable for review, audit or inspection throughout the defined retention period.

7.2 Data Governance & Culture

- 7.2.1 Top management shall establish and communicate a data integrity policy and lead by example, ensuring staff are not placed under undue pressure (e.g. production targets) that could compromise data.
- 7.2.2 An open, no-blame reporting culture shall be maintained so that errors and breaches can be reported and corrected without fear of unfair reprisal.
- 7.2.3 A data integrity risk assessment (Attachment-I) shall be performed for each process area and computerised system at least once every two years and upon any significant change (via Change Control, SIPL/QAS/002).

7.3 Control of Paper Records

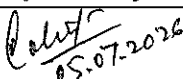
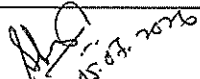
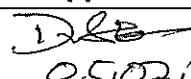
- 7.3.1 All logbooks, worksheets, in-process check sheets and formats shall be pre-printed with a format number, issued and retrieved by QA. Loose or uncontrolled paper shall not be used to record raw data.
- 7.3.2 Entries and corrections shall follow GDP (SIPL/QAS/017): contemporaneous, indelible, single-line cross-out with initial, date and reason; no obliteration or correction fluid.

Prepared By:	Checked By:	Approved By:
 05.07.2026	 05.07.2026	 05.07.2026

For Restricted Circulation only

 SHAKAMBHARI GROUP #SteelWithin		SHAKAMBHARI ISPAT & POWER LTD. (Formerly known as Ess Dee Aluminium Ltd.)	
STANDARD OPERATING PROCEDURE			
Title: SOP for Data Integrity			Page No. 5 of 6
SOP No.	Version No.	Effective Date	Next review date
SIPL/QAS/030	00	07.07.2026	06.07.2028

- 7.3.3 Blank / unused fields shall be lined through and initialled; 'NA' shall be used where not applicable. No blank spaces shall be left to be filled later.
- 7.3.4 Second-person / QA review shall verify completeness, correctness and contemporaneous recording before release of the batch / roll.
- 7.4 Control of Electronic Records & Computerised Systems**
- 7.4.1 A master list of all computerised systems generating GxP data (e.g. QC instruments with software, coating-line SCADA / PLC data loggers, printing colour-measurement systems, weighbridge, SAP quality modules) shall be maintained and each classified by data integrity risk.
- 7.4.2 Each user shall have a unique login ID and password. Sharing of passwords or use of generic / shared accounts is strictly prohibited.
- 7.4.3 Access privileges shall be role-based and follow segregation of duties: personnel who create / enter data shall not hold system-administrator rights that allow them to delete data or alter the audit trail. Administrator rights shall rest with IT / Engineering, not with data originators. Access shall be recorded on Attachment-IV and reviewed periodically.
- 7.4.4 Audit trails shall be enabled and shall not be disabled or altered by users. Where a legacy system cannot generate an electronic audit trail, a controlled hybrid paper record with equivalent controls shall be maintained until the system is upgraded (tracked via Change Control).
- 7.4.5 System date and time shall be controlled / locked and synchronised; users shall not be able to change the clock.
- 7.4.6 Electronic data (including metadata and audit trails) shall be backed up at a defined frequency; back-ups shall be verified by periodic restoration testing and stored securely.
- 7.5 Audit Trail Review**
- 7.5.1 For systems with audit trail capability, a review of the audit trail shall be performed and documented on Attachment-II, at a frequency commensurate with the data's criticality (e.g. review of QC analytical data audit trails prior to result approval).
- 7.5.2 The review shall check for any modification, deletion, re-processing, aborted runs or changes to date / time, and shall confirm the reason for any change is recorded and justified.
- 7.6 Hybrid Systems**
- 7.6.1 Where a printout is attached to a paper record (e.g. balance slip for GSM, thickness gauge printout), both the printout (original) and the associated electronic data (where retained) shall be preserved. The printout shall be signed and dated and cross-referenced to the worksheet / batch record.
- 7.7 Data Retention, Archival & Retrieval**
- 7.7.1 Records shall be retained for the period defined in the retention schedule (minimum as per ISO 15378 and customer / regulatory requirement, and not less than one year beyond the expiry / shelf life of the packaged product supplied, unless a longer period is agreed with the customer).

Prepared By:	Checked By:	Approved By:
 05.07.2026	 05.07.2026	 05.07.2026

For Restricted Circulation only



SHAKAMBHARI ISPAT & POWER LTD. (Formerly known as Ess Dee Aluminium Ltd.)

STANDARD OPERATING PROCEDURE

Title: SOP for Data Integrity			Page No. 6 of 6
SOP No.	Version No.	Effective Date	Next review date
SIPL/QAS/030	00	07.07.2026	06.07.2028

7.7.2 Archived records (paper and electronic) shall be protected from unauthorised access, alteration, loss and deterioration, and shall remain retrievable throughout the retention period.

7.7.3 Destruction of records after the retention period shall be authorised and documented.

7.8 Training & Declaration

7.8.1 All personnel shall be trained on this SOP and on GDP at induction and at defined intervals thereafter (as per SIPL/QAS/003 Training Programme).

7.8.2 Personnel handling GxP data shall sign a Data Integrity Undertaking (Attachment-III) confirming their understanding of, and commitment to, these principles.

7.9 Data Integrity Breach – Reporting & Investigation

7.9.1 Any suspected or confirmed data integrity breach (e.g. falsification, back-dating, unauthorised deletion, sharing of passwords, fabrication of results) shall be reported immediately using Attachment-V.

7.9.2 The breach shall be investigated through Incident Management & CAPA (SIPL/QAS/004) to determine root cause, scope, impact on product quality and any affected batches / customers, and corrective / preventive actions.

7.9.3 Where product quality or supplied material is impacted, the affected customer(s) shall be notified in accordance with the quality agreement, and the need for recall (SIPL/QAS/010) shall be evaluated.

7.9.4 Disciplinary action for deliberate falsification shall be handled as per HR policy; however, genuine, self-reported errors shall be treated under the no-blame culture.

7.10 Prohibited Practices (Illustrative)

7.10.1 Recording data on uncontrolled paper, hands, gloves or scraps and transcribing later.

7.10.2 Back-dating, pre-dating or completing records before / after the activity.

7.10.3 Sharing login credentials or logging in on behalf of another person.

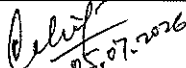
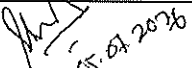
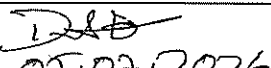
7.10.4 Deleting, overwriting, hiding or 'testing into compliance' (repeating a test until a passing result is obtained and discarding failing data).

7.10.5 Disabling or ignoring audit trails; changing the system clock.

7.10.6 Signing for an activity not personally performed or verified.

8.0 REVISION HISTORY

Revision No.	00	Effective Date	07.07.2026	CC No.	NA
Details of revision: New SOP					

Prepared By:	Checked By:	Approved By:
 05.07.2026	 05.07.2026	 05.07.2026