DATA MIGRATION POLICY

SFPL-POL-005

Sonata Finance Pvt. Ltd.
IInd Floor, CP-1, PG Tower,
Kursi Road, Vikas Nagar,
Lucknow - 226022
Uttar Pradesh, India

Table of Contents

Document Control

Document Reference Number	SFPL-POL-005
Effective Date	16th July 2024
Document Owner	CIO

Document Ownership

Version	Prepared by	Reviewed by	Approved By	Date Approved
1.0	CISO	CIO		

REVISION HISTORY

VERSION NO.		RELEASE DATE	DETAILS OF CHANGES	REVIEWED BY	APPROVED BY
FROM	TO				
1.0	1.0	06.07.2024	New	CIO	

Document Control Statement:

- All rights reserved and this document is confidential.
- This document is intended solely for the use of Sonata Finance Private Limited (SFPL/Sonata) employees and/or the person who have executed non-disclosure agreement with SFPL.
- This document may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced in any form or manner including by any electronic, digital, or mechanical means to any medium, electronic or otherwise, or machine readable form including any information storage, scanning or retrieval system without the prior express, written consent from SFPL
- If this copy is found other than the intended location(s) please inform to ashutosh.chaturvedi@sonataindia.com .
- The User is advised to ensure that the appropriate version of the document is obtained for the intended use.

1. Introduction & Purpose of Data Migration Policy

Data migration is a crucial process for Sonata, involving the transfer of data from one system or storage environment to another. This Data Migration Policy outlines our commitment to ensuring the secure, efficient, and compliant handling of data throughout migration activities. By adhering to this policy, we aim to safeguard data integrity, maintain confidentiality, and uphold regulatory requirements. Effective planning, rigorous testing, and continuous improvement are key principles that guide our approach to data migration, ensuring minimal disruption to operations and maximum protection of sensitive information. This policy serves as a framework to govern all data migration activities within our organization, fostering a culture of accountability and excellence in data management.

2. Scope

This policy applies to all data migration activities conducted by Sonata, including but not limited to migrations between databases, applications, or storage platforms. It encompasses both internal and external data migrations.

3. Responsibilities

- **Data Owner**: The data owner is responsible for identifying the data to be migrated, ensuring its accuracy, completeness, and maintaining data quality throughout the migration process.
- **IT Team**: The IT team is responsible for planning and executing the data migration process, including data extraction, transformation, loading, and validation.
- **Chief Information Security Officer (CISO)**: The CISO has to ensure that appropriate security measures are implemented during data migration to protect against unauthorized access, data breaches, or data loss.
- **Compliance Officer**: The compliance officer ensures that data migration activities comply with relevant laws, regulations, and internal policies, especially concerning data protection and privacy.

4. Data Migration Process

- **Planning**:
  - Define migration objectives, scope, and timelines.
  - Conduct impact assessment to understand risks and dependencies.
  - Identify stakeholders and their roles in the migration process.
- **Preparation**:
  - Backup data from the source system before migration.
  - Ensure data cleansing and validation to maintain data quality.
  - Prepare migration scripts and tools required for the transfer.

- **Execution**:
  - Perform data extraction from the source system.
  - Transform data formats and structures as necessary.
  - Load data into the target system and validate the integrity of migrated data.

- **Testing**:
  - Conduct comprehensive testing to ensure that migrated data meets functional and non-functional requirements.
  - Validate data accuracy, completeness, and consistency.

- **Deployment**:
  - Plan and execute the deployment of the migrated data into production environment.
  - Monitor system performance post-migration to identify any issues or anomalies.

- **Post-Migration**:
  - Document the migration process, including any issues encountered and their resolutions.
  - Conduct a Third Party data migration audit

5. Security and Confidentiality

- **Data encryption:**
  Encrypt data during transmission and storage to protect against unauthorized access. The encryption method should be well documented.

- **Access control:**
  Implement strict access controls to ensure only authorized personnel have access to sensitive data during migration. The access control should be accordance with Information Security Policy and Cyber Security Policy adopted by Sonata.

- **Compliance:**
  Adhere to relevant data protection regulations such as GDPR, CCPA, and local data protection laws in India.

6. Monitoring and Auditing

- Regularly monitor data migration activities to detect and mitigate potential security breaches or data integrity issues.

- Conduct periodic audits of data migration processes to ensure compliance with policies and regulatory requirements.

7. Training and Awareness

- Provide training to personnel involved in data migration to ensure they understand their roles and responsibilities. The personnel involved should be trained in the use of new technologies adopted in the migration.

- Raise awareness among employees about data protection best practices and the importance of data integrity during migration.

- Matching of reports / ledgers / books generated from old systems and new systems should be done by concerned departments / stakeholders to ensure that there is no difference.

8. Documentation

- Maintain comprehensive documentation of data migration processes, including migration plans, risk assessments, test results, and post-migration reports.

- Documentation of all steps should follow the instructions as per change management procedures.

9. Incident Response

- Develop and maintain an incident response plan to address any data breaches or anomalies discovered during the data migration process. The incident response plan adopted by Sonata in its Information Security policy must be adhered to.

- Establish procedures for reporting and escalating incidents to minimize impact on business operations.

- The incident response plan adopted by Sonata in its Information Security policy, Business Continuity and Disaster Recovery Policy must be adhered to.

10. Review and Continuous Improvement

- Regularly review and update the data migration policy to reflect changes in technology, regulatory requirements, and business needs.

- Continuously improve data migration processes based on lessons learned from previous migrations.

- Conduct post-migration reviews to gather feedback and identify areas for improvement.

By following the guidelines outlined herein, Sonata reinforces its dedication to protecting sensitive information, minimizing risks, and ensuring seamless transitions between systems. Continuous adherence to this policy, coupled with regular updates and training, will empower our team to execute data migrations efficiently and confidently, ultimately supporting our mission to serve our customers and stakeholders with excellence. Together, we uphold the trust placed in us by safeguarding the integrity of our data assets throughout their lifecycle.

********** END OF DOCUMENT**********