DATA MIGRATION POLICY

JUNE 2025

DOC POLICY NO:

Developed By

Assistant General Manager, Information Technology and Security Compliance

Executive Summary

North South Power Company Limited recognizes that the accuracy, security, and consistency of its data assets are critical to ensuring business continuity, operational efficiency, and regulatory compliance. This Data Migration Policy establishes a structured and standardized framework to guide the planning, execution, monitoring, and review of all data migration activities across the organization. The policy ensures that every migration—whether involving applications, databases, or systems of record—is conducted with integrity, transparency, and minimal risk. It defines the core principles, roles, and responsibilities required to safeguard data throughout the migration lifecycle and mandates compliance with internal policies and applicable data protection laws.

Applicable to all employees, contractors, and third-party service providers, this policy reinforces North South Power Company Limited’s commitment to protecting its information assets and maintaining data quality, security, and accessibility at every stage of migration.

Table of Contents

Commented [OA1]: Formatted for structure

	INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT	DOC NO: DATE OF ISSUE: REVISED DATE: **N/A**
	DOCUMENT TITLE: **DATA MIGRATION POLICY**	

1. Purpose

The purpose of this Data Migration Policy is to provide a comprehensive framework that governs the planning, execution, and oversight of data migration efforts across North South Power Company Limited. It is intended to ensure that data is transferred in a manner that maintains its integrity, security, and availability, while minimizing business disruption and adhering to legal and regulatory requirements.

2. Scope

This policy covers all data migration activities within North South Power Company Limited, including:

- Migrations of enterprise systems, databases, and applications
- Transfers between storage platforms or cloud service providers
- System consolidations, upgrades, or replacements
- Involvement of all employees, departments, contractors, and third-party providers

This policy applies to both production and non-production environments and governs both planned migrations and urgent/emergency data transfers.

3. Principles

This policy covers all data migration activities within North South Power Company Limited, including:

3.1 Data Integrity

Migration must preserve data completeness and accuracy, without unauthorized alteration or corruption.

3.2 Data Security

Sensitive data must be encrypted during transit and access must be controlled and logged.

Commented [OA2]: What is sensitive data?

3.3 Compliance

Migrations must adhere to relevant legal and regulatory requirements concerning data protection and privacy.

3.4 Stakeholder Engagement

Involve relevant stakeholders in the planning and execution of migration activities to ensure alignment with organizational goals.

3.5 Transparency & Documentation:

Maintain thorough documentation of all migration processes, steps, decisions and outcomes.

4. Processes

4.1 Planning

- **Assessment**: Conduct a comprehensive assessment of existing data sources, identify data to be migrated, and determine data characteristics (e.g., volume, format, structure).

- **Migration Strategy**: Develop a migration strategy that outlines objectives, methodologies (e.g., direct migration, phased approach), timelines, resource requirements, and risk management strategies.

- **Stakeholder Identification**: Identify stakeholders including business units, IT staff, and compliance officers and establish communication channels.

4.2 Execution

- **Preparation**: Cleanse and prepare data for migration by removing duplicates, standardizing formats, and ensuring data quality.

- **Testing**: Perform data migration testing in a controlled environment to verify migration scripts, tools, and integrity of migrated data.

- **Initial Data Verification/Check by User Department:** Prior to executing the live migration, the User Department must review a sample of the prepared data in the staging or test environment. This includes checking for:
  - Accuracy and completeness of data mapping.
  - Correct application of business rules.
  - Any anomalies or inconsistencies that may affect operational use.

  Feedback from this verification is documented and used to make final adjustments before proceeding with the actual implementation.

- **Implementation**: Execute the migration according to the defined strategy, ensuring minimal disruption to ongoing operations.
- **Quality Control Verification/Check (Post-Implementation):** After data migration execution, the IT/Data Migration Team performs a formal quality control check to ensure:
  - Migrated data matches expected totals and record counts.
  - No data loss, corruption, or truncation occurred during the transfer.
  - Integrity constraints and referential links are intact.

Discrepancies or exceptions identified during this phase are documented and corrected before proceeding.

4.3 Oversight

- **Monitoring**: Continuously monitor the migration process for issues and adherence to timelines and standards.

- **Validation**: Validate migrated data against source data to confirm accuracy, consistency, and completeness post-migration.

- **Final Data Verification/Check by User Department:** The User Department conducts a comprehensive review of the migrated data in the live environment. This includes:

  - Validating that all expected data is present and accessible.
  - Verifying that business processes (e.g., reporting, transactions) function correctly with the new data.
  - Confirming that critical workflows are unaffected by the migration.

  A sign-off is provided by the User Department to formally confirm acceptance of the migrated data and readiness for full operational use.

- **Review and Feedback**: Conduct a post-migration review to identify successes, challenges, and areas for improvement. Document lessons learned for future migrations.

5. Standards

- **Data Standards**: Establish data standards for formats, naming conventions, and data structures that must be adhered to during migration.

- **Security Measures**: Implement necessary security measures such as encryption, access controls, and secure transmission protocols.

- **Quality Assurance**: Set up quality assurance procedures to evaluate the quality of data before, during, and after the migration process.

6. Roles and Responsibilities

- **Data Migration Team**
  Responsible for executing the migration process, including planning, testing, and implementation.

- **Data Owners**
  Responsible for the quality and integrity of the data being migrated and providing approvals throughout the migration process.

- **IT Governance**
  Oversee compliance with this policy, ensuring proper documentation and adherence to standards.

7. Training and Awareness

Provide training programs for employees involved in data migration activities to ensure they understand the processes, principles, and standards set forth in this policy.

8. Policy Review and Revision

This policy will undergo a formal review every two (2) years to ensure its continued relevance and effectiveness. The review will be conducted by the IT Security Team in collaboration with key stakeholders. If significant changes in technology, regulatory requirements, or threat landscape arise before the next scheduled review, an addendum will be issued and attached as an update to relevant sections of the policy. Such interim updates will remain in effect until the next comprehensive review and integration into the core policy.