ERP USER ACCESS RIGHTS AND REVIEW POLICY

FEBRUARY 2024

DOC POLICY NO:

Developed By

Assistant General Manager, Information Technology and Security Compliance

Executive Summary

The ERP User Access Rights and Review Policy at North South Power (NSP) aims to establish a robust framework for managing user access to the Enterprise Resource Planning System, specifically Microsoft Dynamics Finance and Operations. This policy is crucial for safeguarding sensitive and confidential data, ensuring that only authorized individuals have the necessary rights to access and manipulate information within the ERP system.

This policy applies to all employees, contractors, vendors, and any individuals granted access to the ERP system. It delineates clear guidelines for granting, modifying, and revoking user access rights, promoting accountability and compliance with organizational and regulatory standards. By adhering to these established principles and procedures, NSP seeks to effectively manage user access, reduce potential security risks, and enhance the overall integrity of its operational data.

	INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT	DOC NO: DATE OF ISSUE: REVISED DATE: **N/A**
	DOCUMENT TITLE: **ERP USER ACCESS RIGHTS AND REVIEW POLICY**	

Table of Contents

Commented [OA1]: Format for structure

	INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT	DOC NO: DATE OF ISSUE: REVISED DATE: **N/A**
	DOCUMENT TITLE: **ERP USER ACCESS RIGHTS AND REVIEW POLICY**	

1.0 Purpose

The purpose of the ERP User Access Rights and Review Policy is to protect sensitive and confidential information within North South Power's Enterprise Resource Planning System. This policy aims to ensure that:

Commented [OA2]: Please Define

I. **Access Control**: Only authorized personnel can access specific functionalities and data within the ERP system, thereby minimizing the risk of unauthorized use or data breaches.

II. **Data Integrity**: By regulating user rights, the policy helps maintain the integrity and reliability of the data processed through Microsoft Dynamics Finance and Operations.

III. **Compliance**: The policy aligns with regulatory requirements and organizational standards, ensuring that access rights are managed in a manner that meets legal and operational obligations.

IV. **Review Mechanism**: Establish a framework for periodic review of user access rights, ensuring they remain appropriate based on role changes, employment status, or operational needs.

Overall, this policy serves to reinforce North South Power's commitment to security and data protection while optimizing the functionality of its ERP system.

2.0 Scope

This policy applies to all employees, contractors, vendors, and any other individuals with access to North South Power's Enterprise Resource Planning System.

3.0 Definitions

- User: An employee, contractor, vendor or any other individual granted access to North South Power's Enterprise Resource Planning system
- Least Privilege: The principle that users are granted the minimum level of access necessary to perform their job role effectively.
- ERP: Enterprise Resource Planning
- UAR: User Access Review
- IT: Information and Technology

4.0 Roles and Responsibilities

<u>ERP Administrator</u>

- The ERP administrator is responsible for the overall management, configuration, and maintenance of the ERP.
- The ERP administrator is responsible for updating user access privileges as directed by either the user's manager, human resources and internal audit.

Commented [OA3]: Is this a joint responsibility or is it either of them?

Heads Of Department

- The head of department is responsible for identifying the access needs of their team members and submitting access requests to the ERP administrator.

Human Resources

- The Human Resource department is responsible for informing the ERP administrator of any changes in job roles or termination of an employee so that access rights can be changed appropriately.

Authorized users

- Users must comply with this policy and use their access rights responsibly and solely to perform their official duties.
- Users must report any suspicious activities or potential security incidents to the IT security team.
- The IT Team should keep the Log of all reported cases.

5.0 User Access Requests

- Access requests will be sent via email.
- Access requests will detail the user's name, email address, job role & description, requested access/privileges.

5.1 User Access Pre - provision Review

- Confirm that the access request is in line with the user's job role & description
- Approval is granted by Head of ITSC for the access provisioning

5.2 Access provisioning

- Upon receiving approval, the ERP administrator shall grant employee access and assign the approved privileges.

5.3 User Access Rights

- Users will be granted the minimum level of access necessary to perform their job role.
- Access rights will be periodically reviewed and adjusted as job roles change.
- No single user should be able to perform a critical process end-to-end without oversight.

5.4 User Access Revocation

- User Access will be removed when the Human Resource department informs the ERP administrator of the exit of any employee.
- Access right may also be temporary suspended when a staff is under certain level of disciplinary action that his/her continued access right may jeopardize the interest of the company.
- Access rights may be temporarily delegated to another staff member when a user is on an extended, approved absence. The delegation request is initiated by the user and must be approved by both the line manager and Internal Audit.

6.0 User Access Reviews:

A User Access Review (UAR) is part of the User Account Management and Access Control Process, which involves periodically reviewing access rights for all North South Power Company Limited (NSPCL) employees and third parties.

The IT Department in collaboration with the Internal Audit & Risk Management Department will perform Periodic Access Reviews to ensure that user rights are appropriate and up to date. During the access review, the UAR Anchors shall be referred to as User Access Security Officers. The User Access Security Officers shall synchronize all Users' Access Rights with the Users' Current Roles respectively and limits employees' privileges to keep the risks of privilege creep, misuse, and abuse at a minimum.

Commented [OA4]: I think this should be specific. i.e quarterly, biannually or annual reviews

Below is the RACI matrix[1] that identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformedfor every task that shall be performed in the UAR Process:

Commented [OA5]: Is this footnote for the table?

S/N	Task Group	UAR Anchors	HR Dept.	User	Mgmt.	User's HOD
1.	Schedule Review	R, A	I	I	C, I	I
2.	User Access Review Scope Definition	R, A	I	I	C, I	I
3.	As-it-is Assigned User Rights and Privileges Report Generation	R, A			I	
4.	Send As-it-is Assigned User Rights and Privileges Report to Owners	R, A		C	I	I
5.	Owners Approve or Deny Access	R, I	I	R, A	I	C, I
6.	As-it-is Assigned User Rights and Privileges Report Review and Evaluation	R, A	C	R, A	C, I	C, I
7.	Remove Shadow Admin Accounts	R, A			C, I	
8.	To-be Assigned User Rights and Privileges Analysis and Approval	R, A	C, I	C, I	R, A	C, I
9.	Change or Resolve User Privileges	R, A	I	I	C, I	I
10.	Ensure Changes and updates are properly Implemented	R, A	I	I	C, I	I
11.	Necessary Permanent Access Verification	R, A	I	I	C, I	I
12.	Analyze the Result of the User Access Review Exercise	R, A	I	I	R, A	I
13.	User Access Review Management Report	R, A	I	I	C, I	I

7.0 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.