



## USER ACCOUNT MANAGEMENT POLICY AND PROCEDURES

JUNE 2025

**DOC POLICY NO:**


-----  
**Developed By**  
-----

**Assistant General Manager, Information Technology and Security Compliance**

---


### Executive Summary

Effective user account management is crucial to ensuring the confidentiality, integrity, and availability of NSPCL's IT systems and data. This policy establishes clear guidelines and responsibilities for creating, modifying, monitoring, and terminating user accounts, with a focus on Microsoft 365 and Microsoft Dynamics 365 for Finance and Operations. This policy aligns with other NSPCL policies including RBAC, Password, Data Protection, and Information Security.

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO: DATE OF ISSUE: REVISED DATE: <b>N/A</b>
	DOCUMENT TITLE: <b>USER ACCOUNT MANAGEMENT POLICY AND PROCEDURES</b>	

**Table of Contents**

1.	Purpose .....	3
2.	Scope .....	3
3.	Policy Statements .....	3
4.	Roles and Responsibilities .....	3
5.	Account Creation Procedures .....	4
6.	Account Management Procedures .....	4
7.	Account Termination Procedure .....	5
8.	Account Control and Monitoring .....	5
9.	Security and Compliance .....	5
10.	Training and Awareness .....	6
11.	Review and Revision .....	6

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO: DATE OF ISSUE: REVISED DATE: <b>N/A</b>
	DOCUMENT TITLE: <b>USER ACCOUNT MANAGEMENT POLICY AND PROCEDURES</b>	

### 1. Purpose

The purpose of this policy is to provide guidelines and procedures for the management of user accounts within North South Power Company Limited (NSPCL) and its subsidiaries. This ensures the security, integrity, and proper use of NSPCL's IT resources, including Microsoft 365 and Microsoft Dynamics 365 for Finance and Operations.

### 2. Scope

This policy applies to all employees, contractors, and third-party users who have access to NSPCL's IT systems, networks, and data, specifically focusing on Microsoft 365 and Microsoft Dynamics 365 for Finance and Operations. This policy compliments the RBAC Policy, Data Protection and Privacy Policy, Password Policy, Data retention policy and Information Security Policy

Commented [OA1]: Are these pre-existing policies?


### 3. Policy Statements

- **Account Creation:** User accounts will be created based on the principle of least privilege, granting the minimum level of access necessary for users to perform their job functions.
- **Account Management:** All user accounts shall be managed in accordance with this policy to ensure security and compliance with regulatory requirements.
- **Access Control:** Access to IT resources shall be controlled and monitored to prevent unauthorized access and ensure data integrity.
- **Account Termination:** User accounts shall be promptly disabled or deleted when no longer needed or when a user exits the organization.

### 4. Roles and Responsibilities

- **IT Department:** Responsible for creating, managing, and terminating user accounts, as well as monitoring access and ensuring compliance with this policy.
- **Head of Departments/Supervisors:** Responsible for approving account creation requests and ensuring that access levels are appropriate for their team members.
- **Users:** Responsible for using their accounts in accordance with all related NSPCL's IT policies and reporting any suspicious activity or security incidents.

Commented [OA2]: Delete


	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO: DATE OF ISSUE: REVISED DATE: <b>N/A</b>
	DOCUMENT TITLE: <b>USER ACCOUNT MANAGEMENT POLICY AND PROCEDURES</b>	

#### 5. Account Creation Procedures

- **Request Submission:** HODs shall submit a user account creation request to the IT department with the Internal Audit and Human Resources Departments in Copy, specifying the required access levels and any special permissions.
- **Approval:** The IT department will review the request in collaboration with the Internal Audit (in the case of any Special or Elevated Permissions) and verify that the access levels are appropriate. If approved, the account will be created.
  - **Notification:** New User and his/her HOD will be notified once the account is created and ready for use.
  - **Account Setup:** The IT department will set up the user account, including assigning a unique username, initial password, and appropriate access permissions.
  - **Microsoft 365:** Set up email, OneDrive, SharePoint, Teams, and other relevant applications.
  - **Microsoft Dynamics 365 for Finance and Operations:** Assign roles and permissions based on the user's job function.
- **Notification:** New User and his/her HOD will be notified once the account is created and ready for use.

#### 6. Account Management Procedures

- **Password Management:** Users shall change their initial password upon first login and follow NSPCL's password policy.
- **Access Reviews:** HODs and the IT department in collaboration with the Internal Audit and Risk Management Department shall conduct regular reviews of user accounts to ensure that access levels remain appropriate and that inactive accounts are disabled.
- **Account Modifications:** Changes to user account permissions shall be initiated by the user through the user's HOD and reviewed by the Internal Audit department before implementation by the IT Department.
  - **Microsoft 365:** Adjust access to applications and data as needed.
  - **Microsoft Dynamics 365 for Finance and Operations:** Modify roles and permissions based on changes in job functions.

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO:
	DOCUMENT TITLE: <b>USER ACCOUNT MANAGEMENT POLICY AND PROCEDURES</b>	DATE OF ISSUE: REVISED DATE: <b>N/A</b>

#### 7. Account Termination Procedures


- **Notification:** The HR Department shall notify the IT department immediately if a user exits the organization or no longer requires access to certain IT resources.
- **Account Deactivation:** The IT department will promptly deactivate the user account to prevent unauthorized access.
  - **Microsoft 365:** Disable email and access to other applications.
  - **Microsoft Dynamics 365 for Finance and Operations:** Revoke roles and permissions.
- **Data Retention:** Any data associated with the terminated account will be retained or transferred in accordance with NSPCL's data retention policy.
- **Account Deletion:** After a specified retention period, the user account and associated data will be permanently deleted.

#### 8. Access Control and Monitoring

- **Access Control:** Access to IT resources will be controlled using unique user accounts, passwords, and role-based access controls.
- **Microsoft 365:** Utilize Azure Active Directory for identity and access management.
- **Microsoft Dynamics 365 for Finance and Operations:** Implement role-based security to control access to data and functions.
  - **Monitoring:** The IT department will monitor user account activity to detect and respond to any unauthorized access or suspicious behavior.
  - **Audit Logs:** All access and account management activities will be logged and retained for audit purposes.

#### 9. Security and Compliance

- **Security Measures:** User accounts shall be protected by strong passwords, multi-factor authentication, and other security measures as deemed necessary by the IT department.
  - **Microsoft 365:** Enforce multi-factor authentication and conditional access policies.
  - **Microsoft Dynamics 365 for Finance and Operations:** Implement security roles and segregation of duties.
- **Compliance:** All account management activities shall comply with relevant regulatory requirements and NSPCL's internal policies.

	<b>INFORMATION TECHNOLOGY AND SECURITY COMPLIANCE DEPARTMENT</b>	DOC NO: DATE OF ISSUE: REVISED DATE: <b>N/A</b>
	DOCUMENT TITLE: <b>USER ACCOUNT MANAGEMENT POLICY AND PROCEDURES</b>	

#### 10. Training and Awareness

- **User Training:** All users shall receive training on NSPCL's IT policies, including user account management and security best practices.
  - **Microsoft 365:** Training on using Outlook, Teams, SharePoint, and other applications securely.
  - **Microsoft Dynamics 365 for Finance and Operations:** Training on using the ERP system securely and efficiently.
- **Awareness Programs:** Regular awareness programs will be conducted to keep users informed about the latest security threats and best practices.

#### 11. Review & Revision

This document 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.