NORTH SOUTH POWER | COMPANY LIMITED

# Role-Based Access Control (RBAC) Policy

JUNE 2025

## Table of Contents

Commented [OA1]: Format for structure

### 1. Executive Summary

North South Power Company Limited recognizes that secure access to its digital resources is critical to business operations, data integrity, and risk management. The Role-Based Access Control (RBAC) Policy provides a structured approach to managing user access rights based on individual job responsibilities. This ensures that access to information systems and tools is granted following the principle of least privilege, which limits exposure to data breaches, misuse, and insider threats.

The RBAC framework outlined in this policy ensures that access is systematically granted, reviewed, and revoked across core platforms, including Microsoft Dynamics 365, Microsoft 365 Suite, Adobe, AutoCAD, MATLAB, Power BI, Zoom, and other licensed tools. It applies to all North South Power Company employees, contractors, and authorized third parties.

By enforcing clearly defined access levels and responsibilities, North South Power Company aims to:

- Reduce the risk of unauthorized data exposure,
- Maintain compliance with internal and external requirements,
- Improve operational efficiency and data accuracy.

### 2. Purpose

The purpose of this policy is to implement a structured and consistent model for managing user access rights within North South Power Company Limited. This model ensures users are granted only the level of access necessary for their job functions — in line with the **Principle of Least Privilege (PoLP)** — and that all access is periodically reviewed and revoked when no longer required.

### 3. Scope

This policy applies to:

- All employees, contractors, interns, and third-party users who access North South Power Company's digital resources. The following information systems, platforms, and licensed tools:
- Microsoft Dynamics 365 for Finance and Operations
- Microsoft 365 Suite (Outlook, SharePoint, OneDrive, Excel, PowerPoint, Word, Teams, Engage, etc.)
- Adobe Acrobat Professional

- Corel Draw
- AutoCAD
- Microsoft Project
- Microsoft Visio
- MATLAB
- Power BI
- Zoom

## 4. Policy Statement

North South Power Company Limited is committed to ensuring a secure, controlled environment where user access is based strictly on organizational roles and responsibilities. To achieve this, the organization will:

- Define and document role-based permissions for each functional area.
- Assign access rights using a standardized matrix.
- Restrict access to only the tools and features necessary for task completion.
- Audit and review user access periodically.
- Revoke access promptly upon role change, resignation, or contract termination.
- Provide training and awareness on proper access use.

## 5. Roles and Responsibilities

| Stakeholder | Responsibilities |
|---|---|
| IT Security Team | Manage and enforce access controls; implement technical configurations; maintain logs. |
| Department Heads | Identify job roles and corresponding access needs; approve or deny access requests. |
| HR Department | Inform IT of personnel changes affecting access (e.g., onboarding, transfer, exit). |
| System Owners | Define access requirements specific to their applications and review access logs. |
| All Employees | Use access responsibly and report unauthorized access or suspicious activities. |

### 6. Access and Permissions by Role

#### a) Executive Management

**Roles:** CEO, ED, Directors, and C-level Executives
**Permissions:**

**Commented [OA2]:** This is not how they are defined in the conditions of service.

- **Dynamics 365:** Management oversight and approval modules
- **Microsoft 365:** Outlook, Excel, SharePoint, Teams etc
- **Adobe Pro:** Financial document handling
- **Zoom:** Virtual meetings
- **BitDefender GravityZone:** Client Side

#### b) Finance Team

**Roles:** Accountants, Financial Analysts, AR/AP Clerks, GL Accountants, Budget/Cost Managers
**Permissions:**

**Commented [OA3]:** Are these roles relevant to NSP

- **Dynamics 365:** Accounting, budgeting, reporting modules
- **Microsoft 365:** Outlook, Excel, SharePoint, Teams etc
- **Power BI:** Dashboard/report access
- **Zoom:** Virtual meetings
- **BitDefender GravityZone:** Client Side

#### c) Operations Team

**Roles:** Operations Managers, Engineers, Production Staff, Maintenance
**Permissions:**

- **Dynamics 365:** Inventory, procurement, supply chain modules
- **Microsoft 365:** SharePoint, Teams, Outlook, Excel etc
- **Power BI:** Operational reports
- **Adobe Pro:** ES & CD
- **AutoCAD:** Draughtsmen only
- **MATLAB:** CTO Office only
- **BitDefender GravityZone:** Client Side

**d) IT Team**

**Roles:** Admins, Developers, Support Engineers
**Permissions:**

- **Dynamics 365:** Admin-level access
- **Microsoft 365:** Admin privileges, backups, user management
- **Visio, Corel Draw, AutoCAD, MATLAB:** Admin/design use
- **Microsoft productivity tools:** Admins & Developers
- **Adobe Acrobat Professional:** Admins & Developers
- **BitDefender GravityZone:** Server & Client Side

**e) HR Team**

**Roles:** HR Managers, Recruiters, Training Managers, Analysts
**Permissions:**

- **Dynamics 365:** HR modules
- **Microsoft 365:** Engage, Outlook, SharePoint, Teams
- **Adobe Pro:** HR documentation
- **BitDefender GravityZone:** Client Side

**f) Project Management Team**

**Roles:** PMs, Coordinators, Analysts, QA Managers
**Permissions:**

- **Microsoft Project, Visio:** Project planning
- **Dynamics 365:** Project Management and Accounting modules
- **Microsoft Teams:** Collaboration and communication
- **BitDefender GravityZone:** Client Side

**g) Supply Chain Management**

**Roles:** Procurement, Inventory, Warehouse, Logistics
**Permissions:**

- **Dynamics 365:** Procurement & sourcing, product info
- **Microsoft 365 + Microsoft Project:** Coordination tools
- **BitDefender GravityZone:** Client Side

### h) Internal Audit, Risk Management, and Tax

**Roles:** Auditors, Compliance Officers, Tax Analysts
**Permissions:**

- **Dynamics 365:** Procurement & sourcing, product info
- **Microsoft 365 + Microsoft Project:** Coordination tools
- **BitDefender GravityZone:** Client Side

### i) General Access – All Employees

**Roles:** General staff (system users)
**Permissions:**

- **Microsoft 365:** Outlook, SharePoint, Teams
- **Dynamics 365:** Self-service portal access only
- **BitDefender GravityZone:** Client Side

## 7. Access Levels and Controls

Each system and tool under North South Power Company's environment shall implement standardized access levels as follows:

| Access Level | Description |
|---|---|
| Read-Only (RO) | Users may view content but cannot modify, delete, or share data. |
| Read-Write (RW) | Users may view and edit content, generate reports, or collaborate actively |
| Admin | Users have administrative privileges including configuration changes. |

**Controls to Enforce Access Levels:**

- Role mapping in Active Directory and Microsoft Entra ID.
- System-specific access groups for quick provisioning and de-provisioning.
- Multi-factor authentication (MFA) enforced on accounts with Full Control.
- Audit logging enabled on all tools for Read-Write and Full Control users.

## 8. Implementation Procedures

### a. Role Mapping and Configuration

1. **Identify Roles:** Based on job descriptions provided by HR and department heads.
2. **Assign Permissions:** Refer to the Role-Permission Matrix (Appendix A).
3. **Provision Access:** Configure access in each system using native RBAC features (e.g., Azure AD groups, D365 security roles).
4. **Document Access Rights:** Maintain a central access log with date of provisioning, reviewer, and expiration timeline.

### b. User Onboarding

- New users will receive access based on their job function and department.
- Provisioning requests must be formally initiated by HR and approved by department heads.
- Access will be granted within 2 business days of receiving complete documentation.

### c. User Offboarding

- Access is revoked within 24 hours of resignation, contract end, or termination.
- IT must receive a formal offboarding checklist from HR.
- Shared credentials must be changed and audit logs reviewed for anomalies.

### d. Role Changes and Transfers

- All internal transfers require an access review.
- Access to previous roles must be revoked before granting new access.
- Temporary dual access may be granted for handover (maximum of 5 working days).

### 9. Monitoring and Auditing

To ensure compliance and identify any violations or anomalies:

#### a. Access Log Reviews

- Logs are automatically generated for login attempts, file access, and configuration changes.
- Reviewed monthly by the IT Security team.

#### b. Periodic Access Reviews

- **Quarterly audits** are conducted for all departments.
- Department heads must confirm that users under them still require access.
- Inactive accounts are flagged and suspended until reviewed.

#### c. Exception Management

- Any user requesting access beyond their defined role must submit an Exception Request Form.
- Exceptions must be time-bound and reviewed monthly.

#### d. Reporting

- All violations of access control policy are reported to Internal Audit.
- Serious violations are escalated to HR and Executive Management for disciplinary action.

### 10. End-User Guidelines

All users are expected to:

- Access only systems/tools required for their duties.
- Refrain from sharing credentials or using another user's account.
- Report suspicious access or unusual system behavior immediately.
- Log out of systems after each session, especially on shared devices.
- Use VPNs when accessing systems from outside the corporate network.

Training will be provided:

- At onboarding.
- When assigned new tools or elevated permissions.
- Annually, as part of IT compliance refresher courses.

### 11. Third-Party Access Considerations

North South Power Company occasionally grants temporary access to third-party vendors, consultants, or auditors. All third-party access must:

- Be sponsored by an internal staff member.
- Be provisioned using time-bound access rights (no more than 30 days).
- Be governed by a signed **Third-Party Access Agreement** including NDAs and security responsibilities.
- Be monitored and logged throughout the duration of engagement.
- Require use of North South Power Company's secure connection tools (VPN, encrypted communication).

IT must disable all third-party accounts upon project completion/contract expiry.

### 12. 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.