EMPLOYEE EXIT AND ACCESS DEPROVISIONING

POLICY AND PROCEDURE

JUNE 2025

DOC POLICY NO:

Developed By

Assistant General Manager, Information Technology and Security Compliance

Executive Summary

North South Power Company Limited is committed to ensuring the secure and orderly transition of exiting employees through a robust Employee Exit and IT Access Deprovisioning Policy and Procedure. This policy protects company assets, safeguards sensitive data, and maintains operational integrity by outlining clear steps for managing employee departures and deprovisioning IT access. The policy addresses various exit scenarios, including resignation, retirement, termination, and death, and emphasizes the secure backup of employee data to designated Microsoft SharePoint and OneDrive locations. Compliance with this policy is mandatory for all employees and contractors, ensuring a secure and seamless transition of responsibilities and the continued protection of North South Power Company Limited's information assets. By adhering to this policy, the company aims to mitigate risks associated with employee departures and maintain a resilient IT environment.

Table of Contents

1. Purpose

This policy outlines North South Power Company Limited's procedures for managing employee exits and deprovisioning IT access, irrespective of exit type. It applies to all employees, contractors, and third-party personnel with access to the company's digital assets regardless of their position or employment status. Its purpose is to:

- Ensure consistency and security in the exit process.
- Protect sensitive data and IT systems from unauthorized access.
- Comply with legal and regulatory obligations.
- Facilitate project continuity through seamless handovers.
- Secure and archive important employee data for future reference.

2. Scope

This policy applies to all employees, contractors, and other personnel who have access to the company's IT systems, data, and software, including but not limited to Microsoft Dynamics 365 for Finance and Operations (MsD365FO), Microsoft 365, AutoCAD, CorelDraw, and MATLAB.

3. Responsibilities

- **Human Resources (HR)**
  Responsible for managing the overall exit process, including resignation acceptance, exit interviews, communication with relevant departments, and managing legal requirements depending on the exit reason.

Commented [OA1]: @Olawale Aro Is it okay for Hr to manage legal requirements? I suggest with consultation from the Legal Department

Commented [AJ2R1]: HR helps in initiating the exit process

- **Information Technology (IT)**
  Responsible for deprovisioning employee IT access, ensuring data security, assisting with asset recovery, and managing data migration/retention according to this policy.

- **Finance & Administration (FO&A)**
  Responsible for settling any outstanding financial matters with the employee or their family/Next-of-Kin (in the case of death).

- **Employee's Manager**
  Responsible for initiating the exit process, recovering company assets, ensuring a smooth handover of responsibilities, identifying critical data for backup, and collaborating with IT on data migration.

4. Procedure

The core steps outlined below apply to all exit methods, with specific adaptations noted for resignation/retirement vs. termination/death.

4.1 Initiation of Exit Process

a. **Resignation/Retirement:** The employee submits a formal resignation or retirement letter to HR, including their intended last day of employment.

b. **Termination:** HR, in consultation with the employee's manager, initiates the termination process according to company policy and legal requirements.

c. **Death:** Upon notification of an employee's death, HR initiates the exit process with sensitivity and respect, following established procedures for handling such situations, including legal and beneficiary considerations.

4.2 Acknowledgment and Exit Form

a. **HR Acknowledges:** HR acknowledges the resignation, retirement, termination, or, in the case of death, proceeds according to established protocols. An exit form is initiated. This form includes sections for asset return, IT access deprovisioning, data backup verification, and final settlement details.

Commented [OA3]: Is there an exit form?

4.3 Recovery of Company Assets

a. **Asset Recovery Begins:** The employee's manager initiates the recovery of all company assets. This includes:

- Laptops, mobile devices, software licenses and other company-owned hardware.
- Access cards and security badges.
- Any other company-owned property.
- *In the case of death, HR and the manager will work with the employee's family/estate to recover assets sensitively.*

4.4 Data Backup and Migration

a. **Data Identification:** The employee's manager, in consultation with IT, identifies critical data requiring backup and migration. This includes:

- Files and documents stored on the employee's local machine.
- Data within Microsoft 365 applications (OneDrive, SharePoint, Teams, Outlook).
- Files and projects within AutoCAD, CorelDraw, MATLAB, and other relevant software.
- **Important:** For sensitive data, ensure compliance with data privacy regulations (NDPR).

Commented [OA4]: What is Sensitive data?

b. **Data Backup to Designated Locations:** The employee (during resignation/retirement) or IT (during termination/death) backs up all identified data to designated Microsoft SharePoint and OneDrive locations.

- *Specific SharePoint sites and OneDrive folders will be designated for archiving departing employee data.*

c. **Backup Verification:** IT verifies the successful completion of the data backup.

4.5 Clearance Process

a. **Departmental Clearance:** Employee's manager, FO&A, Audit, IT, and HR must clear the employee. This includes verifying asset returns, settling any outstanding financial obligations, confirming IT access deprovisioning, and data backup verification.

b. **If Clearance is NOT Complete:** If any department has not cleared the employee, the process loops back to the appropriate step (Asset Recovery, Data Backup) until all clearances are obtained.

4.6 IT Access Deprovisioning

a. **IT Access Revoked:** Once clearance is received, IT immediately revokes all IT access for the departing employee. This includes:

- Disabling network accounts and email access.
- Revoking access to all Microsoft 365 applications (Teams, SharePoint, OneDrive, Outlook).
- Revoking access to Microsoft Dynamics 365 for Finance and Operations (MsD365FO).
- Revoking access to AutoCAD, CorelDraw, MATLAB, and other relevant software.
- Revoking antivirus licence.
- Removing VPN access.
- Changing passwords for any shared accounts the employee had access to.
- Disabling multi-factor authentication (MFA).

b. **Employee De-provisioned:** IT de-provisions the employee from all relevant IT systems.

4.7 Exit Form Completion

a. **Exit Form Returned:** The employee (or their representative in the case of death) returns the duly signed exit form to HR, confirming that all assets have been returned, data backup has been completed, and they understand their obligations regarding company data and confidentiality.

4.8 Final Steps

a. **Exit Notification:** HR sends a notification email to relevant stakeholders (e.g., team members, other departments) about the employee's exit. The duly signed exit form is attached to the email.

b. **Final Settlement:** FO&A settles all final payments with the employee or their estate (in the case of death), including outstanding salary, benefits, and expense reimbursements.

c. **Exit Interview (Optional):** HR conducts an exit interview with the employee (where applicable) to gather feedback and insights.

d. **Final Letter:** A final letter is provided to the employee (or their representative in the case of death) by HR.

4.9 Special Considerations for Death

a. **Sensitivity:** All communication and actions will be conducted with the utmost sensitivity and respect.

b. **Legal Compliance:** HR will ensure compliance with all applicable laws and regulations regarding employee death, including notifying relevant authorities and handling beneficiary matters.

Commented [OA5]: include with consultation from the legal department

c. **Data Access:** Access to the employee's data will be handled according to legal requirements and company policy, in consultation with legal counsel.

5. Data Security

- All data must be backed up to designated Microsoft SharePoint and OneDrive locations before IT access is revoked.
- IT will conduct a final data wipe on all returned devices.
- Access to the archived data will be granted to the employee's manager and other designated personnel as needed.
- Data retention policies will apply to the archived data in SharePoint and OneDrive.

6. Compliance

Non-compliance may result in disciplinary measures, up to termination of employment or contract.

Commented [OA6]: Non-compliance by employee exiting or by the ITSC department?

Commented [OA7]: I am not certain about this as the consequence of non-compliance, because the employee is already in the process of exiting the company. I suggest that non-compliance may lead to delays in final settlements or something else. @Olawale Aro

Commented [AJ8R7]: Are records of deprovisioning actions logged and auditable?

7. Communication

This policy will be communicated to all employees upon hire and made available on the company intranet.

8. Policy Review

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.