Standard Operating Procedure (SOP) for Handling Network Account Needs for Terminated Employees

Objective

To promptly and securely remove network access and account privileges for terminated employees, protecting sensitive data and ensuring compliance with company policies.

Procedure

Notification of Termination

- HR Notification:
  - HR must notify the IT department of the employee's termination as soon as possible and provide the termination date.
- Request Details:
  - HR provides IT with details regarding the employee's role and the specific systems and access privileges the employee had.

Account Deactivation

- Immediate Deactivation:
  - On the date of termination, IT must immediately deactivate the employee's network account, including email, VPN, and other access points.
- Access Revocation:
  - Disable access to all systems, applications, and data storage the employee had privileges to.
  - Revoke access to any shared drives or folders the employee had permissions for.
- Multi-Factor Authentication (MFA) Removal:
  - Disable or remove the terminated employee’s MFA access (e.g., authenticator apps or tokens) to prevent unauthorized access.

Data Handling and Transfer

- Data Backup and Transfer:
  - Assess and back up any work-related data from the terminated employee's account.
  - Transfer ownership of work-related data (emails, files, folders) to the employee's supervisor or another designated employee.
- Data Privacy:

        - Ensure that the terminated employee's personal information and non-work-related data are handled confidentially and securely.

Asset Retrieval

- Hardware Collection:
    - Coordinate with HR to retrieve company-owned hardware (e.g., laptops, mobile devices) from the terminated employee.
- Software Deactivation:
    - Deactivate any licensed software or applications registered to the terminated employee.

Communication

- Internal Notification:
    - Notify the relevant teams or departments of the termination and changes to access rights.
- External Communication:
    - Remove or update any external contact details (e.g., email address) associated with the terminated employee.

Documentation

- Record Changes:
    - Document all account deactivation actions taken, including the time and date.
- Maintain Logs:
    - Maintain logs of all changes for audit and compliance purposes.

Review and Verification

- Confirmation:
    - Verify that all steps in the process have been completed.
- Audit:
    - Conduct regular audits to ensure all terminated employee accounts have been properly deactivated and access revoked.

By following this SOP, you can ensure that network account needs for terminated employees are handled in a secure and efficient manner, protecting sensitive data and maintaining network integrity.