Termination of Employee SOP

Purpose

To define a secure, standardized process for handling IT tasks associated with employee termination. This ensures timely revocation of access, data protection, and operational continuity in compliance with company policy and data security standards. This procedure applies to all employees, contractors, interns, and external users whose employment or engagement has ended, either voluntarily or involuntarily.

1. Pre-Termination (For Planned Separations Only)
2. Inventory all devices assigned to the user, review active accounts, and list any shared access or privileged roles.
3. Open an internal IT ticket with the due date/time to match the employee’s termination date/time.
4. Day of Termination
5. Immediately revoke access exactly at termination time.

* Disable Microsoft 365 account
* Terminate VPN access and revoke tokens
* Disable access to internal systems, SaaS platforms, and admin panels.
* Disable access to mobile device management tools
* Revoke SSO credentials

1. Trigger remote lock or wipe of devices.
2. Transfer ownership of OneDrive/SharePoint files, email inbox, and shared folder permissions. Backup critical emails or project data before disabling mailbox.
3. Confirm collection or shipment of laptop/desktop, mobile device, badge/access cards, USB drives and external media, and hardware tokens or authentication devices.
4. Post-Termination
5. Removes licenses from Microsoft 365 and other platforms.
6. Archive or delete mailbox according to retention policy.
7. Remove user from email groups, Teams, and shared calendars.
8. Close termination ticket, document exceptions, and notify supervisor of any issues requiring escalation.
9. Special Cases
10. Involuntary Termination

* Complete all revocations before notifying the employee.
* Involve HR and Security to ensure device lockout and physical access control.

1. Offboarding Admin/Privileged Users

* Change all shared credentials the employee had access to.
* Review logs for suspicious activity in the past 30 days.

Retain termination logs for minimum one year or as required by HR. Ensure alignment with the Acceptable Use Policy, Care and Retention of Records Privacy Policy, and Incident Response Policy. This SOP should be updated at least annually.