

User Deactivation and Termination Checklist

Enterprise IT

Employee Information

Name		Employee ID	
Department		Last Working Day	
Manager		Date Completed	

Pre-Deactivation Steps

- Receive formal termination notice
- Confirm last working day with HR/manager
- Notify IT support and relevant teams

Account & Access Deactivation

- Disable network (Active Directory, LDAP) account
- Block email account and set auto-reply (if required)
- Revoke VPN, remote access, and Wi-Fi privileges
- Remove or transfer shared folder and file access
- Reassign or backup mailbox and OneDrive/Google Drive files
- Disable access to enterprise applications (CRM, ERP, HRMS, etc.)
- Remove from telephone and collaboration tools (Teams, Slack, etc.)
- Revoke privileged or admin accounts/tokens

Device & Asset Collection

- Recover laptops, desktops, tablets, smartphones
- Collect ID badges, access cards, security tokens
- Recover peripherals: docking stations, keyboards, mice
- Revoke access to BYOD if applicable

Final Actions & Documentation

- Change door/password codes if necessary
- Remove from mailing lists and group communications
- Document account closure and actions completed
- Notify HR and manager of checklist completion
- Archive logs and access rights records

Checklist Completion

Completed by		Date	
Signature			

