

Information Security Offboarding Policy

(Classification and Handling -Safeguarding Sensitive and Confidential Information)

Version: 1.2

Proprietary Notice: This document contains proprietary information that is confidential in BPO Convergence Company. Disclosure of this document in full or in part, may result in material damage to BPO Convergence. Written permission must be obtained from BPO Convergence prior to the disclosure of this document to a third party.

Document Revision History:

Version	Date	Author	Changes Made	Reviewed By	Approval Status
1	1/1/2021	Gyan Singh	Initial creation of Environmental Security Policies and Procedures.	P.Sahoo	Approved
1.1	1/1/2022	Gyan Singh	Added flood prevention and backup power measures.	P.Sahoo	Approved
1.2	1/1/2023	Gyan Singh	Revised incident response procedures and added training requirements.	P.Sahoo	Approve

Purpose

The purpose of this policy is to ensure that all technology-related tasks during an employee's offboarding process are handled securely and efficiently, protecting the company's digital assets, data, and systems.

1. Scope

This policy applies to all employees, contractors, and temporary staff who are leaving the company, whether voluntarily or involuntarily.

2. Responsibilities

HR Department: Initiates the offboarding process and informs the IT team of the employees' departure.
IT Department: Ensures the secure deactivation of accounts, retrieval of devices, and protection of data.
Employee: Returns all company-owned devices and follows the procedures outlined for the offboarding process.

3. IT Offboarding Procedures

3.1. Account and Access Management

Deactivation of Accounts:

IT will deactivate the employees' access to internal systems, company applications, domain id and email accounts on or before the employee's last working day.

Systems include ERP, CRM, email, VPN, Domain ID file storage, and other internal tools.

Revocation of Credentials:

All credentials (passwords, PINs, 2FA tokens, etc.) will be revoked for all systems and applications accessed by the employee.

3.2. Return of Company Devices

Devices:

The employee must return all company-issued devices, including:

- Laptops, desktops, mobile phones, tablets
- External hard drives, USB drives, and other storage devices
- Security access cards, ID badges, or any other physical devices

Inspection:

IT will inspect returned devices to ensure they are in working condition.

3.3. Data Protection and Backup

Data Backup:

IT will back up any important files and documents on the employee's devices and transfer them to the appropriate team members or storage location.

Data Deletion:

Any company-related data stored on personal devices or cloud storage will be securely deleted.

Removal of Sensitive Information:

IT will ensure that no sensitive or proprietary company data remains on the employee's devices.

3.4. Software and Licenses

Software Uninstallation:

IT will uninstall all company-licensed software from the employee's devices.

License Transfer:

Software licenses owned by the company will be reassigned or deactivated for the departing employee.

3.5. Security and Compliance

Security Review:

IT will perform a final security review to ensure there are no remaining vulnerabilities or unauthorized access to company systems.

Confidentiality Reminder:

Employees will be reminded of any non-disclosure agreements (NDAs) or confidentiality obligations they signed during employment.

3.6. Exit Survey & Feedback**Technical Feedback:**

HR or IT may conduct a brief exit interview to gather feedback from the departing employee on the company's IT systems, tools, and technology infrastructure.

3.7. Final IT Audit**Audit Check:**

A final audit will be performed to ensure all company property and access rights have been properly handled. This includes checking for any remaining system access, returned devices, and completed data transfers.

4. Timeline**Week 1 (Notice Period):**

Employee and HR initiate the offboarding process. The IT team is informed, and accounts are scheduled for deactivation.

Last Day:

Return of devices, data backup, and deletion completed. Final security check and access revocation.

Week 2 (post-departure):

Any unresolved issues are addressed, and all systems and devices are fully accounted.

