Employee Offboarding - Account Procedures

Document ID: IT-ACC-006 **Last Updated:** 2024-02-10 **Owner:** IT Operations **Classification:** Internal

---

Overview

This document outlines the IT account deprovisioning procedures when an employee leaves NovaTech. Timely and complete offboarding is critical for security and compliance.

Trigger Events

Account offboarding is initiated when: - Employee resigns (voluntary termination) - Employee is terminated (involuntary) - Contractor engagement ends - Employee transitions to leave of absence >90 days

---

Timeline

Termination Type	Account Disable	Account Delete
Voluntary	Last day of employment	30 days after departure
Involuntary	Immediately upon notification	30 days after departure
Contractor	Contract end date	14 days after end date

Immediate Actions (Day 0)

HR Notification

HR notifies IT via automated Workday workflow including: - Employee name and ID - Last day of employment - Termination type - Manager name - Data retention requirements

Account Disabling

IT Security disables within 1 hour of notification: 1. Okta account (disables all SSO access) 2. VPN access 3. Email access 4. Slack account 5. Building/badge access

For Involuntary Terminations

Additional immediate actions: - Reset all passwords - Revoke all active sessions - Disable MFA devices - Document any shared account access

---

Data Handling

Email

- Manager receives delegate access for 30 days
- Auto-reply set up if requested
- Email forwarding to manager for business continuity
- Mailbox archived after 30 days (retained 7 years)

Cloud Storage

- Google Drive files transferred to manager
- Personal files identified and excluded
- Shared drive permissions updated

Code Repositories

- GitHub access revoked
- Open PRs reassigned to team members
- Personal tokens revoked

Third-Party Applications

Access revoked from all connected applications: - AWS Console - Datadog - PagerDuty - Salesforce - Notion - All other Okta-connected apps

---

Equipment Return

Required Returns

- Laptop and charger
- External monitors
- Keyboards, mice, headsets
- Security keys (YubiKey)
- Access badges

Return Process

1. Remote employees: Prepaid shipping label sent
2. Office employees: Return to IT on last day
3. Equipment must be returned within 7 days
4. Unreturned equipment may be deducted from final paycheck (where legal)

Device Wiping

All returned devices are: 1. Verified returned in IT inventory 2. Securely wiped using DoD 5220.22-M standard 3. Reimaged for reassignment or recycled

---

Manager Responsibilities

Managers must: 1. Identify critical data and knowledge transfer needs 2. Reassign ongoing projects and tasks 3. Update team documentation 4. Notify external contacts of new point of contact 5. Confirm all equipment returned

---

Checklist

IT Security Checklist

- ☐ Okta account disabled
- ☐ VPN access revoked
- ☐ Email access removed
- ☐ Slack deactivated
- ☐ GitHub access removed
- ☐ AWS access revoked

☐ All service account ownership transferred
☐ MFA devices deregistered
☐ Badge access revoked

IT Operations Checklist

☐ Shipping label sent (remote employees)
☐ Equipment returned
☐ Device wiped
☐ Asset inventory updated
☐ Software licenses reclaimed

Audit and Compliance

All offboarding actions are logged and retained for: - SOC 2 compliance: 7 years - GDPR compliance: As required by data retention policy

Quarterly audits verify: - All terminated employees are fully offboarded - No active accounts exist for former employees - Equipment is accounted for

---

Emergency Contact

For urgent offboarding (security incidents): - Security Hotline: +1-512-555-0199 - Email: security@novatech.com - Slack: #security-urgent

---

Related Documents: Exit Interview Process (HR-OFF-002), Equipment Return Policy (IT-HW-010), Data Retention Policy (COM-DP-003)