Tech River

SOMEONE JUST QUIT

10-minute IT Offboarding Checklist

When an employee leaves, their access shouldn't leave with them. Use this quick checklist to close security gaps, protect company data, and make sure nothing important walks out the door.

1. **Disable their primary account**
   Disable their Microsoft 365, Google Workspace, or other primary company login as soon as their employment ends.

2. **Revoke active sessions**
   Signing out of one device isn't enough. Revoke active sessions so company accounts can't remain logged in on a personal phone, home computer, or browser.

3. **Remove access to business applications**
   Think beyond email. Remove or transfer access to:
   - CRM and accounting software
   - File storage and collaboration tools
   - Project management platforms
   - HR and payroll systems
   - Industry-specific applications
   - VPN and remote access tools

4. **Reset shared passwords**
   Did they know the password to a shared account, vendor portal, Wi-Fi network, or other system? Change it. Better yet, replace shared credentials with individual user access wherever possible.

5. **Secure company devices**
   Collect laptops, phones, tablets, security keys, access cards, and other company-owned equipment. Confirm devices are returned, locked, and ready to be wiped or reassigned.

6. **Protect their email**
   Block sign-in, preserve the mailbox according to your company's retention requirements, determine who should receive or monitor future messages, and convert to a shared mailbox to preserve the data. Don't immediately delete the account.

7. **Transfer ownership of important files**
   Identify files, folders, calendars, documentation, contacts, and other business information the employee owned. Provide someone on your team access to their One Drive, and transfer ownership before anything is deleted.

8. **Remove privileged access**
   If they had admin permissions, elevated system access, password-manager access, or access to sensitive company data, remove those privileges immediately.

9. **Check for automatic access**
   Review distribution lists, shared mailboxes, Teams or Slack groups, recurring reports, integrations, API access, and other places where access may continue automatically.

10. **Document the offboarding**
    Record what was disabled, transferred, collected, and changed, along with who completed each step. A repeatable process is much safer than relying on memory.

One more thing: timing matters

IT offboarding should be coordinated with HR and management before the employee's final access window, especially for involuntary departures. Even a short delay can leave company email, files, customer data, and systems exposed.

Not sure your offboarding process covers everything?

Tech River can help you build a repeatable onboarding and offboarding process so employee access doesn't become a security risk. Talk to our IT team at techriver.com.