Employee Offboarding Access Checklist

A checklist for removing access when an employee, contractor, administrator, or vendor contact leaves.

Purpose

This checklist helps small businesses remove access when an employee, contractor, administrator, or vendor contact leaves the company or changes roles.

The goal is to avoid forgotten access, shared password exposure, and business accounts that remain tied to people who are no longer responsible for them.

Before the exit date

When possible, prepare before the person leaves:

- Identify the person's role and access level
- Identify whether the exit is friendly, urgent, or high-risk
- Identify business systems they access
- Identify shared passwords they know
- Identify devices assigned to them
- Identify accounts where they are an owner, administrator, billing contact, recovery contact, or MFA holder
- Plan who will take over their work

Core account checklist

Review and remove or transfer access for:

- Email account
- Microsoft 365 or Google Workspace
- Entra ID, Active Directory, or local directory accounts
- VPN
- Remote desktop or remote access tools
- Password manager
- File shares and cloud storage
- Line-of-business applications
- Accounting and payroll systems
- CRM or ticketing systems
- Phone system
- Messaging and collaboration tools
- Project management tools

- Website CMS
- Domain registrar
- DNS provider
- Web hosting
- Social media accounts
- GitHub, GitLab, or source code repositories
- Backup systems
- Security tools
- Camera systems
- Firewall, switch, wireless, and network management platforms

Administrative access

If the person had administrator access:

- Disable or remove administrative roles
- Revoke sessions
- Remove MFA methods
- Rotate shared admin credentials
- Review recent administrative activity
- Confirm another authorized person has access
- Update emergency access records

Shared credentials

Rotate passwords for any shared accounts the person knew or could access. Common shared accounts include:

- Vendor portals
- Camera systems
- Wi-Fi controllers
- Firewall admin accounts
- Website admin accounts
- Social media accounts
- Shipping accounts
- Shared email inboxes
- Local administrator accounts
- Service accounts where the password was known to the person

Devices and physical items

Collect or disable:

- Laptop

- Desktop
- Mobile phone
- Tablet
- Security keys
- ID badge
- Building keys
- VPN tokens
- Company credit cards
- USB drives
- External drives
- Printed documents
- Access cards

For remote employees, document the return shipping process and deadlines.

Data transfer

Before deleting accounts, preserve business records:

- Transfer email delegation or mailbox access if needed
- Transfer ownership of documents and folders
- Transfer recurring meetings
- Transfer customer records
- Transfer project notes
- Transfer code repositories or tickets
- Preserve records required by law, contract, or company retention policy

Timing

For normal departures, access should be removed at the end of the employee's final work period.

For high-risk departures, access should be removed before notification or at the exact time of notification, depending on the situation and legal guidance.

Verification

After offboarding:

- Confirm the account cannot sign in
- Confirm active sessions were revoked
- Confirm MFA methods were removed
- Confirm shared passwords were rotated
- Confirm company devices were returned or wiped
- Confirm ownership was transferred for critical systems

- Confirm no personal email or phone number remains as a recovery method for business accounts

Documentation

Record:

- Date and time access was removed
- Person completing the offboarding
- Systems checked
- Devices returned
- Credentials rotated
- Exceptions or delayed items

Disclaimer

This starter checklist is general information, not legal advice. Adapt it to your business, contracts, regulatory obligations, and state law.