Employee Offboarding Security Checklist for Small Businesses (2026 Edition)

Use this checklist to shut down access cleanly, protect business data, and reduce the chance of lingering risk. Current guidance emphasizes promptly removing identities, credentials, roles, and entitlements when someone leaves or changes status.

Employee Offboarding Security Checklist

1. Confirm Departure Details and Offboarding Time

□ Final working date and time are documented
□ Manager and IT contact are identified
□ Offboarding actions are scheduled to match the departure time
□ Voluntary and involuntary exits are handled with the right urgency

Why this matters:
Timing matters. Access removal should be coordinated, not delayed until "later." Modern identity governance guidance treats leaver events as structured workflows tied to the employee lifecycle.

2. Disable or Block the Employee Identity Account

□ Business email account is blocked
□ Directory/SSO account is disabled
□ Password resets are forced if needed before disablement
□ Browser sessions and active sign-ins are terminated

Why this matters:
The first priority is stopping access through the user's main identity. Current guidance emphasizes managing and revoking credentials and access as part of identity lifecycle control.

3. Remove Access to Apps, Cloud Services, and Shared Resources

□ Access to Microsoft 365, Google Workspace, CRM, accounting, and line-of-business apps is removed
□ File shares, team folders, and collaboration spaces are reviewed
□ VPN, remote access, and support portals are revoked
□ Group memberships and role assignments are removed

Why this matters:
Offboarding is not complete until app and entitlement access are removed. Identity governance guidance specifically calls for managing entitlements, roles, and access packages as part of leaver processes.

4. Revoke MFA, Passkeys, Security Keys, and Tokens

□ Authenticator app registrations are removed
□ Passkeys are revoked where supported
□ Hardware security keys are collected or disabled
□ API tokens, app passwords, and other persistent credentials are revoked

Why this matters:
Modern access is no longer just username and password. Current security guidance stresses issuing, managing, and revoking identity tokens, cryptographic credentials, and related secrets.

5. Remove the Employee from the Password Manager

□ Employee account is suspended or removed from the password manager
□ Access to shared vaults is revoked
□ Recovery options tied to the user are reviewed
□ Business-owned credentials remain with the company

Why this matters:
Passwords and shared secrets are often overlooked during offboarding. Removing password manager access protects shared credentials and reduces the chance of silent retained access. 1Password's business materials emphasize centralized vault access, admin visibility, and account recovery controls for this reason.

6. Rotate Shared Credentials and Sensitive Secrets

□ Shared account passwords are changed
□ Admin or break-glass credentials are reviewed and rotated if necessary
□ Wi-Fi passwords, remote management credentials, and service account secrets are checked
□ API keys, SSH keys, and automation secrets tied to the employee are replaced

Why this matters:
Offboarding without secret rotation can leave invisible access behind. Current NIST and CSF

implementation guidance explicitly includes revoking keys, certificates, tokens, and other credentials.

7. Recover and Secure Company Devices

□ Laptop, desktop, phone, tablet, badge, and hardware keys are collected
□ Device inventory is updated
□ Remote wipe or lock is triggered if a device is not returned promptly
□ Local data on returned devices is preserved or sanitized appropriately

Why this matters:
Devices often retain sessions, tokens, cached files, and saved credentials. Current Zero Trust and identity/device guidance ties safe access to managed, known devices and secure recovery of those devices when someone leaves.

8. Transfer Business Data and Ownership

□ Email mailbox handling is decided
□ Files and documents are transferred to the manager or successor
□ Shared drives, cloud folders, and project ownership are reassigned
□ Calendars, contact lists, and business records are preserved as needed

Why this matters:
Offboarding is not only about removing access. It is also about preserving business continuity and making sure company-owned information stays available to the organization. Identity governance deployment guidance treats offboarding as part of broader access and resource continuity planning.

9. Review Email Forwarding, Auto-Login, and Hidden Access Paths

□ Email forwarding rules are reviewed and removed
□ Recovery emails or phone numbers tied to business accounts are changed
□ Saved browser passwords and synced browsers are reviewed on company devices
□ Meeting tools, chat platforms, and connected integrations are checked for lingering access

Why this matters:
Hidden persistence is a real risk. Former employees may retain access through forwarding, saved sessions, alternate recovery methods, or third-party integrations even after the main account is disabled. This is a practical extension of current identity and credential revocation guidance.

10. Review Physical Access

□ Office keys, access cards, alarm codes, and gate codes are collected or changed
□ Server room or network closet access is revoked
□ Visitor/vendor lists are updated if relevant

Why this matters:
Offboarding should address both digital and physical access. Security controls are stronger when physical and logical access changes happen together. NIST control frameworks continue to treat access management as broader than just user accounts.

11. Update HR, Licensing, and Audit Records

□ HR confirms departure status
□ Software licenses are reclaimed
□ Access removal is documented
□ Exceptions or unresolved items are logged and assigned

Why this matters:
Documentation improves accountability and helps prove that access was removed properly. Current governance guidance emphasizes workflow visibility, auditability, and review of user lifecycle actions.

12. Perform a Final Access Review

□ Manager confirms business access has been removed
□ IT confirms device and app removal is complete
□ High-risk systems are reviewed one more time
□ Shared credentials and critical systems have been rechecked

Why this matters:
One final review catches missed access, especially in smaller businesses where systems are spread across multiple vendors and tools. Current governance guidance supports access reviews and ongoing cleanup of entitlements that are no longer needed.

What To Prioritize First for Higher-Risk Exits

Disable main identity account
Terminate active sessions
Revoke MFA, passkeys, and tokens
Remove password manager access
Collect or lock company devices
Rotate shared credentials

Why this matters:
In a contentious or urgent exit, speed matters more than perfect sequencing. The objective is to cut off identity-based access first, then clean up apps, devices, and secrets immediately after. That matches current lifecycle and credential-revocation guidance.

Quick Rule of Thumb

Offboarding is not complete when the email is disabled.
It is complete when identity, device, app access, shared credentials, and business data are all accounted for.

SofTouchSystems.com
No-Surprise IT — Predictable. Proactive. Proven.