



J3 Systems Group Quick Resource

Employee Offboarding Checklist

A practical checklist for removing access when an employee leaves.

Practical guidance for small businesses and nonprofit organizations

Prepared by J3 Systems Group LLC

Overview

Employee offboarding protects business data, client information, files, email, devices, and internal systems. This checklist gives leadership a clear process to follow when access must be removed.

Who This Is For

- Business owners who need a repeatable offboarding process.
- Office managers who coordinate employee changes.
- Nonprofit leaders who need access removal to be documented.

Offboarding Checklist

Check	Review area	What to confirm
<input type="checkbox"/>	Final work date	Confirm the final work date, final access date, and whether access should end immediately.
<input type="checkbox"/>	Account status	Disable or suspend the main business account at the approved time.
<input type="checkbox"/>	Password reset	Reset the password when account access must be preserved for business continuity.
<input type="checkbox"/>	Microsoft 365 or Google access	Remove access to email, files, calendars, Teams, Drive, and other cloud services.
<input type="checkbox"/>	Group access	Remove the employee from security groups, shared mailboxes, distribution lists, shared drives, and team spaces.
<input type="checkbox"/>	Business systems	Remove payroll, accounting, customer records, ticketing, phone, and vendor portal access.
<input type="checkbox"/>	Mailbox forwarding	Review forwarding needs and confirm forwarding does not create privacy or data exposure issues.
<input type="checkbox"/>	File ownership	Transfer OneDrive, SharePoint, Google Drive, or shared drive ownership before deletion.
<input type="checkbox"/>	Company devices	Collect laptops, phones, tablets, badges, keys, chargers, and security tokens.
<input type="checkbox"/>	MFA methods	Remove personal phones, authenticators, recovery emails, and backup codes from business accounts.
<input type="checkbox"/>	Remote access	Remove VPN, remote desktop, remote support, and device management access.
<input type="checkbox"/>	Documentation	Record who completed each step, when it was completed, and where proof is stored.

Important Timing Note

For involuntary departures, same day access removal should be planned before the employee is notified whenever possible. This helps prevent accidental or intentional data loss.

When To Ask For Help



Ask for help when admin roles are unclear, business data is spread across personal accounts, access removal depends on memory, security alerts are not being reviewed, or the organization is not sure which settings are currently protecting users and files.

Quick Review

- Final access date is confirmed.
- Main account is disabled or suspended.
- Groups and shared access are removed.
- Files are transferred.
- Devices are collected.
- Completion is documented.

Conclusion

Offboarding should never depend on memory. A clear checklist helps protect data and gives leadership proof that access was removed.

Need help reviewing your Microsoft 365, Google Workspace, offboarding, or small business IT security setup?

J3 Systems Group LLC provides practical IT support, documentation, cloud administration, and security focused reviews for small businesses and nonprofit organizations.

Contact J3 Systems Group LLC to request a practical review and clear next steps.