Offboarding Checklist

A Step-by-Step Checklist for Employee Offboarding

Off-boarding is a multi-step process that ensures your company data and infrastructure is secure. The key to offboarding employees properly lies in finding areas where your process needs improvement and fixing that. This employee offboarding checklist will help you achieve just that.

☐ 01. Identity and Access Management

The first step in your off-boarding checklist starts with an HR notification.

☐ 02. Select User(s) to Deprovision

- When HR notifies you of employee(s) leaving your company, it's time to start deprovisioning those employees.
- Scheduling deprovisioning prevents you from scrambling when the ex-employee's notice period ends.

☐ 03. Select an Account Executor

- You need to select an account executor for each ex-employee.
- The account executor will become the new owner of the ex-employee's data in subsequent steps.

☐ 04. Onwership and Data Transfer

Since you've chosen an account executor, you can begin ex-employee data transfer.

☐ 05. Transfer Account Ownership

Transfer all the ex-employee's digital property to the account executor. These digital properties include sites, calendars and apps.

☐ 06. Reassign System Ownership

If the former employee was a system owner in several tools, reassign system ownership to the account executor.

☐ 07. Transfer Group Ownership and Membership

If the ex-employee owns or is a member of any important groups, transfer group ownership to your account executor. Transfer any assignments to the account executor.

☐ 08. Secure Application Data

- Transfer all app data from the ex-employee to the account executor. App data includes drive content, zoom recordings, documents, and other data.
- Place the transferred documents in a new folder titled with the ex-employee's email address. This folder should be in the account executor's drive.
- When you finish the data transfer, create an archive for your records. This is important as you can access this data if your company needs it in the future.

☐ 09. Prevent Software and Account Access

This step helps you prevent disgruntled ex-employees from tampering with files, sending unauthorized emails, stealing data or intellectual property.

☐ 10. Prevent Access From idP and SSO

- Resetting an ex-employee's password is usually the first step in preventing them from logging into their account and causing damage.
- If your company uses an IdP, log into your admin console and disable the ex-employee's account. Then, go into your Single Sign-on (SSO) tool and disable the ex-employee's account.

☐ 11. Disable Accounts Not Part of SSO

- SaaS tool providers are usually unaware that the ex-employee has lost access to your company's SSO. And that account is still active on the SaaS provider's site.
- Go in and deactivate accounts that are outside your SSO.

  For non-IT apps where ex-employees signed in and created an account. Log into the password manager, locate the various accounts and deactivate them.

☐ 12. Prevent Access to Shared Accounts (Without Directory Connection)

- If a former employee has access to a shared account, you need to revoke all existing tokens, sessions. And then create a new password.
- It's also a good time to revisit your policy on shared passwords.

☐ 13. Prevent Access Through Cookies/ Active Session

- Log out ex-employees from any current sessions. Then prevent further access by resetting sign-in cookies.
- You can also require a password on their next sign-in.

☐ 14. Inbox Access

Forward an ex-employee's emails to the account executor. This ensures your company maintains partnerships with outside vendors, handled by the old employee.

☐ 15. Hide Employees From Directory

- This prevents them from popping up when others type in their email address.
- Check all messaging apps your company uses. And hide old employees in those apps

☐ 16. Set Up an Auto-Reply Email & Delegate It To The Account Executor

- Auto-replies are important for business continuity after an employee's departure.
- Set up an auto-reply for people trying to contact the ex-employee. And provide information on who they should contact instead.
- You can delegate a user's inbox when you disable an old employee's G Suite or Office 365 email address.

Removal of Licenses and Accounts

☐ 17. Reclaim Employee Licenses

Different SaaS tools have different pricing models. Disabling access is no longer enough. To prevent paying for unused licenses, remove ex-employee's accounts.

☐ 18. Spend Management

When an employee is leaving a company, the finance department usually disables the company card held by the employee.

This action may cause the SaaS tool vendor to block access to the service when it is time for renewal.

☐ 19. Maintain an Employee File

Keep an employee file. Log all the processes you have taken after their departure in it.

☐ 20. Safe Deletion/Account Removal

- Delete the employee's accounts.
- Once you've transferred all their data, and revoked their access to your systems and infrastructure, it's time to delete their account.

☐ 21. Final Documentation

Prepare their workstation for incoming arrivals. And update your company directory to reflect their departure