BetterCloud

Offboarding Employees:

The Ultimate Checklist for Modern IT Professionals

What should a complete offboarding workflow look like?

Offboarding in the age of SaaS is more than just revoking access. There are many more steps than people often realize–steps that are critical for data security, compliance efforts, and business continuity.

Of course, every company's offboarding process will differ slightly, from the timing of certain steps to what your source of truth is. We've offboarded one million employees across 3,000 companies, and we've seen all kinds of variations. But generally speaking, these best practices will make sure that every user is fully offboarded, every time, without fail.

START FROM YOUR SOURCE OF TRUTH

Offboarding should start from your source of truth. In most cases this is your HR system. In others, this is your identity provider (IDaaS).

It's important to work with your HR/People team to map out your process. In the best case scenario, your HR system will feed directly into your identity provider (e.g., Okta, OneLogin, Active Directory) or your mail system (G Suite, Office 365).

If this is not possible, you may want to consider having the People/HR team open a ticket to notify you of a newly termed user (in JIRA, ServiceNow, etc.) or submit a form notifying you of this (e.g., Google Forms). These requests should include: whether the term is immediate or should be scheduled for a certain time, who their data should be transferred to, if mail will be forwarded, etc.

In more advanced cases, this form submission can automatically trigger an action in your IDaaS or your mail provider (e.g., G Suite). You may also want to consider creating a Slack channel for notifications during your offboarding process.

IT CHECKLIST: *The Essential Steps of a Perfect Offboarding Workflow*

STEP 0: The retrieval *(for physical security)*

Retrieve the user's machine (if applicable) and any other company-owned devices. This ensures that the departing employee does not leave, intentionally or unintentionally, with a device that belongs to the company.

STEP 1: The lockout

Lock the user out of their account and clear any associated sessions across SaaS apps. This is an important first step to take because the departing employee can still interact with email or Slack once they're gone if you fail to do this.

This step is especially important if you're dealing with a disgruntled employee. By locking them out, it prevents them from being able to take data with them or send negative messages to employees.

Recommended steps across SaaS apps:

Google: Reset password

Office 365: Reset password

Okta: Clear user session

Okta: Reset factors

Slack: Disable user

Zendesk: Sign out user

Salesforce: Freeze user

Box: Update user profile (set to "Inactive")

STEP 2: The directory cleanup

Make sure that the user is hidden in the directory so that their name will not auto-complete in emails and is not visible in any groups, calendars, etc.

This step is important for maintaining good organizational hygiene. Once it's completed, the departed user will no longer be visible in your system, which prevents confusion and keeps things orderly.

Recommended steps across SaaS apps:

Google: Hide user in directory
Google: Remove from all groups
Google: Remove all email aliases
Google: Remove from shared calendars
Google: Move to Org Unit
Office 365: Remove from all groups
Salesforce: Remove user from permission set

STEP 3: The security cleanup

Continue to clean up any security-related items for the account. This includes authentication, delegation, mail routing rules, etc.

These additional steps prevent the departing user from being able to log into their accounts. They also prevent mail from going to accounts that it should no longer be going to.

Recommended steps across SaaS apps:

Google: Delete 2-step backup codes
Google: Delete app-specific passwords
Google: Revoke delegation access
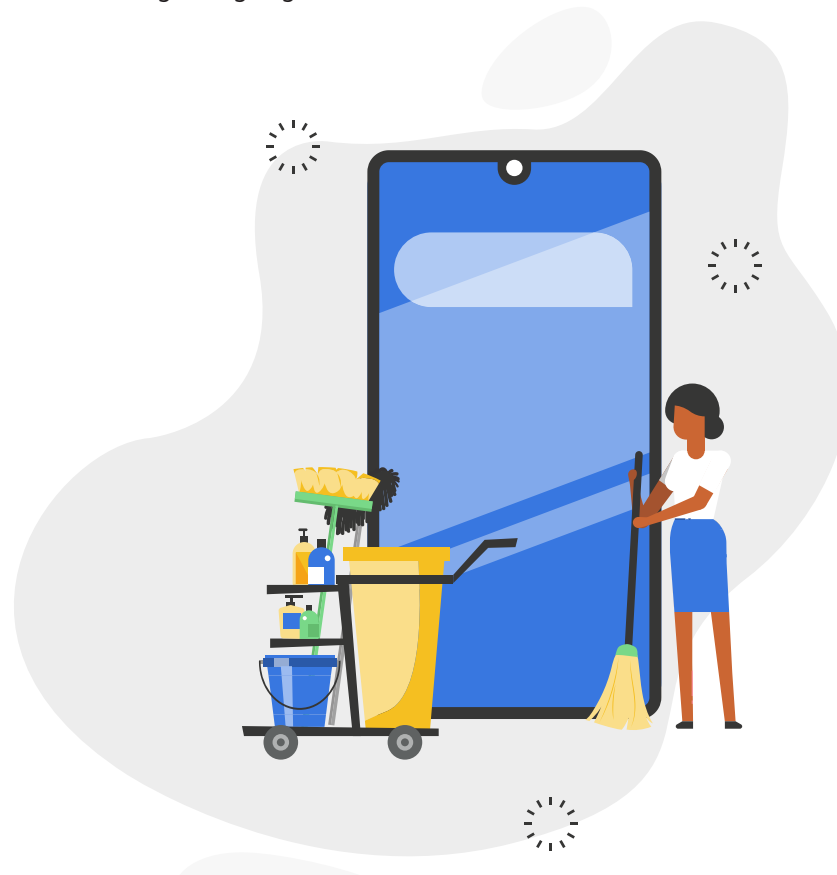**Google:** Revoke user's apps
Google: Revoke super admin privileges
Google: Disable IMAP
Google: Disable POP
Google: Disable email forwarding
Dropbox: Revoke third-party apps from user virtually

STEP 4: The devices

Clean any data off of the user's personal device across all SaaS applications. Similar to step 0, this includes actions like removing data from the departing user's device, locking them out of their company laptop, removing the MDM solution, and sending a lock command (e.g., through Jamf).

Recommended steps across SaaS apps:

Office 365: Remove devices from user

Google: Account wipe mobile device

Google: Remove device from user

Dropbox: Revoke devices from user account

STEP 5: The data transfer

Transfer any data on the account to other users within the organization. In most cases, this will be the user's manager or an archive service account (e.g., backup@bettercloud.com).

This step is critical because it preserves data for compliance reasons. It also ensures that other team members can continue working without any disruption. Additionally, this step keeps your environment clean and organized. For example, you can delete recurring calendar events and free up those resources.

Recommended steps across SaaS apps:
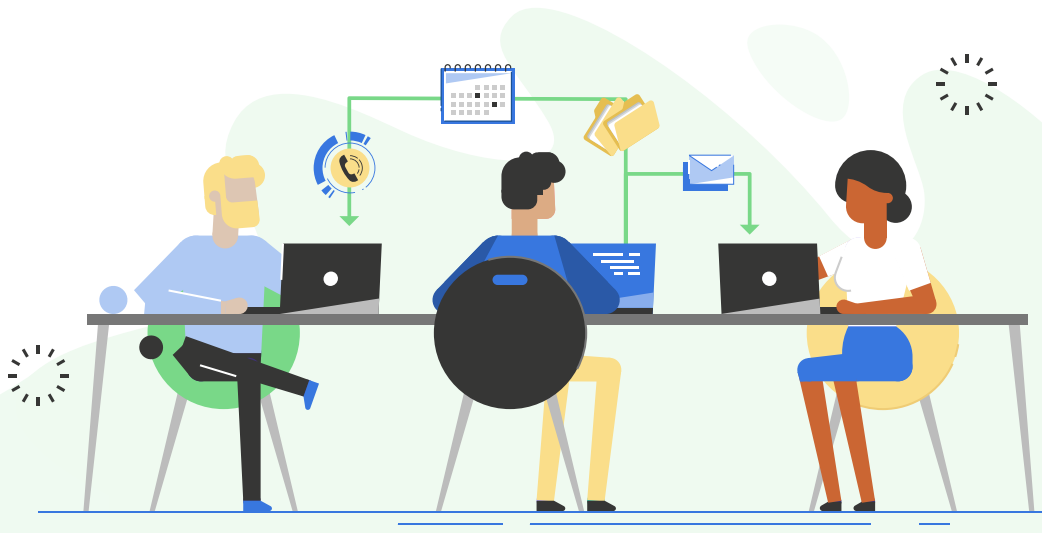
Google: Transfer Drive files

Google: Transfer primary calendar events

Google: Transfer group ownership

Google: Transfer secondary calendars

Box: Move owned items

Dropbox: Remove team member and transfer files

STEP 6: The mail routing

Decide what will happen to the user's email once they are offboarded. Who should their email be routed to? Is it okay if the mail bounces? Should there be an auto-reply in place? If you suspend an account, mail automatically bounces. If you decide to leave the account active, how do you ensure that the email is being directed to the right people?

If you do leave a Google license active, you can create an email delegation rule so that the emails will be accessible to the departing user's manager. Alternatively, you can change the departing user's primary email address and then create a (free) Google Group with their email address. This allows you to free up that license while making sure that their mail is being properly routed.

Recommended steps across SaaS apps:

Google (if active): Set auto-reply

Google (if active): Set email forward

Office 365: Set email forward

Office 365: Set auto-reply

Office 365: Change primary email address

Google: Add email alias

STEP 7: The backup *(optional)*

Take the necessary steps to back up the departing user's data. You can download all Drive data and store it using Google Takeout, Spanning, Backupify, or whatever backup system you use.

While backing up data isn't critical for your offboarding process, it's likely important for legal and/or compliance reasons.

STEP 8: The notification

Step 8 rounds out the initial offboarding. Now that these steps are complete, we recommend setting up multiple notifications before you go on to step 9. These notifications should go to the IT team as well as to the user's manager (if applicable). They should inform the team that the initial offboarding steps have been completed and when they can expect the remaining steps to be completed.

Recommended steps across SaaS apps:

Slack: Send message to channel

Slack: Send direct message

Google: Send email to group

Google: Send email to user

STEP 9: The wait

Steps 0-8 were the initial steps of offboarding; steps 10-11 are the final steps that will finish up the offboarding process. Step 9 is the period in between.

After the initial offboarding, you will likely want to keep the account active for some time (e.g., for legal hold or data retention reasons) before completely deleting it and freeing up the license.

STEP 10: The license management

Remove or add licenses, depending on what SaaS applications you use. This step ensures that you won't be paying for unused licenses.

Recommended steps across SaaS apps:

Office 365: Remove license

Google: Remove license (less common than assigning a Vault license)

Google: Assign license (e.g., Vault)

STEP 11: The deletion

The final offboarding step is to delete the accounts and free up licenses. This completes your process, and the departed user is now fully offboarded.

Recommended steps across SaaS apps:

Google: Delete user

Office 365: Delete user

Box: Delete user

Zendesk: Delete user

Dropbox: Remove team member

Salesforce: Deactivate user

How BetterCloud can help with offboarding

BetterCloud automates all of the granular actions necessary to fully offboard users and ensure corporate data is secure in the process. Our automated workflows are completely customizable to meet your company's specific requirements.

Thousands of customers rely on BetterCloud to automate their offboarding processes.
Learn:

- Why First Round Capital said, "Even if you use Okta for deprovisioning, it can't do everything you need to do. BetterCloud picks up where Okta leaves off."

- How Drivy reduced their offboarding time (per person) by 94% with BetterCloud

- How BetterCloud made offboarding "effortless" for Fullscreen Media

To learn how you can automate your offboarding process with BetterCloud, *request a demo.*

About BetterCloud

BetterCloud is the first SaaS Operations Management platform, empowering IT to define, remediate, and enforce management and security policies for SaaS applications. Over 2,500 customers in 60+ countries rely on BetterCloud for continuous event monitoring, threat remediation, and fully automated policy enforcement. BetterCloud is headquartered in New York City with an engineering office in Atlanta, GA. To learn more, *request a demo*.