Delinea

The Ultimate IT Offboarding Checklist

The employee offboarding process contains multiple stages. You can follow the recommendations of this IT offboarding checklist and create your own template to ensure you leave no stone unturned when offboarding employees.

1. Announce employee departures

Employers sometimes terminate workers privately, without alerting other team members. While this strategy may minimize disruptions, it can enable outgoing employees to continue to attend meetings, chat with team members, and request files, even as they have one foot out the door.

Because of this, make a point to formally announce departing staff. It may also help to inform team members about departing members' termination dates and the current projects they're wrapping up. This can prevent employees from exploiting colleagues who may not be aware of their expected departure.

2. Revoke or restrict privileged account access

Though rare, disgruntled departing employees may attempt to sabotage corporate resources as a means of revenge. This can significantly impact operations, damage client relationships, and cost money.

For example, an outgoing marketing employee could use a corporate social media account to post harmful materials and damage your brand reputation. Or, an IT team member like a system administrator could do even greater damage by shutting down business-critical systems operations that customers rely on.

To avoid these types of risks, immediately identify all systems they manage or have access to once you learn an employee is leaving—like applications, databases, cloud environments, or network devices. Transfer ownership to other team members and terminate their access to coincide with the departing employee's last day.

Suppose an employee will be sticking around a while after announcing their departure. In that case, you may want to add an extra layer of approvals prior to granting them access to sensitive resources. Or, you could enforce stricter rules for Multi-Factor Authentication (MFA). This ensures business continuity and adds an extra layer of security to prevent outgoing workers from inflicting harm on your organization.

During high turnover or transition, it's also a good idea to increase privileged activity session monitoring for signs of abuse. You'll want to know if employees are suddenly downloading or sharing information in large volumes, moving contacts lists to personal accounts, or sending unauthorized messages to clients or partners.

3. Block remote access

Security and IT teams sometimes overlook remote access when offboarding employees. As a result, employees are sometimes able to continue accessing private resources using VPNs and other mechanisms. Make sure you consider all the ways your employees access resources, including all identities and access management systems they use.

4. Change all passwords on shared accounts

Workers often share privileged accounts among team members, perhaps to manage rotating monitoring or maintenance responsibilities. These shared privileged accounts make it impossible to track the activity of individual users. If your organization uses shared accounts, make sure you rotate passwords or create new accounts whenever a team member leaves.

5. Cancel email access

Email systems contain troves of valuable data, ranging from key contacts to sensitive files and internal communications. In many cases, employees continue accessing email systems after they stop working for a company.

Revoke email access at the end of the employee's final day. In addition, monitor the outgoing employee's account and set up email forwarding to handle future requests from customers or clients. That way, you'll avoid confusing customers and impacting future projects.

6. Check for telephone forwarding

In some cases, employees will forward telephone numbers to external accounts—like their mobile numbers. Unhappy workers could even route telephone numbers to competitors out of spite.

Because of this, check to make sure that telephone numbers don't connect to external numbers and that all systems are functioning as designed. In addition, deprovision employees' voicemail accounts.

7. Remove mentions from internal documents

Companies are often slow to update internal documentation—especially during times of mass layoffs or restructuring. Unfortunately, this can make it look like previous team members are still with the company.

It's important to remove all outgoing employee mentions from documents like contacts lists, websites, social media channels, documentation, and organizational charts.

8. Update physical access controls

It's also necessary to update physical access to prevent former employees from entering offices, data centers, or storage locations. Change door codes and locks, revoke clearance cards, and take back any physical access wearables or devices that employees use.

9. Collect company-owned devices

Employees may be reluctant to return company-owned devices, especially if they use them for personal activities or other projects. Devices often store data locally, making them a security liability. These devices can also be expensive to replace.

For this reason, it's a good idea to track company-owned devices—like laptops, desktops, mobile devices, tablets, cameras, and external storage devices.

10. Back up and secure critical files

For some former workers, it can be tempting to use important files as bargaining chips when negotiating with potential new employers, particularly if the information is sensitive or valuable. In the worst-case scenario, people may delete files or hold them ransom for higher compensation.

You can avoid this risk by requiring team members to store information in company-owned accounts and regularly backing up and validating critical files. Restricting local data storage eliminates the threat of rogue or negligent account owners.

11. Create forensic computer images

Security issues can be difficult to detect. Sometimes, they may not appear for weeks or months after an employee leaves.

Create forensic images of an employee's computer and securely retain them after the employee leaves. Doing so can aid in future investigations and help hold outgoing employees responsible for future security violations or data breaches.

12. Perform real-time network monitoring

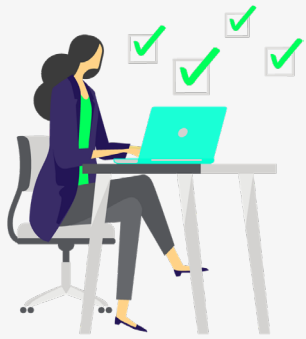
IT should remain on high alert after an outgoing employee leaves the company. One way to accomplish this is to set up a Security Information and Event Management (SIEM) solution to detect suspicious behavior and restrict access. Network monitoring should take place around the clock, and all network communications devices must be monitored.

13. Conduct a thorough exit process

The last item on our offboarding checklist is one that's easy to overlook as interviews are, not surprisingly, associated with job applicants, not those terminating their employment. The exit interview is the company's last chance to communicate with an employee before they part ways. As such, it's critical to have security and IT administrators present to ask questions and go over last-minute items.

At this point, the employee should sign statements confirming the return of all company-owned assets. It's also necessary to inform the employee not to access any systems, files, or accounts and to remind them of the repercussions that may ensue for doing so.

Bonus checklist for offboarding IT administrators



You should **exercise greater caution when offboarding certain employees** like domain administrators, systems administrators, developers, and security or operations professionals. These individuals have high levels of privileged access to sensitive resources that—if abused—could threaten the operational stability of your organization.

With that in mind, here are more recommendations to add to your checklist when offboarding high-risk IT employees.

Transfer knowledge in advance

Team leaders should meet with outgoing employees to ask questions and transfer knowledge. During this meeting, the departing employee should provide access to any sensitive systems they control and share information about where crown-jewel data lives.

Involve your legal team

In highly sensitive systems and data cases, it's a good idea to bring the legal department into the fold when offboarding certain employees. Legal assistants can help advise on what questions to ask and help to properly document information (e.g., forensic computer files).