ITGlue

Employee Onboarding and Offboarding for Clients

MSPs are responsible for ensuring the smooth IT onboarding of their clients' new hires. Setting up the hardware and providing guidelines on best practices should be done promptly to get the new hires up and running in no time. Similarly, offboarding is another critical process where MSPs play a vital role. Whether it is revoking security access or ensuring hardware retrieval, it should be done instantly to ensure security.

To avoid uncertainty and reduce time wastage, we've come up with this checklist to help your MSP implement a systematic process to properly onboard and offboard your clients' employees.

Onboarding Checklist

The following steps are essential to ensure the effective onboarding of your client's new employees in remote and hybrid work environments.

Step 1: Gather Information

- [ ] Coordinate with your client's HR department to collect information such as name, contact details, job titles, departments, starting date, etc.
- [ ] Determine which software, hardware, tools and access rights the new employees need, such as company email, internal messaging, productivity tools, analytics, spreadsheets, etc.
- [ ] Get the necessary approvals from your client to set up new accounts.
- [ ] Invite the new hires to join your client's corporate accounts and send them setup guidelines.

Pro-tip: Gather the required information well ahead of the employees' start date to ensure smooth onboarding from the very first day.

Step 2: Hardware Delivery & Setup

- [ ] List the IT hardware that the employees require and identify the location of this hardware. If required, order it in.
- [ ] Set up employee workstations or laptops including all required peripherals such as keyboards and monitors.
- [ ] Ensure that your client's new hires have access to a high-speed internet connection.

Pro-tip: Schedule equipment delivery to arrive before the start date, if needed, for remote setup.

Step 3: Software Installation & Account Setup

- [ ] Ensure all required software is installed and updated before the start date.
- [ ] Provide access to all software and any cloud-based software systems your client uses.
- [ ] Create company user IDs (username and password).
- [ ] Grant access to network shares.
- [ ] Set up mail accounts and passwords.
- [ ] Facilitate email setup and best practices (email signature).
- [ ] Familiarize new users with the Global Address List and verify that their information is correct.
- [ ] Ensure computer setup and configuration of mail client, if applicable.
- [ ] Ensure telephone code and phone setup (voice mailbox), if applicable.
- [ ] Provide database(s) access, if applicable.
- [ ] Provide accounting system access, if applicable.
- [ ] Provide access to the intranet, banking websites, company websites and social media sites, if applicable.
- [ ] Provide access to cloud storage, if applicable.
- [ ] Facilitate mail setup in mobile devices/smartphones, if applicable.

Pro-tip: If your client uses any custom software tools, ensure you provide the necessary training on how to use these tools during onboarding.

Step 4: First Day Review

- [ ] Ensure the new hires understand and sign data privacy agreements.
- [ ] Provide training on how to secure their workstations.
- [ ] Provide guidelines on best practices and productivity tips.
- [ ] Reset initial user ID passwords.
- [ ] Check to see if all software is properly installed.

Pro-tip: Once onboarding is done, provide your contact details and instruct them on how to reach you in case of IT issues or other doubts.

Offboarding Checklist

Offboarding is as important as onboarding. A disgruntled employee with access to sensitive data even after being let go poses a high level of threat to your client's network security. Apart from being quick, your offboarding should also follow a systematic process to reduce potential security risks. The following checklist will help you organize your client's offboarding process in remote and hybrid work environments.

Step 1: Assessment & Equipment Retrieval

- [ ] Determine if the employee is "high-risk" or not. If yes, then:
  - [ ] Immediately disable the employee's access to all systems.
  - [ ] Remove all client data from the employee-owned devices.
- [ ] Ensure the employee returns any company-owned equipment and assets.
- [ ] Compile a list of all locations where the employee stored data, including cloud storage platforms.

Pro-tip: Make a list of applications that contain critical data the employee has access to.

Step 2: Phone & Email Access

- [ ] Ensure the employee's phone does not forward to any external numbers and change the voicemail password.
- [ ] Reset the password in your email system and disable the Active Directory ID.
- [ ] If the employee used a personal cell phone or tablet to access work email, wipe or remove the email account.
- [ ] Create an out-of-office message for emails as per your client's communication guidelines.
- [ ] Remove the employee from generic and specialized email distribution lists.
- [ ] Set up of mail forwarding, if applicable.

Pro-tip: For employees dealing with your client's customers, ensure you forward all critical emails to another employee before disabling the account.

Step 3: Network & Cloud Access

- [ ] Terminate VPN and review any remote access methods.
- [ ] Remove the employee from all access control security groups.
- [ ] Move any association files that may have been stored outside your primary file repositories to a central location.
- [ ] Revoke access to your client's corporate cloud storage accounts.
- [ ] Remove association files from any personal cloud storage accounts.

Pro-tip: Determine and grant access to anyone who will need access to the ex-employee's local and network files.

Step 4: Personnel

- [ ] Review your password database logs to determine which passwords were accessed by the employee.
- [ ] Reclaim employee licenses.
- [ ] Ensure related staff change their passwords to minimize the risk of shared passwords.
- [ ] Contact any vendors that the terminated employee managed or worked with to alert them of the employee's departure and provide a new contact.
- [ ] Remove the ex-employee from the authorized list of contacts.
- [ ] Remove or change credentials (usernames/passwords).

Pro-tip: Check if there are any vendor licenses assigned to the employee. Your clients don't want to be paying for the licenses even after the employee's exit.

This list may not be exhaustive but it provides a much-needed framework for onboarding or offboarding your clients' employees in a remote and hybrid environment. Most importantly, you need the right tools that can make the process easier and quicker through automation.

For instance, IT Glue's smart documentation can help you collaborate with other teams and widely share SOPs, checklists and other critical information across multiple departments. Make sure you use the right technological tools that can assist you with streamlining the employee onboarding/offboarding process for your clients.

To know more about how the right tools and documentation process can help you with client employee onboarding and offboarding, tune in to our webinar.

WATCH WEBINAR

To see how IT Glue can help you with employee onboarding and offboarding, request a demo.

REQUEST A DEMO