IT Offboarding

IT-specific offboarding of employees typically requires working with your IT Support Group and/or IT Administrators to revoke access to multiple systems, recover equipment, and help former employees exit on good terms. A well-structured checklist will help you:

- Protect your data.
- Mitigate legal and security threats.
- Uphold compliance standards.
- Ease the transition for remaining staff.
- Part on good terms.

Most of all, a checklist will give you assurance that you have dealt with every requirement of employee offboarding. If you don't deal with them all, the risk for problems down the line can increase.

Technical Offboarding Steps

Use this checklist whenever an employee with technical access leaves the organization:

1. Inform HR as soon as termination occurs.
2. Revoke access ASAP by having IT support group or administrators perform duties such as resetting passwords; blocking access; resetting door combinations; etc. Remember to include shared credentials as well.
3. Remove access/accounts from applications such as databases, group apps, etc.
4. Terminate VPN and employee remote access.
5. Decide how to handle e-mail accounts; phone line/extension (including voicemails)
6. Update system ownership (data files; etc.) being sure to backup critical information.
7. Recover company devices and physical assets including laptops; cellphones; storage devices; credit cards; security badges; etc.
8. Based on role, reassign (or simply cancel) employee's vendor credentials; subscriptions; etc.
9. Regularly review access logs to ensure nothing slips through.

In Conclusion

If your offboarding process doesn't give you confidence that former staff no longer have access to your organization's infrastructure, then chances are your environment is sprinkled with security gaps. That means former employees may still be able to delete files, misconfigure servers, alter data, or steal intellectual property. Not to mention that bad actors may discover forgotten keys, certificates, and "zombie credentials."

Removing access is especially important for those with elevated access – including external/3rd-party IT Support Groups and (security) staff. These users often have far-reaching rights to shared folders, user email accounts, and other critical information. Users with network-wide access can even make significant changes in the environment.

In an effort to streamline the process, maintain an accurate IT inventory, including knowledge of who has access to what and where—keys, credentials, certificates, etc.—and take care to revoke access from all sensitive systems.