

Protect Your Business By Removing Account Access When Employees Leave - blueAPACHE

Canonical: <https://www.blueapache.com/blog/blog-protectyourbusiness>

Details:

2022

Employees are the lifeblood of every business, with the right people able to ignite and inspire growth from the inside out. Staff turnover is a reality of life, however, and it's important to safeguard your organisation when people move on. Setting up an employee offboarding policy is the best way to manage risk and protect yourself against unauthorised data access. Without an appropriate offboarding policy, you are risking your data, damaging your credibility, and putting your reputation in danger.

What is an employee offboarding policy?

People come and go from employment all the time, and detailed management and security protocols are needed to ensure an effective transition. Offboarding is the process of formal separation between an employee and a company. An employee offboarding policy is a document and set of procedures designed to manage this process. Whether an employee leaves due to resignation, termination, or retirement, this policy helps to document transition processes and ensure they are followed. For the purposes of this policy, its scope needs to encompass everyone who has been granted any sort of access to a system or platform. Therefore, it needs to apply not to only employees, but also to directors, (sub) contractors, partners and suppliers, accountants and auditors, temps and even in some instances clients.

What does a best practice employee offboarding policy include?

Among other things, an offboarding policy deals with transferring job responsibilities, protecting business assets, and restricting system access. In the modern world, access to computer systems is an integral part of most employment positions. Effective offboarding deals with this issue explicitly, cancelling accounts, changing authorisation credentials, restricting access to externally hosted cloud systems, and preventing access to sensitive databases. A best practice policy must be complete and comprehensive, identifying all those who have been granted access and linking them to all possible systems. Once people and systems have been listed, it's essential to analyse authorisation details, accounts, and passwords. Then, after all this information is collated and tracked, sign-on details and other changes can be made.

What are the business risks of not having an employee offboarding policy?

Without an effective employee offboarding policy, you are risking the integrity and security of your business. A security loophole is created when former employees and others are not removed from your system. This can have disastrous consequences, and it's an open-ended problem that needs to be closed. The following are key risks:

Unauthorised system entry

Data theft, corruption and loss

Malicious insertion of malware
Lack of business continuity
Theft of intellectual property and personal information
Long-term reputation damage

What are the challenges for SaaS services with an employee offboarding policy?

Creating and implementing an employee offboarding policy can be highly challenging. Traditionally systems were held within an on-premises data centre, which could only be accessed via devices “inside the firewall” or via VPN. This added additional layers of security and control. SaaS services are designed to operate in the cloud (i.e. out of the premises) and be accessible from any device, anywhere. This approach, of course, presents huge efficiencies, cost savings and convenience, but it also means access control becomes substantially more complex. Under the old model, revoking network and VPN access effectively meant shutting ex-employees out of all systems. This approach no longer works with SaaS, and access needs to be tracked, logged, and revoked on each platform and system.

What solution can overcome these challenges?

Offboarding policies are best managed through an identity and access management tool (IAM), which is a broader set of protocols designed to administer user identities and control access to enterprise resources. This tool is capable of tracking and managing diverse user access across multiple platforms. Key IAM features include single sign-on functionality, adaptive multi-factor authentication, and user provisioning as an aspect of lifecycle management. Modern organisations often use Identity as a Service (IDaaS) offerings to simplify authentication through cloud-based services.

Discover how your business can benefit from IAM

IAM is recommended to any business that needs a comprehensive offboarding solution. If you rely on employees in any way, they must be carefully managed. A dedicated IAM offers the following benefits:

Reduce costs and complexities – IDaaS solutions help you avoid capital equipment expenses and simplify operations. With automated identity management, you can free up staff to focus on core business initiatives.

Improve value creation – Quick and easy deployment of IDaaS solutions allows you to focus on value creation. As a cloud solution, you don't need to deploy or configure on-premises technology.

Reduce risks – IDaaS solutions enhances security across your organisation. When password management practices are eliminated, you can reduce risks, remove vulnerabilities, and minimise attack vectors and surfaces.

Better user experiences – By eliminating password fatigue and providing consistent access to all applications using a single set of credentials, IDaaS solutions improve user experience.

We have created a simple checklist that highlights the key areas of focus to ensure the employee offboarding policy created is fit for purpose and secure. Access the Employee Offboarding Checklist [here](#). Call us today to secure your business with a professional offboarding solution. At blueAPACHE, we leverage the power and integrity of CyberArk: Identity Security and Access Management Leader. To find out more, please contact us directly at: 1800 248 749 <https://www.blueapache.com/contact/>

According to you, what is an employee offboarding policy?

An employee offboarding policy is a document and set of procedures designed to manage the formal separation process between an employee and a company, whether the employee leaves due to resignation, termination, or retirement, ensuring transition processes are documented and followed.

Who should be covered by the scope of an employee offboarding policy?

According to us, the policy's scope should encompass everyone granted any sort of system or platform access, including employees, directors, (sub)contractors, partners and suppliers, accountants and auditors, temps, and in some instances clients.

What does a best practice employee offboarding policy include, according to you?

A best practice policy deals with transferring job responsibilities, protecting business assets, and restricting system access—cancelling accounts, changing authorisation credentials, restricting access to externally hosted cloud systems, and preventing access to sensitive databases. It must be comprehensive, identifying all people with access and linking them to all possible systems, then analysing authorisation details, accounts, and passwords before making sign-on changes.

Why do SaaS services create challenges for employee offboarding policies?

Traditionally, systems were held in an on-premises data centre accessible only 'inside the firewall' or via VPN, adding security layers. SaaS services operate in the cloud and are accessible from any device anywhere, which brings efficiencies and cost savings but makes access control more complex—revoking network/VPN access no longer shuts ex-employees out of all systems, so access must be tracked, logged, and revoked on each platform individually.

What solution do you recommend to manage offboarding challenges across multiple platforms?

We recommend managing offboarding policies through an Identity and Access Management (IAM) tool, a broader set of protocols for administering user identities and controlling access to enterprise resources. Key IAM features include single sign-on functionality, adaptive multi-factor authentication, and user provisioning as part of lifecycle management, often delivered via Identity as a Service (IDaaS) offerings.

What benefits does a dedicated IAM/IDaaS solution offer businesses, according to the blog?

The blog lists four benefits: reduce costs and complexities (avoiding capital equipment expenses and freeing staff via automation), improve value creation (quick, easy cloud deployment without on-premises configuration), reduce risks (enhanced security by eliminating password management practices and minimising attack vectors), and better user experiences (eliminating password fatigue with consistent single-credential access to all applications).

What resource do you offer to help create an offboarding policy, and which vendor's technology do they use?

We offer a simple Employee Offboarding Checklist highlighting key areas of focus to ensure an offboarding policy is fit for purpose and secure. We leverage CyberArk, described as an Identity

Security and Access Management Leader, for professional offboarding solutions.

How can someone contact you to secure their business with an offboarding solution?

According to the blog, businesses can call us at 1800 248 749 or visit <https://www.blueapache.com/contact/> to find out more about securing their business with a professional offboarding solution.