CYBERSECURITY **EMPLOYEE OFFBOARDING CHECKLIST**

When employees leave your organisation, it's standard procedure to ensure the return of physical assets like laptops and phones and terminate physical access to buildings and work sites – but what about digital access? With more and more IT services being provisioned "as-a-Service", removing network log-in is no longer enough to protect data assets and platforms.

This checklist has been designed to help businesses build and adapt offboarding policies to ensure they are fit for purpose in a cloud-first environment.

1 MAKE SURE OFFBOARDING IS COMPREHENSIVE

Offboarding policies need to apply to everyone who has access to your systems and data. It can't just be limited to employees but also needs to include temporary staff, contractors, employees of sub-contractors, directors, advisers, interns – the list is long.

2 ENSURE OFFBOARDING IS RETROACTIVE

Many policies focus on preventing ongoing access to systems and data from the point the employee leaves the business, but studies have found that 70% of intellectual property theft happens in the three months before an employee resigns. Offboarding processes need to review employee activity prior to resignation to ensure no theft has occurred, and should also include graduated deprovisioning of systems access before the employee leaves.

3 TRACK AND RESCIND ALL SYSTEM AND PLATFORM ACCESS

With the plethora of tools employees now use – especially SaaS – it's virtually impossible to track all access without using specialist tools. Identity and Access Management (IAM) solutions provide the means to automate provisioning, tracking and de-provisioning of access to all systems and platforms – for both on-premises systems or cloud hosted – for all users in an organisation.

4 CEASE THE HABIT OF ALLOWING FOR SHARED ACCOUNTS

It's important that any system or platform access is granted on an individual basis – even if for a short period of time. If an employee leaves and they have been granted shared access, then a security risk is created unless all passwords are changed or access revoked. Best practice is to not allow shared access or password sharing in the first instance.

5 OFFBOARDING STARTS WITH ONBOARDING

It sounds counterintuitive, but the best place to start the offboarding process is when you onboard a new employee. This means ensuring individual access to systems is provisioned, and new employees are trained on the organisation's data retention, cybersecurity awareness and access control policies – and how they relate to their role. It's especially important to be clear that any data or documents created during their period of employment remain the organisation's property – not theirs to take with them when they leave. This is also a good time to start creating a record of what assets and access are being issued to the user; this assists in collecting all assets from the user when offboarding.

6 DISABLE ACCESS, BUT DON'T DELETE DATA

In order to comply with data retention regulations that are enforced across multiple industry sectors, it's vital that when employee access is rescinded, that doesn't mean that their data is deleted. Consider backing up subscriptions like Microsoft 365 so that emails, chats and shared documents remain accessible long after the employee has moved on.

7 ENSURE HR, IT AND FACILITIES MANAGEMENT (FM) ARE OFFBOARDING PARTNERS

It's too late if HR inform IT and FM that an employee has left the organisation, after they have left. Policies need to direct that the IT and FM teams are informed as soon as HR becomes aware that a person will be exiting the organisation. The three teams should then work to a shared offboarding schedule covering employee engagement, physical asset recovery, systems and platform access, and site access.

8 DON'T FORGET REMOTE WORKERS

With many employees now spending their entire tenure with a business in a remote setting, offboarding processes need to explicitly include remote-first or remote-only team members. Policies need to consider the complexities of remote access, personal device usage and unauthorised copying of company data.

For more information on how blueAPACHE can support your Identity Access Management and other security needs, please contact our specialist security team.

1800 248 749

www.blueAPACHE.com

blueAPACHE