Preventing Rogue Access

How to manage user access to IT services during employment—and after employment ends.

Processes for managing IT access

Best practices for onboarding new employees

An exhaustive onboarding checklist

Plus: Advice for regulated companies

Osterman Research recently surveyed knowledge workers about their access to former employers' IT systems.

An incredible 89% of respondents retained access to at least one system—such as Salesforce, PayPal, email, SharePoint and other sensitive corporate apps.

One of Osterman Research's key recommendations for preventing this kind of access is to implement best practices for managing employee access to IT services as well as a rigorous IT offboarding process for departing employees.

This document presents a template for bringing these practices to your company. It includes guidelines for setting up internal processes as well as specific actions to take when onboarding and offboarding employees.

In addition, it includes recommendations specific to regulated industries such as financial services, legal services and healthcare.

THE EX-EMPLOYEE **MENACE**

Intermedia's 2014 SMB Rogue Access Study

Best practices for tracking access to IT systems

The first step to preventing unauthorized access by current and former employees is to develop a complete understanding of your IT landscape and the access privileges within it.

IT systems access recommendations

1. **Establish a security and compliance group within the company**
   This group should monitor two key areas: 1) who has access to which IT services and 2) how information is being accessed and shared. You should build this group's role into broader IT policies so that alerts can go out when a policy has been violated. This group should provide compliance and security training to employees on a quarterly/yearly basis.

2. **Put in place a clear set of company IT policies.**
   This includes policies on app usage, a list of approved sites and services and a list of approved software and apps that employees can use. Also, require that employees use company-provided logins for these apps instead of personal logins.

3. **Provide role-based access to applications.**
   Create a stringent approval process for all services, apps, and equipment that employees need. Employ two levels of approval for each request: approval from the employee's direct manager, as well as a VP or account owner. Keep records in a centralized database, so you have a clear "paper trail" of all services and equipment given to each employee.

4. **Create a central repository for admin logins and passwords.**
   Don't give users admin rights to their laptops. Instead, require employees to log tickets with IT to get access to download new software.

5. **Eliminate shared logins/accounts.**
   Assign accounts to one person whenever possible. If you have to use a shared account for budgetary reasons, make sure you rotate out the password on a monthly basis and employ strong password policies.

6. **Conduct regular audits.**
   Audit all your user accounts (LDAP, Active Directory, all apps) regularly. Have a single place for running audit reports and searching for users. Make sure you track all the apps being used—regardless of department— so you know who's paying for them, who "owns" them, and what access and control IT has.

7. **Regularly inquire with the finance department about the contracts that are in place with external vendors.**
   This is a great way to identify web applications that might be in-use by the company that did not go through IT.

Employee onboarding recommendations

1. **Set up your accounts in Active Directory, and make sure all cloud apps are SAML authenticated.**
   This gives you one central location to manage employee accounts. It also makes it faster and easier to provision and de-provision employees.

2. **Use unique identifiers when creating new employee accounts.**
   In the system in which you're creating the account, fill an unused attribute field with the employee's unique HR-assigned ID number. This way, if a user has different name listings (e.g. J. Smith, Joe S., etc.), it's easier to find all the apps with which they are associated.

3. **Maintain a distribution list to announce new hires.**
   A distribution lists ensures that all key departments (Finance, HR, Facilities, etc.) are notified without fail when someone new is coming onboard.

4. **Run a system audit when employees change departments.**
   Make sure you de-provision access to anything the employee no longer needs in their new role. That way, employees always have access to only those systems and applications that they really need to do their jobs.

Employee offboarding recommendations

1. **Adhere to a strict employee offboarding checklist.**
   A sample checklist is included in this document.

2. **Maintain distribution list for terminations.**
   Similar to your new hire distribution list, create a list that informs key departments (Finance, HR, Facilities, Legal, etc.) when an employee is leaving.

3. **Direct the email account of a departing employee to his/her manager.**
   Reroute the departing employee's email account to their manager for the first 2-3 months so that important messages are retained and handled.

4. **Terminate all employee accounts.**
   It is critical to terminate every employee account to every service, both on-premises and in the cloud. If the employee is the primary contact for an online account or project, make sure that contact gets re-assigned.

5. **Review the apps saved in your employee's single sign-on portal.**
   This is an excellent method for discovering apps that an employee may have provisioned or used without IT's knowledge. (These "unknown" apps are the most likely to create the risk of post-employment access.)

6. **Make sure to collect all company assets: laptops, phones, ID badges, software, etc.**
   Also make sure you collect any external hard drives or company-owned equipment an employee may have used as part of a home office.

Recommendations for regulated companies

If you're in a regulated industry such as finance or healthcare, you must put extra measures in place to ensure compliance with governmental regulations. Here's a list of suggestions that regulated companies can implement to better control access to corporate accounts and data.

1. Eliminate access to outside email/internet.
2. Restrict access to certain sites/apps (e.g. Facebook) to read-only.
3. Only allow access to company-approved sites.
4. Require employees to use desktop machines or dummy terminals.
5. Don't allow employees to take laptops or work computers home.
6. Remove the ability for employees to utilize USB or external hard drives to save data from their computer.
7. Implement an approval process for all outbound email. This may include requiring approval by a manager before email goes out.
8. Only allow work email and information to be accessed on company-issued mobile devices.

Employee Offboarding Checklist

Presented by: INTERMEDIA®

Employee name: _____ Department: _____

Supervisor name: _____ Separation date: _____

Item(s) to collect	Done	If No, explain
Computer, laptop and any other company equipment		
All digital certificates, key files, and passwords, including any client certificates that may be used for identity verification and/or "signing" purposes		
Keys to any company building or equipment (file cabinets, company car, machinery, etc.)		
ID badge		
VPN key fob or card		

Actions to perform	Done	If No, explain
Instruct employee to remove personal data from company devices and accounts within a clear timeframe.		
Inform employee that devices, files, accounts, etc. revert to the company after they leave.		
Transfer ownership or access to any company records to the employee's department. This includes records stored on non-company devices.		
Have employee remove company data from personal file sharing services and non-company devices.		
Have employee sign an agreement acknowledging that their data has been removed from personal services and devices.		

Actions to perform	Done	If No, explain
Have employee sign a non-compete or other NDA agreements.		
Ask employee whether there is any sensitive data on devices or in accounts that must be protected.		
Securely wipe employee's laptop or computer and retain custody of all equipment.		
Disable ActiveSync and Active Directory for the employee.		
Disable employees accounts on external web-apps		