Optimizing Security Practices Among Employees

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

- Processes for establishing a highly secure environment
- Best practices for onboarding new employees
- An exhaustive offboarding checklist for exiting employees
- Plus: Advice for regulated companies

In our 2015 Insider Risk Report, Intermedia surveyed over 2,000 knowledge workers in the US and UK about their security practices at current and previous places of employment.

And incredibly, 93% of respondents admitted to engaging in a least one form of risky data security – from sharing account credentials to installing non-sanctioned applications.

Our key recommendation for preventing this kind of behavior is to implement a set of guidelines incorporating best practices for employee security and access to IT services during employment 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.

Learn how Intermedia's Office in the Cloud™ suite of IT services can dramatically reduce risky security practices by employees. Call **(800) 379-7719** or email **sales@intermedia.net.**

presented by

INTERMEDIA The Business Cloud™

Find more information about the threat presented by risky user security practices, visit **Intermedia.net/RiskiestUsers**

Best practices for employee security and tracking access to IT systems

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

Recommendations for setting security ground rules

1. **Establish a security and compliance team within the company.**
   This team 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 team's role into broader IT policies so that alerts can go out when a policy has been violated.

2. **Put in place a clear set of company IT policies.**
   Have a comprehensive security policy that follows the latest trends. This includes policies on strong password practices, application usage, and a list of approved websites, services, software and applications that employees can use. Also, require that employees use company-provided logins for these applications instead of personal logins.

3. **Provide regular training for all employees.**
   Have your security and compliance teams hold quarterly training sessions for all employees--not just new-hire sessions. Remind everyone that security risks are real. Make sure they know why your company rules are important. Training should include lessons on avoiding phishing attacks, hacking, viruses and malware. Read our phishing report at Intermedia.net/phishingevolves to learn more about educating your employees on these topics.

Recommendations for establishing a security framework

1. **Engineer your security measures around the lowest level of technical savvy.**
   Architect your controls uniformly to the lowest common denominator in terms of technical know-how. By targeting the lowest technical skill level, and minimizing the likelihood that a person at that level can do any damage to your system, you automatically thwart the people with higher levels of technical skill who "think they know better".

2. **Follow the "least privilege" model.**
   When provisioning users for access and services, keep in mind the user's role and only give them the access they need for that role. Err on the side of less access, rather than more. And as a person moves from one role to the next, re-evaluate that level of access and change it accordingly. Use groups in Active Directory® to make role-based access control (RBAC) easier.

3. **Segregate duties for high-risk functions.**
   Make sure at least two people sign off on high-risk activities like financial transactions, money transfers, changes to payroll, use of HR data, etc. This also helps prevent accidents that could cost the company money or damage its reputation.

4. **Make sure managers know what access their employees have.**
   Create a stringent approval process for all services, applications, and equipment that employees need. Employ two levels of approval for each request: approval from the employee's direct manager, as well as approval from 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.

5. **Put IT Admins in a special access category.**
   Develop a risk-based categorization process for your employees so that you can account for all levels of access when people leave. That way, when a high-risk individual like an IT Admin leaves, more red flags are raised so that you can ensure that they are completely cut off from access.

Recommendations for securing IT systems

1. **Create a central repository for admin logins and passwords.**
   Use a single sign-on (SSO) solution to manage passwords and account access, including access to shared accounts.

2. **Control access to hardware and track IT activity with a ticket system.**
   Don't give users administrative rights to their laptops. Instead, require employees to log tickets with IT to get access to download new software. This ticketing system will also provide an audit trail of IT activity and user requests.

3. **Eliminate shared logins/accounts.**
   Assign accounts to one person whenever possible. If you have to use a shared account because an application doesn't support multiple users (like Twitter), make sure you rotate out the password on a monthly basis and enable 2-Factor Authentication for added security. When someone with shared access leaves the company or changes roles (and doesn't need to use that account), you should immediately perform a password reset.

4. **Conduct regular audits.**
   Audit all of 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 of the applications being used—regardless of department—so you know who's paying for them, who "owns" them, and what access and control IT has. Check with Finance to discover applications that may be in use without your knowledge. If licenses are being purchased or a subscription is in place, Finance will know. Utilize an outside service provider to run an application usage audit on your network.

5. **Check access logs to critical systems frequently.**
   Look for unusual activity: IT Admins logging into systems that don't usually require their input (payroll, finance, etc.) or employees logging into systems too frequently, at odd times, or in unusual order.

Employee onboarding recommendations

1. **Set up your accounts in Active Directory, and make sure all cloud applications are SAML (or ADFS, WS-Fed, or OAuth) authenticated.**
   This gives you one central location to manage employee accounts. It also makes it faster and easier to provision employees. Using AD with SAML, ADFS, WS-Fed or OAuth also ensures that you'll be able to turn off access, even for higher level employees like IT Administrators, with the flip of a few switches.

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 of the applications with which they are associated.

3. **Maintain a distribution list to announce new hires.**
   A distribution list 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.**
   As mentioned before, 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. **Plan for the "two-weeks notice".**
   Work with department managers to draft a plan for each department to manage access for employees that have given notice, but haven't left yet. Reduce access to sensitive information and restrict the ability to perform high-risk actions like money transfers.

3. **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.

4. **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.

5. **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. Also make sure you deprovision users (and thereby delete data) from enterprise sync and share systems.

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

7. **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 that 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 zero-client terminals.**
5. **Block personal mobile devices and laptops from accessing the office network – both Wi-Fi and Ethernet.**
6. **Don't allow employees to take work laptops or computers home.**
7. **Remove the ability for employees to utilize USB or external hard drives to save data from their computer.**
8. **Implement an approval process for all outbound email. This may include requiring approval by a manager before email goes out.**
9. **Only allow work email and information to be accessed on company-issued mobile devices.**

About Intermedia

Intermedia's Office in the Cloud™ offers email, phone service, file sync and share, single sign-on, archiving and more. They're all fully integrated, secure and mobile. And they're all managed through our central HostPilot® control panel.

Our services help thwart risky security practices by making it easy to control access to the entire cloud footprint. Learn more at Intermedia.net/RiskiestUsers.

INTERMEDIA
The Business Cloud™

Intermedia's cloud IT services can help you optimize employee security practices. Contact us to learn more.

CALL US	EMAIL US	ON THE WEB
1.800.379.7729	**sales@intermedia.net**	**intermedia.net**

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		
Logins for all corporate and department applications		
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.		

About Intermedia

Intermedia's Office in the Cloud™ offers email, phone service, file sync and share, single sign-on, archiving and more. They're all fully integrated, secure and mobile. And they're all managed through our central HostPilot® control panel.

Our services help thwart risky security practices by making it easy to control access to the entire cloud footprint. Learn more at Intermedia.net/RiskiestUsers.

INTERMEDIA
The Business Cloud™

Intermedia's cloud IT services can help you optimize employee security practices. Contact us to learn more.

CALL US
1.800.379.7729

EMAIL US
sales@intermedia.net

ON THE WEB
intermedia.net