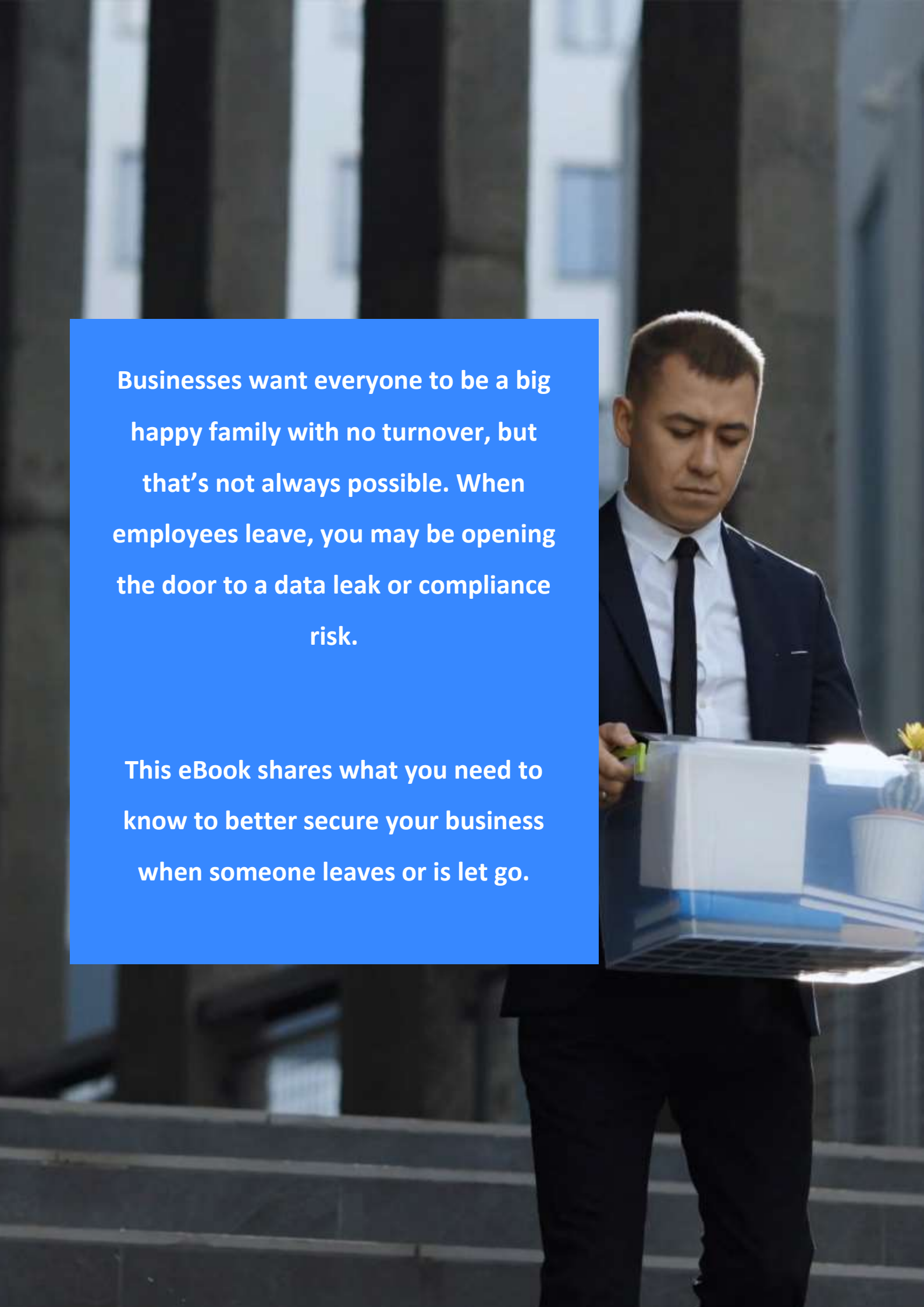
VBS iT Services

8 STEPS
TO PROTECT YOUR COMPANY DATA
WHEN PEOPLE LEAVE



Businesses want everyone to be a big happy family with no turnover, but that's not always possible. When employees leave, you may be opening the door to a data leak or compliance risk.

This eBook shares what you need to know to better secure your business when someone leaves or is let go.

When people leave, data should not go with them

Employee turnover is costly for many reasons:

Productivity can lag, you may lose institutional knowledge, and you have to recruit and train new talent. But, have you thought about the risks to your data security? An exiting employee taking data or accessing your systems risks sensitive information.

This ebook shares steps you can take to protect your data:

- Find out more about the risk when people leave your firm.
- Learn how to create a culture of security throughout employee tenure.
- Explore strategies to prevent turnover.
- Read about the ways a managed service provider helps protect data.

Understanding IT risks related to employee turnover.

There are times when you have to let employees go, but in this age of the Great Resignation, you may have more people leaving voluntarily. They could be younger workers who see greener pastures elsewhere, or older workers ready to retire. Problems arise if employees take data with them or leave with continued access.

When people exit your company, whether on good terms or not, they represent a data risk. Due to bring-your-own-device policies, they could have company data on a laptop, tablet, or smartphone. They may also have user accounts set up for business software on those mobile devices.

With people working remotely or on their own devices, there may also be questions about professional or personal data. Your business may need to consult with a lawyer about who has rights to what data and work done.

Someone leaving involuntarily might also remove data from your company with ill intent. They could download data to a portable thumb drive (USB drive), or transfer information to the cloud for continued access after leaving. They might release data publicly, sell it to criminals, or take it to your competition.

What can you do to offset the risk?

#1 Begin at the beginning

Obviously, you want to hire honest people with the right intentions for your business. Then, when you are first onboarding new employees, educate them about data security. Ensure they understand the importance of strong passwords, encryption, and saving information securely. That means using a secure server or using the business's cloud storage rather than a local machine.

#2 Provide ongoing training

If you have data compliance requirements, offer ongoing instruction about regulations. Keep employees current on treatment of confidential data, whether working for you or leaving.

Cover what they can and cannot use to access corporate data, especially intellectual property or trade secrets.

#3 Develop a security culture

Onboarding and training prove your business prioritizes security. Also, set clear policies on visibility into employee practices, data encryption, and backup.

If you are going to allow people to use their own devices, use remote management to monitor that activity. When someone does leave you, immediately go in and secure or remove company data.

What can you do to offset the risk?

#1 Begin at the beginning

Obviously, you want to hire honest people with the right intentions for your business. Then, when you are first onboarding new employees, educate them about data security. Ensure they understand the importance of strong passwords, encryption, and saving information securely. That means using a secure server or using the business's cloud storage rather than a local machine.

#2 Provide ongoing training

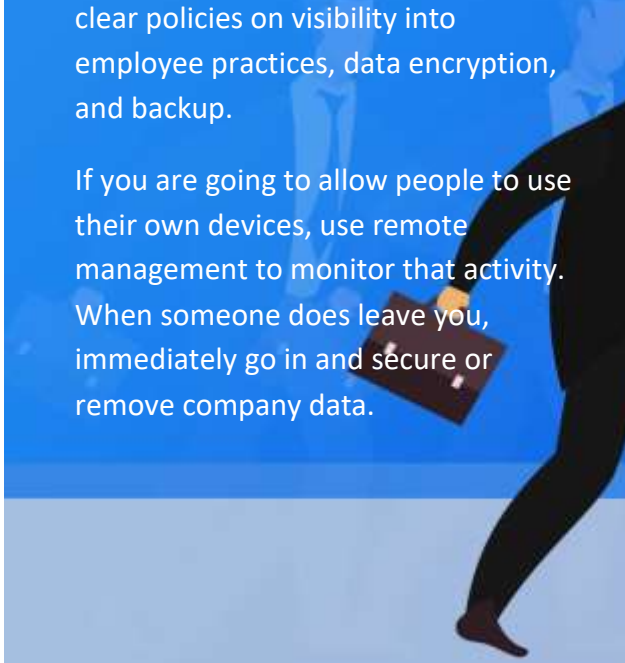
If you have data compliance requirements, offer ongoing instruction about regulations. Keep employees current on treatment of confidential data, whether working for you or leaving.

Cover what they can and cannot use to access corporate data, especially intellectual property or trade secrets.

#3 Develop a security culture

Onboarding and training prove your business prioritizes security. Also, set clear policies on visibility into employee practices, data encryption, and backup.

If you are going to allow people to use their own devices, use remote management to monitor that activity. When someone does leave you, immediately go in and secure or remove company data.



Why people take data with them?

There are three main reasons employees take business data when leaving their employer:

1. They do it unwittingly: they don't even realize that they have data they shouldn't on their personal devices.

2. They don't think they're doing anything wrong. Maybe they did the work to create that data, or they don't see that data as something that is valuable enough to protect.

3. They are not happy. They may be upset about being fired or being passed over for a promotion. They may intend to leak the information, sell it to criminals, or use it to their own personal advantage.

#4 Monitor employee Behaviour

Have a clear overall picture of who is accessing what and from where. Knowing where resources are, and what employees use them, can help you spot questionable behaviours. For example, people regularly download documents or send information to the cloud, but is someone suddenly doing that a lot more? That may mean they are preparing to leave and could be taking data with them.

In the news: *Leica Geosystems in Australia sued an employee for downloading 190,000 files containing sensitive information on his last day at work.*

#5 Limit access to data

Having a full map of your IT and employee roles can also help you to limit access. Taking a least-privileged access approach is the safest route. This allows someone to have access only to what they need to get their job done, nothing more. This can help cut the damage if someone inadvertently or intentionally takes data.

#6 Prioritize data protection

Put policies in place to force people to save important work to secure locations. Good data backup is critical. This can help you recover more quickly in the event of a malicious attack. It can also be useful if someone inadvertently deletes something important while trying to wipe devices clean for a new user.

#7 Have an exit policy

Your employment contracts need clear language about protecting sensitive and confidential data. Reiterate those now. If the employee has access to your social media, ensure they are no longer able to log in and post.

Also, establish a procedure for proper data removal from employee devices. Enlist IT to clear corporate technology and wipe employee personal devices.

In the news: *Atlantic Marine Construction Company sued a former employee for installing Google Chrome Remote Desktop without authorization. The former SVP accessed the company's network at least 16 times after he left to take confidential information.*

#8 Communicate Internally

Make sure all relevant parties know about terminations immediately. If Sue leaves accounting but IT doesn't know for a week, that could leave you exposed.

Know who needs to know about terminations to remove logins and close accounts. Expect prompt action to change passwords on shared accounts or blacklist terminated employees.

Keeping employees happy helps, too.

Another way to stem disgruntled employees leaving with your data is to engage employees and give them meaningful work. Be a place where people want to work. Some strategies to help encourage employee loyalty, while also boosting productivity, include:

Welcome feedback. Make it obvious you're willing to hear from employees. Then, where possible, act on what the employees say. This shows you respect their input and helps everyone feel more involved at work.

Encourage risk-taking. People like to feel challenged so they are less likely to look elsewhere to work. Make yours a company where people feel safe trying new things or making fresh suggestions.

Set goals. Help individuals identify challenging areas. You don't want to make the goals too difficult, as that could lead to the frustration you are aiming to avoid.

Outsourcing security steps up your posture

Enlisting a managed service provider (MSP) is one more way to cut risks when employees move on. The MSP can establish content management solutions and set up virtual desktops. These experts can also help with cloud solutions, encryption, and access authentication. They can provide valuable guidance for isolating sensitive data.

The MSP can remove employee access, wipe devices, and disable accounts. If a disgruntled employee deletes or corrupts files, the MSP can do backup and recovery to get you back on track.

VBS iT Services

Phone: **416-900-6852**
Email: **hello@vbsitservices.com**
Web: **www.vbsitservices.com**