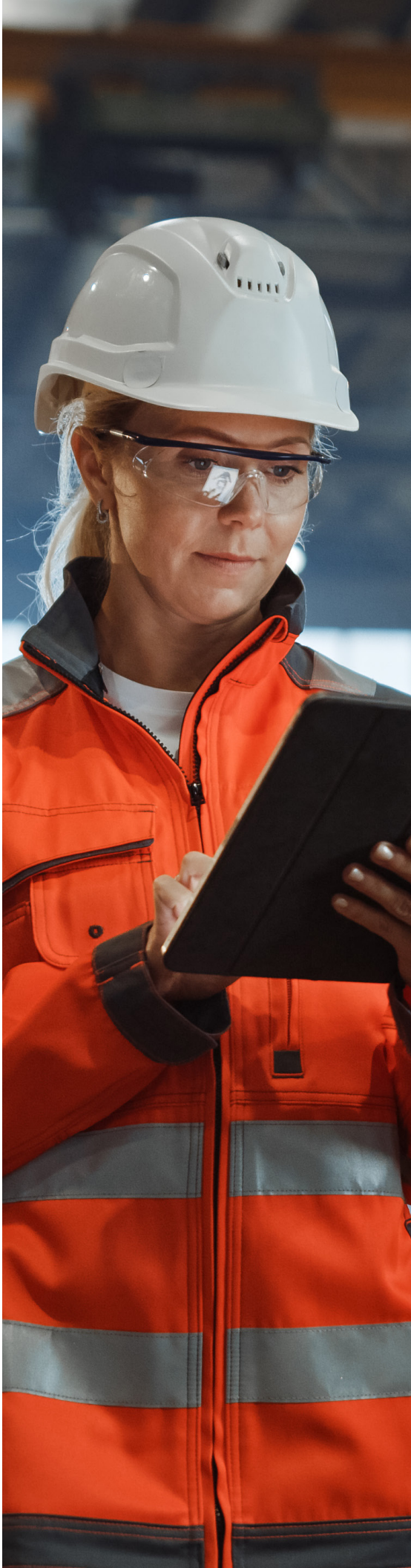
Construction

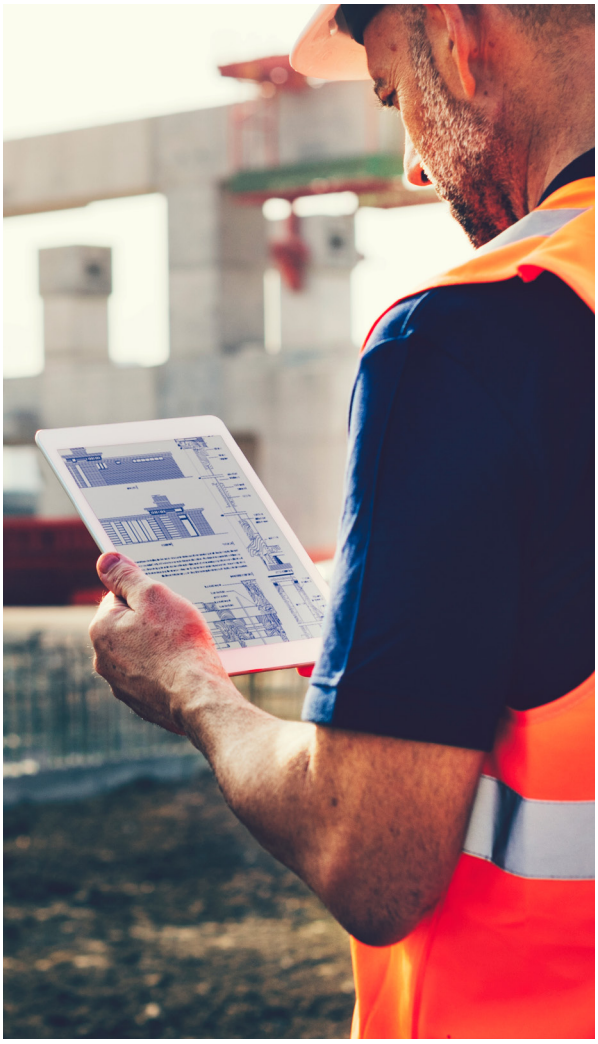
Data security guidance: Two checklists for safe data handling

Use these checklists to assess the efficacy of your data security tech stack and your crew's awareness of the role they place in mitigating security risks.



ShareFile™

Risk on the rise



In the world of construction, the need for data security is universally accepted. Emerging technology creates new data security risks that cybercriminals are all too eager to exploit.

It's no longer a question of whether data security matters, but how construction companies can integrate it seamlessly into their operations. CIOs, project managers, and other leaders are dependent on subcontractors and material vendors to get a job done. The company's data security is only as strong as the efforts of those subcontractors to protect financial and proprietary information.

The good news is there are security solutions that accommodate the construction industry's distinctive features, like tight deadlines, a skilled labor force, and the handling of sensitive data. This is only half the equation to addressing risk, though.

It takes both technology and the participation of your work crews:

1. **Using the right SaaS technology:** Your SaaS security features need to be accessible and easy to operate, while also providing robust layers of protection.
2. **Encouraging security awareness:** Every employee, regardless of their tech-savviness, can act more securely when creating or exchanging sensitive information.

The goal of this checklist is to help you implement these two solutions. Part I helps you assess whether your current tool (or tool you might be considering) correctly balances protection with productivity. Part II is a checklist you can share with employees in an effort to help them quickly run through a few simple steps to be more secure.

Understanding your biggest security risks

According to **Statista**, the average data breach in the United States in 2023 cost $9.48 million. Even your construction company is exposed to financial and reputational damage that can last months or years beyond the initial breach. Here are factors putting your company most at risk.

Smarter cyber criminals

Providing password protection and virus scanning software is not enough. Today's cybercriminals are more sophisticated than ever before. A 2022 study **found** that phishing campaigns attempting to trick professionals into downloading malware or giving away sensitive information increased 61% from the previous year.

In addition to becoming more common, these attacks are becoming more calculated. Cybercriminals may send emails or texts that appear to be from a trusted source or use **topical issues** to lure their victims, with subject lines that suggest shopping deals around the holidays or fake alerts about tax filing during tax season.

AI-created malware is especially good at avoiding detection by traditional antivirus software, leading to a sharp **increase in ransomware cases** in 2023. In fact, construction is now the third highest sector **impacted by ransomware**. These mounting threats from cybercriminals increase the likelihood for employees to fall into a well-conceived trap.

Preferring familiar tools and applications

With the rapid adoption of cloud-based services, employees have become more comfortable downloading and using outside applications without informing their IT departments. While they don't mean to do any harm with this practice, known as Shadow IT, they end up bypassing security measures and putting business and customer information in jeopardy.

It's human nature to prefer tools and applications we're already used to, and it can be difficult to adjust to working with different platforms even if they are more secure.

Working under pressure

Reluctance to adopt secure tech goes beyond the Shadow IT issue. Your employees and subcontractors need to collaborate or exchange information quickly and in ways they know how. That often means using un-secure platforms like email and downloading the document to local drives. Adding an extra step or changing their workflow altogether can feel overwhelming.

Security solution checklist

Your security tools should make it easy for you to protect customer information while still working efficiently on their behalf. Adopting stronger, more comprehensive solutions that integrate into existing workflows is a modern-day business imperative.

If your teams lack the technological capabilities outlined below, implementing software that allows everyone to do their best work in a more secure way is essential.

Check to make sure your solution has the following (and that you are actively using these features):

Single sign-on capabilities to avoid repeated log-ins across apps.
☐ Yes
☐ No

Secure link sharing so your clients can access documents with one click (instead of having to download a file).
☐ Yes
☐ No

A single, secure space such as a portal or dashboard where you can track and collaborate internally or directly with clients (as opposed to a platform that isn't secure).
☐ Yes
☐ No

Built-in workflows for safe document requests and collection.
☐ Yes
☐ No

Document links with customizable security settings.
☐ Yes
☐ No

Email encryption for the body of the message and attachments.
☐ Yes
☐ No

File encryption to protect sensitive information in transit or at rest.
☐ Yes
☐ No

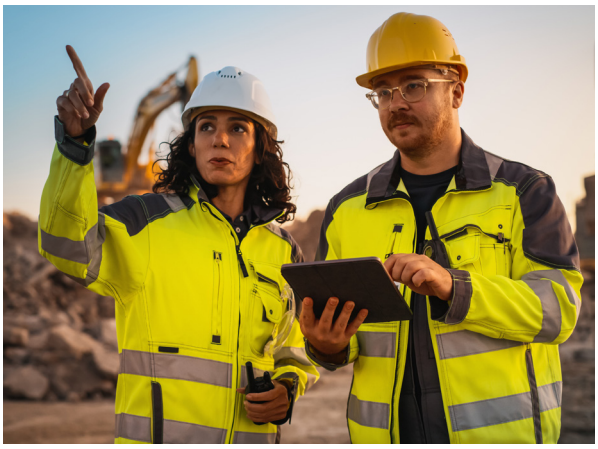
Custom permissions for folders and files to control who has access and for how long.
☐ Yes
☐ No

Multi-factor authentication for more secure log-ins.
☐ Yes
☐ No

Automated alerts that immediately flag potential security threats.
☐ Yes
☐ No

Security awareness checklist

Your crew's workflows contribute significantly to the effectiveness of your data security practices. To ensure protection of all sensitive data involved in a project, every worker on your crew should be answering 'Yes' to all 10 questions in the checklist below.



When receiving, storing, and sending files containing sensitive customer information, are you:

Limiting info collection to necessary data?
☐ Yes
☐ No

Determining how much protection information needs and applying the right level of permissions?
☐ Yes
☐ No

Avoiding the use of personal devices?
☐ Yes
☐ No

Creating strong, unique passwords for your accounts and devices?
☐ Yes
☐ No

Storing passwords in a secure place?
☐ Yes
☐ No

Staying on top of software updates that impact the effectiveness of your security features?
☐ Yes
☐ No

Taking an occasional free security course or reading about the latest phishing threats?
☐ Yes
☐ No

Checking if an email is suspicious, like closely reading the sender email address and/or not opening attachments right away?
☐ Yes
☐ No

Locking up your devices when they're not in use to prevent theft?
☐ Yes
☐ No

Limiting activities when using public wi-fi?
☐ Yes
☐ No

Seeing more no's than yes's?

While rigorous security practices can interfere with productivity, **they don't have to**. There are solutions available for construction firms that offer both productivity and protection by embedding greater security into existing workflows.

Considering both the pressure construction professionals are under to work efficiently and the costly consequences of a data breach, security solutions and practices should ensure that neither are ever compromised. Software that protects data while allowing for streamlined workflows and end-to-end productivity is well worth the investment.

With these checklists you can identify where you need the most support from a security solution and help your team stick to needed best practices for keeping data from every job secure. **Learn more about partnering with ShareFile to enhance data security through collaborative technology.**