

Information Security Tips By Shred-it

Here are some tips about how you and your company can implement organizational information security policies in your workplace.

Communicate your commitment to information security.

Emphasize your data security achievements and milestones during new employee orientation. Devote a section/subsection of your website to your company's security initiatives and how they help keep client information protected. Promote your company's new security programs or new initiatives in a press release, through social networks, etc. Highlight your track record of security in fact sheets, presentations, brochures or other marketing materials.

Hire security-conscious people.

Begin your *security-centric* thinking in the interview process by asking prospective employees questions about information security so you can gauge whether it's important to them.

Use secure practices for all documents.

Extend the same secure document handling practices used with client information to corporate documents, and shred documents once they are no longer needed.

Encrypt the data.

On portable devices such as smart phones, tablets, external memory drives and laptops, all confidential data should be encrypted, so company information is better protected in the event of theft or loss.

Think prevention, not reaction.

Instead of just dealing with breaches as they happen, develop preventative approaches that are strategic, integrated and long-term, such as eliminating security risks at the source and permanently securing the entire document lifecycle in every part of your organization.

Shred regularly and shred before recycling.

Implement a regularly scheduled process to avoid the accumulation of confidential paper waste. Don't let confidential documents sit unattended in recycling bins.



Don't overlook hard drives on computers or photocopiers.

Erasing your hard drive does not mean that the data is gone. Physical hard drive destruction is proven to be the only 100 percent secure way to destroy data from hard drives.

Conduct a periodic information security audit.

Develop a comprehensive overview of how internal documents are generated, revised and stored so you can spot any security weaknesses. Examine the document workflow and lifecycle; look for risk points throughout the process where confidential information is left unattended or easily accessible. Remember to analyze both electronic and paper-based sources.

Introduce a shred-all policy.

To avoid the risks of human error or poor judgment, don't ask your employees to decide which documents are confidential. Simply decide that all business documents should be shredded when no longer needed.

Make document security convenient.

Having a locked receptacle in your office or at conveniently accessible locations throughout your office will ensure that no one has access to sensitive documents after they have been disposed.

Build a culture of respect.

With all of the potential hazards for security breaches and identity theft, a company can only minimize the risks it faces, as opposed to eliminating them entirely. Therefore, the company needs to create a culture that values and respects confidentiality and privacy. Employees will be better educated and motivated to adhere to the privacy policy and treat document security as an important company initiative.

Destroy documents securely.

Confidential documents must be destroyed once they are no longer needed or the legal retention period is met. Secure destruction means they are shredded in such a way that the document cannot be reconstructed, and the intact document is not exposed to risk prior to shredding.



Train your employees.

Ongoing updates to privacy legislation and personnel changes mean that it's not enough to simply create a privacy policy – it also must be adapted and reinforced from the top down. It makes sense to implement quarterly training or retraining sessions so the privacy policy is easily understood and followed.

Limit access.

The more people who have access to sensitive documents, the greater the risk of a theft or breach. Restrict employee access to confidential data. This should be done based on specific business needs or specific categories of personnel. From limiting access to the record-keeping room to locking filing cabinets, there are many ways to accomplish this task.

Develop security policies.

By creating an internal document handling process, employees will have a clear understanding of what constitutes a sensitive document, how to handle them properly and what to do in the event of a potential breach or suspicious behavior. Additionally, it is important to research national and local legislation to ensure your new policy is 100% compliant with rules and regulations.

Examine the entire document lifecycle

Before you can identify any security vulnerabilities, you must first understand your company's document workflow and lifecycle. From creating the documents to storing and transferring them, many documents touch multiple departments and personnel. The more touch-points, the greater the risks.

