FACT SHEET

Creating a Total Security Culture

Creating a culture of security is about cultivating a corporate environment where employees consistently make decisions aligned with security policies. It is a culture where everyone strongly believes in the importance of information security. To help instill this belief, organizations must educate employees about the importance of protecting digital data, as well as secure document management and destruction. A holistic view of security must be instilled into all strategies, policies, procedures, and overall thinking to help build a security culture.

Self-Assess Your Information Security Culture

Ask yourself these questions about your organization to see how secure your your information security culture really is:

	YES	NO
1. Do we have the facilities and resources necessary to ensure that confidential information is protected?	☐	☐
2. Do we use a method of document destruction that is safe and secure?	☐	☐
3. Are document security policies clear, easy to understand, and effectively communicated to all employees?	☐	☐
4. Is there an employee that manages document security issues and ensures that all policies are strictly followed?	☐	☐
5. Are employees regularly and thoroughly trained on all document security regulations and the importance of protecting sensitive information?	☐	☐

If you answered "**No**" to any of the questions above, follow these steps to help keep your information secure.

Practical Steps to Help Establish a Total Security Culture

1 Identify all potential risks.

There are several risks that may threaten the information security of your organization, including customer, business, and employee information. It is critical to determine what these risks are, so you are aware of what needs protection.

2 Examine document workflow and lifecycle for electronic and paper documents.

By understanding the process each document goes through, you will be able to discover areas of improvement to better protect your confidential information.

3 Create a comprehensive information security strategy.

By identifying the key issues from the first two steps, you can develop a strategy to help keep your information secure and avoid a potential data breach.

4 Develop security policies that are compliant with state and federal privacy laws.

Use your legal department or counsel and trusted third party suppliers to help ensure company policies comply with applicable regulations.

5 Control access to confidential information.

Several laws, such as the Health Insurance Portability and Accountability Act (HIPAA), contain specific provisions regarding who may access information and how it may be used. Certain information should be made available only on a need-to-know basis.

6 Implement physical safeguards.

Implement a shred-it-all policy, which requires all employees – regardless of level – to shred all papers when no longer needed before they leave the office. Additionally, enforce a clean desk policy, requiring employees to securely store sensitive materials.

For more information, contact us at 877-510-8132.

We protect what matters.℠

Shred-it®
A Stericycle® Solution