FACT SHEET

Human Resource Guide to Creating a Total Security Culture

The average cost of a lost or stolen record is $141. The average cost of a data breach is $3.62 million.

A culture of security is about educating employees about the importance of secure document management and destruction. It is a culture where all employees strongly believe in the importance of information security. The attitudes and values reflected in your organization's security strategies, policies, procedures, and overall security thinking are the foundation of this security culture.

SELF-ASSESS YOUR CULTURE

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

» Does my organization have the facilities and resources necessary to ensure that confidential information is protected?

» Do we use a method of document destruction that is safe and secure?

» Are document security policies clear, easy to understand, and effectively communicated to all employees?

» Does the company have an employee that manages document security issues and ensures that all policies are strictly followed?

» Are the 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 the steps in the next section to keep your information secure.

We protect what matters.

Shred-it®

Practical Steps to Establish a Total Security Culture

» **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.

» **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.

» **Create a comprehensive information security strategy.**

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

» **Develop security policies that are compliant with national identity theft and privacy legislation.**

Ensure that the processes that you develop into your strategy work together with the legislation governing your business. By doing this, you will achieve compliance and protect your information.

» **Restrict access to confidential data, in electronic and paper form, based on specific needs of specific categories of personnel.**

Only the relevant person should have access to their respective confidential data (i.e. Only the HR Department and Managers should have access to payroll information for an employee). This limits exposure to keep confidential information secure.

» **Train your staff in secure document management and destruction.**

Ensure that you implement a ***Shred-it All* Policy** and a **Clean Desk Policy**, to make sure the documents are destroyed securely on a regular basis and information remains locked when it is not being used.

» **Build an organizational culture that values and respects confidentiality and privacy.**

With all these policies in place in addition to ongoing training and support from senior leadership, your employees will begin to show that they believe in the values and work to keep all information secure.

For more information, contact us at 800-697-4733 or visit us at shredit.com

Shred-it®

Shred-it® is a Stericycle solution. © 2017 Shred-it® International. All rights reserved.