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 believes strongly in the importance of information security. To help instill this belief, educate your employees about the importance of secure document management and its safe and sustainable 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 organisation to see how secure 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 communicated effectively 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 organisation, 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 privacy laws

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

5 | Control access to confidential information.

Privacy and security laws, including the EU/UK GDPR, 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.

Enforce a clean desk policy that requires all employees to securely store sensitive materials. Additionally, implement a shred-it-all policy so employees securely dispose of any paper they no longer need before they leave the office.

For more information, visit shredit.co.uk or call 0800 197 1164.

We protect what matters.

Shred-it®
A Stericycle® Solution