Knowing What to Shred in the Financial Services Industry

The relationship between finance professionals and their clients must be built on a foundation of trust. Data management is a fundamental element of trust between finance professionals and the clients they serve.

What to Shred:

Although individual needs may vary, the following is a list of the types of information you may choose to manage via secure destruction in the financial services industry:

Customer Information

▸ Account numbers

▸ Personally Identifiable Information (PII)

▸ Information protected by privacy laws such as the Gramm-Leach-Bliley Act (GLBA)

▸ Loan applications and documentation

▸ Banking data

Human Resources

▸ Job applications

▸ Health and safety documents

▸ Medical records

▸ Performance appraisals

▸ Training information and manuals

▸ Payroll information

▸ Resumes

Accounting and Information Technology

▸ Customer lists

▸ Supplier information

▸ Internal reports

▸ Accounts payable statements

Executive Level

▸ Budgets and other financial data

▸ Correspondance

▸ Strategic reports

▸ Legal contracts

▸ Financial statements

WARNING: FIRE HAZARD

X Batteries of any type

X Large metal objects

X Electronic devices (Hard drives are securely destroyed upon request)

What Not to Shred

X Food, glass, cans, etc.

X Candy/food wrappers

X Tissues

X Cardboard tubes

X Ink cartridges and toners

X Hanging folders

X Electrical items

X Office supplies, hole puncher, staple remover, etc.

X Nuts and bolts

X Syringes

Still Confused?

Ask yourself the following questions. If you answer YES to any of these, then SHRED the document.

1. Does it have any personally identifiable information (PII)?
2. Does it contain information protected by privacy laws?
3. Does it include any confidential corporate information?
4. Does the document list any financial information?

Shred-it®
A Stericycle® Solution

Tips to Help Keep All Of Your Data Secure

Use the following tips in order to keep your data secure and avoid a potential data breach:

▶ **Identify Areas of Risk**

Conduct an information security risk assessment and a walk-through of your administrative areas, including the front desk, to identify high-risk areas, such as printing stations, messy desks, and exposed trash and recycling bins. Flag these vulnerabilities and develop policies that can help to mitigate the threat.

▶ **Develop Retention Schedules**

All documents should have a recommended retention period, determined by their importance and content. Depending on the specific record, there may be laws and regulations that dictate which documents need to be kept and for how long. Follow document retention schedules to help keep offices free of clutter and to contribute to information security. To create an effective document retention policy for your financial services business, you may choose to consider including the following:

   ▶ A checklist of common document retention guidelines

   ▶ Recommendations for implementing a document destruction policy

   ▶ The proper document retention schedule

   ▶ To understand how a secure shredding program can help you meet your obligations

▶ **Adopt a *Shred-it-All* Policy**

Often there is confusion when deciding whether or not a document should be shredded. This policy encourages the regular destruction of all documents (in accordance with internal policy). By implementing a shred-it-all policy at your workplace, you help ensure that all documents are shredded. It is one of the most effective ways to help prevent physical data breaches.

▶ **Adopt a Clean Desk Policy**

A clean desk policy helps ensure staff shred or contain physical documents and that all technological devices are locked each time an employee leaves a workspace. This policy can also help reduce clutter, improve the security and confidentiality of information, and contribute to an organized workspace as a best practice throughout the organization.

▶ **Reinforce Policies through Reminders and Rewards**

To get buy-in from employees, place posters reminding them of the new policies in place to protect confidential information in the workplace. You can also drive employee engagement initiatives to encourage employees and incentivize good behavior through rewards such as team member recognition.

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

We protect what matters.^{SM}

Shred-it®
A Stericycle® Solution