

# Knowing What to Shred is Vital

## What to Shred

Personal data and confidential information must be protected. Here is a list of what to shred:

### Accounting

- Contracts
- Customer lists
- Internal reports
- Supplier information
- Payroll statements

### Procurement

- Corporate records
- Supplier purchase orders
- Supplier records
- Supplier specifications

### Research & Development

- Appraisals, product testing, etc.
- Formulas, product plans, and tests
- Specification drawings
- New product information
- Reports

### Human Resources

- Job applications
- Health and safety documents
- Medical records
- Performance appraisals
- Training information and manuals
- Payroll information

### Executive Level

- Budgets
- Correspondence
- Strategic reports
- Legal contracts

### Sales & Marketing

- Advertising
- Customer lists and contracts
- Strategy documents
- Training information

## Fire Hazards

- Batteries of any kind
- Large metal objects
- Electronic devices

## What NOT to Shred

- Batteries of any kind
- Large metal objects
- Electronic devices
- Food, glass, cans, etc.
- Candy/food wrappers
- Hand tissues
- Cardboard tubes
- Ink cartridges and toners
- Hanging folders
- Electrical items
- Office supplies, hole puncher, staple remover, etc.
- Nuts and bolts
- Syringes
- Hard drives (securely destroyed upon request)

## Not Sure? If You Answer YES to Any of These Questions, Then SHRED:

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?

# Tips For Keeping Your Data Secure

Use the following tips to keep your data secure and avoid the risk of a 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 remove the threat.

## Develop Retention Schedules

All documents have a recommended retention period, depending on their importance and content. There may also be laws and regulations that dictate which documents need to be kept and for how long. Follow document retention schedules to keep offices free of clutter and to contribute to information security.

### To create an effective document retention policy, you need 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 meet your obligations

## Adopt a “Shred-it All” Policy

There is often confusion when deciding whether or not to shred a document. Implementing a *Shred-it All* policy at your workplace encourages the regular destruction of all documents, ensuring that all documents are properly destroyed. It is one of the most effective ways to help prevent physical data breaches.

## Adopt a Clean Desk Policy

Clean desk policies help ensure staff shred or contain physical documents and that all technological devices are password protected each time an employee leaves a workspace. A clean desk policy helps reduce clutter, improves the security and confidentiality of information, and can 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.

Visit [www.una.com/shred-it](http://www.una.com/shred-it) for more information.



CONTRACT #SV2473

