Document Shredding

- ✓ Create a document shredding plan as part of your policy.

  Best Practice: Evaluate whether your company should shred the documents or hire a sub-contractor.

- ✓ Require a micro shredder if your company conducts onsite shredding.

- ✓ If you choose to hire a disposal company, consider the following:

  - **Does the company offer on-site and off-site shredding?** Some documents may contain information so sensitive that they should not leave the building thereby requiring on-site shredding services.
  - **Is the company familiar with federal and state requirements for document disposal and privacy regulations?** These include the federal Fair and Accurate Credit Transaction Act of 2003 (FACTA), Health Insurance Portability and Accountability Act (HIPAA), and Gramm-Leach-Bliley Act (GLB).
  - **Is the shredding company a member of NAID (National Association for Information Destruction)?** While it is not necessary for a company to hold a membership in this non-profit trade association, NAID provides its members with updates about information destruction, and highlights legal and government actions impacting the document destruction industry.
  - **Will the company allow you to watch documents being shredded upon request?** Watching your documents and information being destroyed can provide a sense of comfort and a demonstration of the shredding company's security measures.

Electronic Data Destruction

Consider the following components:

- ✓ Prior to the destruction of electronic records, ensure that the use of such information is no longer needed. This calculation should consider any potential lawsuits.
- ✓ Use a wipe or over-write program to eliminate personal information on hard drives before disposing of the computer. An alternative is to physically destroy the hard drive.
- ✓ Destroy tapes, disks or any electronic storage device containing sensitive information before their disposal.

REMEMBER...

- ⇒ Ensure that your written policy is followed by employees and consistently enforced. It is a good idea to appoint a senior member of your organization to be in charge of employee compliance with your document retention and destruction plan.
- ⇒ Ensure that you include education awareness and training in your document retention and destruction plan.
- ⇒ Ensure that your document retention and destruction plan is current by regularly reviewing its components and updating if necessary.

ADDITIONAL RESOURCES

National Association for Information Destruction
1951 W. Camelback Rd., Suite 350
Phoenix, AZ 85015
Phone (602) 788-6243
Fax (602) 788-4144
E-mail Info@naidonline.org

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-FTC-Help (1-877-382-4357)

NYS Consumer Protection Board

Advocating for and Empowering NY Consumers

www.nysconsumer.gov

1-800-697-1220

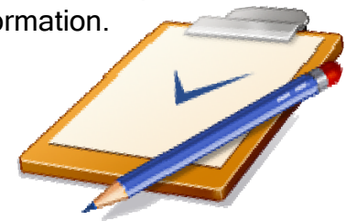
CREATING A DOCUMENT RETENTION AND DESTRUCTION POLICY FOR YOUR BUSINESS: A CHECK LIST

NEW YORK STATE
CONSUMER PROTECTION BOARD

Introduction

The protection of customer and employee personal information must be an integral part of your business. Specifically, it is vital for your business to have a written policy for the retention and destruction of personal information to guard against identity theft and security breaches. This plan should encompass retention and destruction of both paper files and electronic data.

Please use this checklist to incorporate fundamental elements into your written policy for the retention and destruction of personal information.



This brochure is for informational purposes only and should not be construed as legal advice or as policy of the State of New York. It is recommended that you speak with a privacy professional and an attorney for further advice.

Document Retention

- ✓ Determine what documents are to be stored.
- ✓ Determine where and how (e.g., physical form or electronically) documents are to be stored.
- ✓ Examine document retention time. Annual reports, articles of incorporation, board meetings and minutes, and fixed asset records are some examples of records that must be permanent. Other types of documents, such as contracts or correspondence, have different shelf lives.
- ✓ Check with attorneys and accountants to determine the appropriate length of time you should store various types of documents.
- ✓ Apply your document retention plan to electronic data. Electronic documents, including e-mail, must be retained as if they were paper documents. Where there is sufficient reason for e-mail messages to be retained, these messages should be printed in hard copy and kept in an appropriate file or moved to an "archive" computer file folder.
- ✓ Anticipate and be prepared for litigation. Ensure that your plan includes procedures to retain electronic data in the event of litigation.
- ✓ Create an emergency back-up plan in case of a loss of records and data.
- ✓ Ensure data back-up is performed regularly, consistently and safely to avoid the financial cost of data loss.

Key Elements of Data Retention

- ✓ Prohibit retaining a customer's personal or credit information unless there is a legitimate business purpose.
- ✓ Restrict access to any data that is retained for legitimate business purposes and make sure that it is physically secure.
- ✓ Password protect and encrypt data that contains personal information.
- ✓ Encrypt sensitive personal data sent via e-mail.
- ✓ Encrypt personal information stored on computer networks or portable storage devices.
- ✓ Provide for education awareness and training in your data retention and destruction plan for employees. Employees should also be trained to recognize security threats and potential breaches.
- ✓ Restrict employee access to offsite storage facilities.
- ✓ Require any contractors that retain personal information to follow the same written privacy and security guidelines in your organization.
- ✓ Ensure compliance with the New York State General Business Law Article 29-A, Section 520-a which states that credit and debit card receipts may not include the expiration date of the card or more than the last five digits, where appropriate.
- ✓ Ensure compliance with New York City Administration Code Section 20-117(g), where appropriate.

Document Destruction

- ✓ Ensure compliance with NYS General Business Law Article 26, Section 399-h which governs disposal of records containing personal identifying information (PII). PII includes:
  - Social Security number;
  - Driver's license number or non-driver identification card number; or
  - Mother's maiden name, financial services account number or code, savings account number or code, checking account number or code, debit card number or code, automated teller machine number or code, electronic serial number or personal identification number in combination with any additional information that can identify a person.
- ✓ When you dispose of information containing PII:
  - Shred the record before disposal; or
  - Destroy the PII contained in the record; or
  - Modify the record to make the personal identifying information unreadable; or
  - Take action consistent with commonly accepted industry practices to ensure that no unauthorized person will have access to the personal identifying information contained in the record.
- ✓ Ensure compliance with Federal Trade Commission's Disposal Rule, 16 CFR (Code of Federal Regulations) Part 682, where appropriate. This rule requires any business or individual using a consumer report, such as a credit check, for a business purpose to dispose of the report or information derived from such report to prevent "unauthorized access to or use of the information."
- ✓ Include the destruction of electronic