



**“A destruction policy is not just a good idea, it’s a must have.”**

# Would an **auditor** find an effective document retention and destruction policy in your office? Do *you* know what one is?

A destruction policy is not just a good idea, it’s a must have. It spells out what is to be destroyed, when it is to be destroyed and how it should be destroyed. This creates a standardization of destruction for a company, giving the act of shredding documents ethical reform to a now vital business practice.



***Problem Solved.***



Before a destruction policy can be fully implemented a company must first determine what documents it has, or will create, and how long to keep them.

Creating a retention schedule for all documents whether paper or electronic standardizes what is kept, for how long, and why. If you know why you are keeping something the answer to why you are destroying it will be obvious – it no longer has *any* value to your company or organization for retention purposes but may still contain sensitive, private or proprietary information.

Destroying documents is not illegal or unethical unless a company does so to hide something. This is addressed for public companies in the Sarbanes-Oxley Act of 2002:

18 USC Section 1519 - “Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.”



Here is a list of the typical documents that companies have with their retention period. This list is nonexclusive and may represent a small portion of what your company has. The periods listed are for reference only and are not to be implemented without first checking with your legal advisor, accountant, etc.

# Retention Schedule

## Corporate/Company Records

Articles of Incorporation	Permanent
Board/Committee Meetings	Permanent
Board Policies/Resolutions	Permanent
By-Laws	Permanent
Fixed Asset Records	Permanent
IRS Business Structure Letter	Permanent
Loan documents and notes	Permanent
Legal Correspondence	Permanent
Contracts (expired)	7 years
General Correspondence	3 years

## Accounting and Corporate Tax Records

Tax Returns and worksheets	Permanent
Annual Audits and Financial Statements	Permanent
Depreciation Schedules	Permanent
General Ledgers	Permanent
Chart of Accounts	Permanent
Business Expense Records	7 years
IRS 1099s	7 years
Journal Entries	7 years
Invoices (to customers/from vendors)	7 years
Sales Records	7 years
Petty Cash Vouchers	7 years
Cash Receipts	7 years
Credit Card Receipts	3 years

## Bank Records

Check Registers	Permanent
Bank Deposit Slips	7 years
Bank Statements/Reconciliation	7 years
Electronic Transfers	7 years

## Payroll and Employment Tax Records

Payroll Registers	Permanent
State Unemployment Tax Records	Permanent
Earnings Records	7 years
Garnishment Records	7 years
Payroll Tax returns	7 years
W-2 Statements	7 years

## Employee Records

Employment and Termination Agreements	Permanent
Retirement and Pension Plan Documents	Permanent
Records Relating to Promotion, Demotion or Discharge	7 years after termination
Accident Reports and Worker's Compensation Records	5 years
Salary Schedules	5 years
Employment Applications	3 years
I-9 Forms	3 years after termination
Time Cards, Payroll Records, Leave/Vacation	7 years
Donor Records and Acknowledgement Letters	7 years
Inventory records	7 years
Grant Applications and Contracts	5 years after completion

## Legal, Insurance and Safety Records

Appraisals	Permanent
Copyright Registrations	Permanent
Trademark Registrations	Permanent
Environmental Studies	Permanent
Insurance Policies	Permanent
Insurance Claims (in effect)	Permanent
Insurance Claims (expired)	3 years after close
Real Estate Documents	Permanent
Stock and Bond Records	Permanent
OSHA Documents	5 years
General Contracts	3 years after termination

# Emergency Planning

Disasters happen, both natural and man-made. Companies lose documents and files that are vital to the operation of the company. Companies need to have a plan on how to back up, store, and access their documents. Contact us today for help in implementing an information technology disaster recovery plan. For more information on preparing your company for a disaster visit [www.ready.gov](http://www.ready.gov).



## Other Documents

A partial list of documents not typically thought of as needing to be destroyed:

- Envelopes – they provide a list of who your customers are and who your vendors are
- Post-it notes – most times thought of as unimportant they contain meeting times, bid amounts, phone messages, etc.; smart businesses file these with their correspondences
- Memos – often time management leaves messages or memos for employees; they can reveal trade secrets, or proprietary information
- Photocopies – believe it or not many people feel that because a document is not an original it does not need to be treated the same and they simply throw the photocopy in the trash; if a document was made as a quick copy it still contains the same information as the original and should be shredded when no longer needed
- Misprints – ever had the printer spit something out that was only halfway legible; don't you think you should protect the other half that is legible?

**With a retention schedule in place the decision on what to destroy is a lot easier.**



**Once the time period has elapsed, documents need to be destroyed.**

## Destruction Process

**How are the documents going to be destroyed?**



Paper documents are typically destroyed by one of two methods – burning or shredding. Burning documents requires a constant high heat source such as an incinerator. While burning completely destroys the document it is time consuming and not environmentally friendly.

Destroying electronic documents is relatively easy. They can simply be deleted. However, this is only effective if the media on which they reside is going to remain within the company. For example, if a company has a computer in which it stores documents the company may simply delete the files according to its retention schedule. However, if the company is no longer using the computer and is going to sell or give the computer away, it should remove the hard drive and have it physically destroyed.



Destruction policies should not be long or complicated, short and easy to understand is the best approach.

## Particle Size

The most accepted and widely used method of destroying document is shredding. In short there are three different types of shredders – cross-cut, strip, and pierce and tear. Each type produces a different output particle size. Particle size refers to the size of the paper on the out put side of the shredder. Keep in mind that the smaller the output the more expensive the cost of the shredder. Government agencies typically *require* a cross-cut. Private companies should not exceed a 5/8 inch continuous strip shred.





# Disposal

Associated with determining particle size is determining how the shred is going to be disposed of. There are really only two options – trash or recycle. For companies that use small office shredders the option to simply throw the shred away is tempting because this means sending an employee to the dumpster. However, most office shredders are strip shredders and without bailing the paper, it leaves the paper shred easy access for dumpster divers. Some companies and almost all shred contractors practice diligence by recycling their shredded paper. Shred contractors have the advantage in that they mix the paper of many companies and bail it together.

*How often should you destroy documents and how should you collect paper to be shredded?*

A company needs to decide how often it will destroy its documents – daily, weekly, monthly, or annually. This does not seem complicated but remember there are different retention periods for different documents and there is the daily office paperwork. In addition to determining how often the destruction will occur is how the documents will be collected. Open paper ream boxes or file boxes are used in some offices but provide zero security. There are document collection containers that can be secured and provided for a centralized collection. Most shred contractors use such containers.



# Responsibility



No policy would be complete without naming the party who is ultimately responsible for seeing the policy enforced. This person should be knowledgeable in almost all the different types of paperwork and the retention schedule. This person should also be able to verify, with written records, that the destruction of the documents was completed.

The total responsibility for the destruction policy being implemented is not solely left to the person enforcing the policy. Every company employee needs to know and understand the importance of such policy. They also need to understand that failure to follow the policy could open the company to lawsuits.



Associated Records, Inc. has the expertise to assist you in protecting your company's secrets.

Call us today at 575.622.1515

## Who is going to do the actual shredding?

If done internally, companies typically do one of two things in shredding their company secrets. They either have their lowest paid employee do it or a well-paid office worker. Lowest-paid employees have been known to sell company secrets. Using well-paid office workers raises shred costs to unacceptable levels while decreasing their income-producing time.

If a company hires a shred contractor, it needs to research the company to ensure it will help them meet their destruction policy requirements.

