Document Management Policy Brought to You by Shred-it®

*(These are templates only and should be customized according to your organization's information security requirements.)*

*(Insert your company logo in the blue box provided on the right by clicking the picture icon.)*

**STATEMENT OF POLICY:**



**Document Management Policy**

**[Enter Your Company Name Here]­**

**Workplace Policy#:** Enter Policy Number Here

**Effective Date:** Enter Date Here

**Issued by:** Enter Name Here

**Approved by:** Enter Name Here

1. **PURPOSE**

The purpose of this policy is to assist [Enter Your Company Name Here] in managing all documents produced in the operation of the company. It will provide a clear and comprehensive understanding of which documents contain confidential information and how to manage, store, and securely destroy them. In addition, it explains which documents are legislated to be retained for requisite periods of time and the procedures governing their maintenance.

[Enter Your Company Name Here ] will help ensure that our employees:

* Retain important documents for reference and future use
* Dispose of documents that are no longer necessary for the proper functioning of the company through secure destruction and recycling in a Shred-it container
* Deliver obsolete electronic storage devices to IT for secure destruction
* Organize important documents for efficient retrieval
* Know which documents should be retained, the length of their retention, means of storage, and when and how they should be destroyed
* Ensure information will be available for legal investigations or actions as required

Implementation of and compliance with the policy is essential to its effectiveness. Incomplete or selective implementation exposes [Enter Your Company Name Here ] to legal risks. Therefore, each employee must understand and cooperate in the implementation and enforcement of the policy.

**Policy Administration**: Should any questions, comments or suggestion arise regarding this policy, please contact [Insert Team And Contact Information Here].

1. **SCOPE**

This policy will apply to all paper and electronic documents, confidential information, and general business information (as defined in Section 4 below) belonging to [Enter Your Company Name Here] or to which [Enter Your Company Name Here] is a party or signatory.

1. **RESPONSIBILITIES**

**Senior management** is responsible for ensuring that this policy is followed at all company locations. One member of senior management is appointed as the Document Control Administrator (DCA) with the responsibilities outlined below. Other members of senior management are responsible for applying this policy within their areas of responsibility.

The role of DCA is currently assigned to [Enter The Name Of The Position Responsible]. The DCA should advise and direct the implementation of this policy, including ensuring all employees are aware and have been trained on how to comply.

The DCA shall appoint departmental policy ambassadors to represent the needs for security and storage across the company.

**Employees**: All [Enter Your Company Name Here] employees are responsible for complying with this policy.

1. **DEFINITIONS**

**4.1. Documents and Records:** These refer to all business records documents of [Enter Your Company Name Here], including written, printed, and digital electronic records. Documents include, but are not limited to, papers, photocopies, drafts, bound records, drawings, maps, photographs, electronic communications, and any other physical device containing information, including electronic storage devices. The term includes any and all copies or originals taken, moved, or sent off any [Enter Your Company Name Here] site and are within [Enter Your Company Name Here] control.

**4.2 Electronic Storage Device**: Refers to any and all electronic storage devices that were provided by or contain information that is the property of [Enter Your Company Name Here], are under [Enter Your Company Name Here] control, and are used by any of its employees, contractors, officers, or directors. Electronic storage devices include personal computers, servers, laptops, and related storage devices such as hard drives, flash drives, and CDs.

**5. STORAGE OF RECORDS AND DOCUMENTS**

**5.1 Tangible Records:** Tangible documents that *do not* contain confidential information are those that can be physically moved to storage. These may include paper records (including printed versions of electronically saved documents), photographs, investor presentations, promotional items, etc. These active, tangible records and documents that need to be easily accessible may be stored in [Enter Your Company Name Here] office space or equipment.

**5.2 Confidential Information:** Documents that contain confidential information but are in use should be stored in the locked storage of the responsible individual accountable for them. All confidential information shall be kept out of view from unauthorized personnel and locked up when not in use.

**5.3 Inactive Documents**: These records can be sent to an off-site storage facility. This off-site storage facility must be evaluated for security and reliability by [Enter The Name Of The Position Responsible], which is to be reviewed periodically by the DCA.

**5.4 Legal and Financial Regulations**: Please note that in some jurisdictions   
and domains, human resource, legal, and financial documents may have specific  
rules and regulations governing their retention, distribution, storage, and destruction. Please contact the DCA for specific information, direction, and practices regarding those documents. See Appendix A.

**6. DOCUMENT DESTRUCTION PROCEDURES**

This section describes the process of document destruction for all types of information that is recorded by employees including **confidential information** and **general business Information.**

At [Enter Your Company Name Here], our document management policy requires that all documents and all information deemed to be no longer needed, required, or retained is to be destroyed through the Shred-it secure recycling process. Specifically, this means that all paper documents, including **confidential information** and **general business information**, should be placed in a locked Shred-it container for destruction and secure recycling when no longer required.

We also require that all electronic storage devices that are no longer in use be disposed of through secure hard drive destruction. It is the IT department’s responsibility to immediately dispose of obsolete hard drives.

**APPENDIX A: DOCUMENT RETENTION SCHEDULE**

To help you create the right retention schedule for your business, here’s a non-exhaustive list of documents that may contain confidential information or that may be subject to retention obligations. These recommendations are general guidelines only. They are not intended to represent legal advice. Contact your legal expert(s) or federal, state, or provincial government to ensure you are following current legal requirements for your area.

|  |  |
| --- | --- |
| **TYPE OF RECORD/SPECIFIC RECORD**  **Accounting Records**  Annual financial statements  Data for acquired/divested business  Monthly financial statements  General ledger  Annual audit records  Journal entries  Cancelled checks  A/P paid invoices  Business expense records  Data for non-acquired/non-divested business  Accounts payable  Accounts receivable  Audit reports  Expense records  Loan documents  Purchase orders  Sales records  Bank reconciliations  **Tax Records**  Payroll tax Returns  Federal tax returns (not payroll)  Local/provincial/state returns  Supporting documentation for taxes  **Purchasing and Sales**  Purchase orders  Requisitions  Sales contracts  Sales invoices  **Insurance Records**  Policies (including expired)  Claims for property loss/damage Accident Reports Appraisals  Settled insurance claims  **Legal and Workplace Records**  General contracts  Real estate contracts & records  **Personnel**  Attendance records  Contracts  Benefits  Disability claims  Employment applications  Performance records – after terminations  Personnel files – terminated  Withholding tax statements  **Traffic - Shipping and Receiving**  Export declarations  Freight bills  Manifests  Shipping and receiving reports  Waybills and bills of lading | **RETENTION PERIOD** |

[Enter The Name Of The Position Responsible] is designated with the responsibility and authority to file, store, and/or archive the information outlined above.