**STATEMENT OF POLICY AND PROCEDURE**

**Document Management Policy**

**[ Enter Your Company Name Here ]**

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

**Effective Date:**

**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, which documents are legislated to be retained for requisite periods of time and the procedures governing their maintenance.

[ Enter Your Company Name Here ] will 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
* Organise important documents for efficient retrieval;
* Know what documents should be retained, the length of their retention, means of storage, and when and how they should be destroyed;
* Comply with laws regarding the retention of records and data
* 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 CONTACT NAME AND TITLE Here ].

1. **SCOPE**

This policy will apply to all printed 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” with responsibilities outlined below. Other members of senior management are responsible for applying this policy within their areas of responsibility.

The role of **Document Control Administrator** (“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** (used interchangeably) refer to all business records of   
[ Enter Your Company Name Here ], including written, printed, as well as electronic records (i.e., e-mails and documents saved electronically). Documents and records include but are not limited to papers, copies, 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 ] premises and within [ Enter Your Company Name Here ] control.

**4.2 Confidential Information** – all information that is produced in the course of [ Enter Your Company Name Here ] business that is not available from public sources is considered confidential. In general, any or all documents or files that contain business, client, partner or employee names, pricing, and personal information. This includes, but is not limited to, [ Insert ANY SPECIFIC DOCUMENT-TYPES here ]. This also includes private information on individuals as defined by the Data Protection Act (1998), as well as information that is available to our company as a result of our business practice(s) but which is not generally known or readily obtainable by others outside of our business but can be used in general throughout our business.

**4.3 General Business Information** – General business information documents including, but not limited to:

|  |  |
| --- | --- |
| Accounting documents  Information technology documents  General Contracts  Customer lists  Internal reports  Payroll statements  Training information and manuals  Executive level budgets  Customer correspondence  Legal contracts  Strategic reports  Health and safety records  Medical records  Payroll information  Performance appraisals | Corporate legal records  Supplier purchase orders  Supplier records  Supplier specifications  Research and development reports  Performance appraisals  Product testing and results  Product development plans  Sales and marketing reports  Specifications and drawings  Internal communications  Advertising materials  Business strategies |

**4.4 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 records that *do not* contain confidential information are those that can be physically moved to storage; such as paper records (including printed versions of electronically saved documents), photographs, investor presentations and 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 –** Records and documents that contain Confidential Information but are in use should be stored in the locked storage of the responsible individual accountable for them. Each employee shall be provided at least one lockable drawer/cabinet to store documents that should be kept off their desktop. All confidential information shall be kept out of view from unauthorised 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 Document Control Administrator (“DCA”) for specific   
information and 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 are to be destroyed through the Shred-it secure recycling process. Specifically, this means that all printed 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 departments’ 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 list of documents that contain confidential information. These recommendations are general guidelines only. They are not intended to represent legal advice. Contact your legal expert(s) or government or regulatory authority 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 cheques  A/P paid invoices  Business expense records  Data for non-acquired/non-divested  Accounts payable  Accounts receivable  Audit reports  Expense records  Loan documents  Purchase orders  Sales records  Bank reconciliations  **Tax Records**  PAYE records  VAT records  Corporation Tax records  Supporting documentation for taxes  **Purchasing and Sales**  Purchase Orders  Requisitions  Sales Contracts  Sales Invoices  **Insurance Records**  Policies (including expired)  Claims for loss/damage,  Accident reports, appraisals  Settled Insurance Claims  **Legal and Workplace Records**  General Contracts  Premises contracts & records  **Personnel**  Attendance Records  Contracts  Benefits  Disability  Employment Applications  Performance Records – After Terminations  Personnel Files – Terminated  **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.