# Information Disposition and Retention Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

|  |  |
| --- | --- |
| **Policy Owner** | Name the person/group responsible for this policy’s management. |
| **Policy Approver(s)** | Name the person/group responsible for implementation approval of this policy. |
| **Related Policies** | Name other related enterprise policies both within or external to this manual. |
| **Related Procedures** | Name other related enterprise procedures both within or external to this manual. |
| **Storage Location** | Describe physical or digital location of copies of this policy. |
| **Effective Date** | List the date that this policy went into effect. |
| **Next Review Date** | List the date that this policy must undergo review and update. |

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The purpose of this policy is to provide a corporate policy framework to govern decisions on whether, in any given case, a particular document or set of documents should be retained, and if so, in what form and for what period.

[Company Name] aims to ensure that:

* + Compliance with all legislation, regulations, and standards concerning the proper management of information sources is undertaken.
	+ All information sources are properly titled, described, indexed, referenced, and where necessary, security marked.
	+ Our existing information remains relevant and useful by removing low value or incorrect information from our stores.
	+ Appropriate training is provided to staff dealing with the management of information sources.
	+ Disposal techniques are carried out securely by only those who are authorized.
	+ All employees are active participants in managing information as an asset to ensure they can perform their tasks efficiently.
	+ Reviews are carried out at regular intervals and amendments are made when appropriate.
	+ [Expand based on specific needs.]

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

* This policy applies to all departments, divisions, sections, and services of [Company Name] and all information sources created and received by employees of [Company Name], regardless of the format or media type.
* It shall apply to records and information sources that exist solely in electronic format. Departmental Information Management Policies will specify the electronic and hard copy retention periods for documents in each area.
* This policy is not concerned with the disposal/retention of unused materials such as stocks of paper, unused forms, materials, or equipment that do not comprise, or form part of, a record of a business activity/transaction.

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

1. **Personal data.** This is defined as any information from which a person can be identified, from names and addresses to photographs and ID numbers.
2. **Sensitive data.** This is defined as anything relating to: political opinions, racial or ethnic origin, religious or similar beliefs, trade union membership, physical/mental health or condition, sexual life, offences or criminal proceedings.
3. **Records.** These are defined as information maintained by an organization or person for the purpose of legal obligations or in the transactional business.

# Governing Laws & Regulations & Standards

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

|  |  |
| --- | --- |
| **Guidance** | **Section** |
| ISO 5454:2000 | Recommendations for the storage and exhibition of archival documents. |
| ISO 15489 | Standard on best practice in records management. |
| ISO 7799 | Standard on information security management. |
| DISC PD 0008:1999 | Code of practice for the “Legal admissibility and evidential weight of information stored electronically”. |
| DISC PD 0010:1997 | The principles of good practice for information management. |

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

All records must be retained in our dedicated systems: the “system of record.” [Company Name] has three systems of record: [ERP, CRM, and Y system; *replace with the names of systems the users use].* Records will be held, classified, and disposed based on the appropriate regulations under the guidance of the [Information Governance Leadership (IGL) and the compliance office]. Users should take no actions to store, transmit, or modify records outside of the system of record and its associate applications.

1. [Information Asset Officers (IAOs)] are designated by the [Information Governance leadership council] and are responsible for ensuring that the enterprise-wide Information Governance program is carried out at the department level.
2. Information is an asset and will be valued based on its worth as an asset.
* In order to appropriately focus on information that is highly valuable to [Company Name], all information sources will move to a disposition schedule that matches the value of that asset to [Company Name].
* Information sources that contain information that is of low value to the organization as a whole will be occasionally purged. All users of that information source will be made aware of the purge schedule. As the [IGL and department level IAOs] cannot be expected to understand and be appraised of the value of all information being generated by end users, it is expected that end users will be an active participant by ensuring that information is appropriately valued.
* The assessment of information sources will be reviewed on an [annual] basis or when the business use of the information source is altered. All decisions on information value reside primarily with [the IAO council] and require approval of [the IGL].
1. A Record Retention Schedule will be maintained outlining the value of information sets as well as the associated retention and disposition procedures. The retention and disposition of records/information will conform to this schedule unless otherwise advised by [role/position].
2. Documents of high value to [Company Name] may be required to be retained for a long period, even permanently. Documents can be retained to ensure the preservation of documents of historic or other value, to meet operational needs, to fulfil statutory or other regulatory requirements, and to evidence events/agreements in the case of dispute(s).
3. Documents that have not been accessed in [XX year(s)] will be moved to an archival location. Access to these documents in the archive location will require the approval of their local [Information Asset Officer] to restore these files to active storage.
* Documents that exist only in our tape backups will only be restored when the value of the information retrieved is greater than the cost of recovery.
* Similarly, storage formats have changed greatly in the last [XX years] and tape backups more than [XX years] old require specialized consulting firms to recover the information.
* The exception to the above rule is the project-specific folders [work-in-progress] and [final]. The final folder represents historical records that [Company Name] has identified as high value. Any final project deliverable will be stored in our archival location and will be searchable through file name or author.
1. Users that work with high value or high risk documents should identify those documents at the time of creation and store them in the appropriate location. If you are unclear as to what type of document you are working with, contact [the departmental IAO or your manager].
2. Consideration must be given to the location and controls needed to maximize the value of documents while maintaining sufficient control of access and modification. The higher the potential value and/or risk, the stricter rules governing storage and access need to be to ensure the asset is maximized. This decision is to be made by the [Manager or IAO, or a designated SME] that has received appropriate training and approval from [the IAO council].

Responsibility for determining whether to retain or dispose of specific documents rests with the [Records Officer] in respect of those documents that properly fall within the remit or control of their service. However, it is expected that all employees that handle records will be trained, and will follow the organizational rules governing records. As such, the main role of the [records officer(s)] is education and training of identified workers. [The officer] must be fully acquainted with this policy and also familiar with the operational requirements of the particular service so that a valid assessment of the documents can be established.

Whenever there is the possibility of litigation, the records and information that are likely to be affected should not be amended or disposed of until the threat of litigation has been removed.

When records identified for disposal are destroyed, a register of such records needs to be kept. It is not sufficient to document that a quantity of records had been destroyed on a certain date. Enough details should be retained to identify which records have been destroyed.

* It is essential that any paper records destroyed, which contain personal or sensitive information, are either shredded or destroyed via the confidential waste service.
1. Directors/Managers shall ensure that they proactively undertake an audit trail of the training of new employees and will ensure that they stay knowledgeable of the retention and storage policies that govern information.
2. Legal advice may be sought to establish whether minimum retention periods are prescribed by law. However, Legal Officers cannot be expected to acquire the operational background knowledge required to assess the minimum retention period of a specific document within a department; the manager(s) or designated officer(s) are best placed to make such an assessment.
3. Individual employees are responsible for ensuring that:
* Disposal procedures are implemented consistently
* The Corporate Record Retention and Disposal Policy is followed
* Actions taken with regards to disposal or retention are properly recorded
1. All records will be handled, stored, and disposed of in accordance with our legal and regulatory obligations.

* In essence, the disposal record should be able to demonstrate that the disposal was in accordance with this Retention and Disposal Policy or in very exceptional circumstances, provide explanations for departing from it.
* However, the Modern Records system will identify the date on which boxes are destroyed. The eForm will also identify the number of bags disposed of.
1. This Policy will be annually reviewed and revised; updates, amendments, and changes to both the policy itself and the Retention Schedules will be recorded.

* Any amendments will be logged on the next policy version and if significant changes are made, they will be reported to and agreed by Council. “Significant changes” is taken to include a major structural change to the approach taken to document management or external legislative requirements that require wholesale changes to the general approach to document retention.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Agreement

Include a section that confirms understanding and agreement to comply with the policy. Both signatures and dates are required. A sample statement is provided below.

I have read and understand the [name of policy]. I understand that if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or company policy.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Name

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Signature Date

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For acceptable use of this template, refer to Info-Tech's [Terms of Use](http://www.infotech.com/terms). These documents are intended to supply general information only, not specific professional or personal advice, and are not intended to be used as a substitute for any kind of professional advice. Use this document either in whole or in part as a basis and guide for document creation. To customize this document with corporate marks and titles, simply replace the Info-Tech information in the Header and Footer fields of this document.