# Data Archiving 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.

Information maintained by [Company Name] is a vital asset that will be available to all employees who have a legitimate need for it, consistent with [Company Name]'s responsibility to preserve and protect such information by all appropriate means.

[Company Name] has various data retention and archiving requirements to meet local compliance and regulatory constraints, contract obligations, and promises made to employees, customers, and partners. In the event that [Company Name] becomes involved in litigation or business disaster recoveries that requires access to original data to protect [Company Name]’s interests or those of our employees, customers, and/or partners, data must be archived appropriately and available for retrieval.

Where Big Data is being considered for archiving, only data that is critical and required for compliance purposes will be archived. Archiving too much Big Data will result in higher storage and retrieval costs.

# 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 critical data in [Company Name], including data outside of [Company Name] stored in a cloud service. “Critical data,” in this context, includes email, personal and shared files, specific databases and web contents, and operating systems. The definition of critical data, and scope of this policy, will be reviewed on an annual basis.
* This policy applies to *staff* who may be creators and/or users of such data. The policy also applies to third parties who access and use [Company Name] systems and IT equipment or who create, process, or store data owned by [Company Name].
* This policy does not cover retention periods, only archival. Records retention policies are documented separately.

# Definitions

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

1. **Big Data.** This is defined as a data set that is so large in volume that it becomes difficult to process using traditional means.

# Governing Laws & Regulations

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.

# 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.

1. Data must be archived in a way that it can be swiftly and inexpensively located and used, amended or destroyed, and monitored and secured.
2. Data owners are responsible for regularly reviewing whether their data shall be immediately available on a day-to-day basis or whether it is sufficient for the data to be made available within a period of a few days or weeks.
3. The IT [applicable committees] are responsible for securing appropriate data archival technology and storage on or off-site. Data owners are responsible for documenting their data archive and retrieval procedures, and performing the data archive.
4. Data owners are responsible for periodically testing the data archive retrieval procedure to ensure data remains available when required.
5. Data owners must keep a running inventory of their archived data sets.
6. All requests for exceptions to data archiving policies must be made in writing to the [applicable committee]. Email requests are acceptable. The request must specify the exception, justification, and implications.
7. Archived data that contains sensitive personal information or business sensitive information is subject to the same controls as live data as governed by the data protection and security policies.

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

Data archive retrieval approval procedure.

1. Establish the need.
2. Determine which data sets need to be retrieved.
3. Contact the data owner with a formal request to retrieve the data sets. An estimate of how long the data will be required is mandatory.
4. If any sensitive personal information or business sensitive information is included in the data being retrieved, include protective measures that meet with [Company Name]’s data protection and privacy policy(s).
5. Wait for confirmation from the data owner that the data has been retrieved.
6. Once the data has been used and is no longer required, inform the owner that it can be returned to the archive.

# 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.