# Data Management 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.

This policy establishes uniform data management standards and identifies the shared responsibilities for assuring the integrity of the data and that it efficiently and effectively serves the needs of [Company Name]. [Company Name] values access to, and the timeliness, accuracy, and consistency of information, while fully appreciating the basic security and privacy requirements involved. Controlled access by employees to administrative information is necessary in order to support business functions.

# 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].

# Definitions

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

# 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. All corporate data is owned by [Company Name] and, as such, all staff of [Company Name] are responsible for appropriately respecting and protecting the asset.
2. In order for [Company Name] to effectively manage and safeguard the data assets, procedures must be in place to guide appropriate data access, ensure the security of the data, and provide a means to address procedural exceptions.
3. Roles, including those both of individuals with data responsibilities and of eligible users, are necessary to support data integrity and security.
4. Sharing information across organizational boundaries should be facilitated where appropriate.
5. A sustained data administration function should reinforce a set of definitions for commonly consumed data, with the understanding that there may be multiple valid definitions.
6. Data integration across [Company Name] should be encouraged to foster data accuracy and uniformity, and demonstrate an understanding of [Company Name’s] institutional complexity, various data systems, and differing data formats.
7. Data should be safeguarded to maintain the confidentiality and privacy of personally identifiable information; such safeguards should be balanced and reflect the necessity for [Company Name] to conduct its business.
8. Access to [Company Name] data should be based on the business needs of the organization and should enhance the ability of [Company Name] to achieve its mission. Employees should have access to the data needed to perform their responsibilities, without regard to arbitrary barriers. In many cases, that data need not be individually identifiable.
9. Before individuals will be allowed to access [Company Name] data, training in the use and attributes of the data, functional area data policies, and [Company Name] policies regarding data is mandatory.
10. A terminology/taxonomy shall be developed by the [Data Stewardship Advisory Group], or an appropriate subset, in order to provide a framework for requesting and producing consistent data across all levels of the enterprise. The definitions shall be accessible to all [Company Name] data users and shall be included in training.
11. Data, as a [Company Name] asset, must be safeguarded and managed at all points and across all systems, from creation, to use, to archive, through coordinated efforts and shared responsibilities to ensure its accuracy. Each functional area will develop and implement processes for identifying and correcting erroneous or inconsistent data. When and if erroneous or inconsistent data has been identified, the [Data Steward] from the corresponding functional area shall within five business days either correct the data or escalate the issue to the appropriate Data Owner and [the Data Governance Steering Committee]. Information Technology services will develop and implement data auditing processes.
12. Any exceptions to this policy will be fully documented and approved by [the IT steering committee].
13. Extraction, manipulation, and reporting of [Company Name] data must be done only for [Company Name] business purposes:
	* Personal use of [Company Name] data, including derived data, in any format and at any location, is prohibited.
	* Where appropriate, before any information is used outside the Data User's functional unit, verification with the functional area manager and data owner is recommended.
14. Before decisions are made concerning data retention and data archiving, the appropriate Data Users must be consulted.
15. Individuals that seek permission to access data outside of the access plan and defined roles must submit a written request seeking non-standard access.
* This request should include a statement indicating the access being sought and the reason for the request, and should be submitted to [the Chair of the Data Governance Steering Committee].
* [The Chair] will send the request to the appropriate Data Steward for review and decision. The Data Steward will report the decision to the appropriate Data Owner and to the requestor's manager.

# 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.