# Data Security 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 document defines the data security policy of [Company Name]. [Company Name] takes the privacy of our employees and clients very seriously. To ensure that we are protecting our corporate and client data from security breaches, this policy must be followed and will be enforced to the fullest extent.

The purpose of this policy is to inform employees at [Company Name] of the rules and procedures relating to data security compliance.

# 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 data, but is not limited to electronic information found in email, databases, applications, and other media, or paper information, such as hard copies of electronic data, employee files, internal memos, and so on. It is inclusive of data outside of [Company Name] stored in a cloud service, and/or held on a mobile computing device.

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 applies to all employees, management, contractors, vendors, business partners, and any other parties who have access to company data.

# Definitions

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

### Data Types

1. **Company-owned data.** This is defined as data that relates to such areas as corporate financials, employment records, payroll, etc.
2. **Private data.** This is defined as data that is the property of clients and/or employees, such as social security numbers, credit card information, contact information, etc.

### Data Classifications

1. **Public/Unclassified Data.** This is defined as information that is generally available to anyone within or outside of the company. Access to this data is unrestricted, may already be available, and can be distributed as needed. Public/unclassified data includes, but is not limited to, marketing materials, annual reports, corporate financials [and other data as applicable].
2. **Private Data.** This is defined as corporate information that is to be kept within the company. Access to this data may be limited to specific departments and cannot be distributed outside of the workplace. Private data includes, but is not limited to, work phone directories, organizational charts, company policies [and other data as applicable].
3. **Confidential Data.** This is defined as personal or corporate information that may be considered potentially damaging if released and is only accessible to specific groups [e.g. payroll, HR, etc.]. Confidential data includes, but is not limited to, social security numbers, contact information, tax forms, accounting data, security procedures [and other data as applicable]. [Company Name] considers it a top priority to protect the privacy of our clients and employees. A separate privacy policy [provide link] outlines our commitment to protecting personal data.
4. **Secret/Restricted Data.** This is defined as sensitive data which, if leaked, would be harmful to [Company Name], its employees, contractors [and other parties as applicable]. Access is limited to authorized personnel and third parties as required. Secret/restricted data includes, but is not limited to audit reports, legal documentation, business strategy details [and other data as applicable].

# 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. Any employee who authors or generates corporate or client data must classify that data according to the data types and classifications defined above.
* All information not otherwise classified will be assumed to be Private.
1. It is the responsibility of everyone who works at [Company Name] to protect our data. Even unintentional abuse of classified data will be considered punishable in accordance with the extent and frequency of the abuse.
2. Employees may send or communicate a public/unclassified piece of data with anyone inside or outside of the company.
3. Employees may not disclose private data to anyone who is not a current employee of the company.
4. Employees may only share confidential data within the department or named distribution list.
5. Secret/restricted data cannot be disclosed by anyone other than the original author, owner, or distributor.
6. Data that falls under Private, Confidential, and/or Secret/Restricted classifications must be encrypted with minimum [128-bit cryptography] while in transit and at rest. This includes data stored on corporate systems and mobile computing devices, including personal devices used to access corporate systems.
7. All [Company Name] employees are responsible for adhering to the policy and reporting any activities that do not comply with this policy.
8. Management is responsible for ensuring that their direct reports understand the scope and implications of this policy. HR must also ensure that all employees have a signed copy of this policy in their file.
9. Security staff will be monitoring data for any unauthorized activity and are responsible for updating access requirements as needed.
10. These are the accepted technologies [Company Name] used to enforce and ensure data security:
* Access controls
* Strong passwords
* System monitoring
* [other]
1. This policy will be reviewed [annually/quarterly] or as circumstances arise.
* Also [annually], a full security audit will be performed by [a third-party auditing firm, the security team, etc.] to ensure that the policy is properly aligned with [company directives, SOX, HIPAA, etc.].
1. Ownership of this policy falls to [role, department]. For any questions about this policy, or to report misuse of corporate or personal data, please contact him/her at [phone number/email address]. The IT department will work in conjunction with [the policy owner] to maintain data access privileges, which will be updated as required when an employee joins or leaves the company.

# 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.