# Data Protection 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.

Data protection mechanisms allow information to be provided a greater level of security than can be achieved with system-based protection mechanisms alone. Without data protection mechanisms, the potential exists that [Company ABC]’s information assets could be exposed to an unnecessarily high level of risk, particularly in circumstances where data is taken out of the information system.

# 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 Data Protection Policy applies to all data assets of [Company ABC]. Specifically, it includes:

* Intellectual Property (IP), whether owned by [Company ABC] or provided by a third party.
* Personally Identifiable Information (PII) for employees, clients, or other third parties.
* Business Sensitive Information (BSI) for [Company ABC], partners, or other third parties.
* Financial information for [Company ABC], its employees, clients, or other third parties.
* Other non-public data or information assets deemed the property of [Company ABC].
* Other public data or information assets deemed the property of [Company ABC].

# 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 privileged information, whether stored in system or out of system (via information media) will be protected by data protection mechanisms to ensure the highest levels of confidentiality, integrity, and availability. Non-privileged information will be protected to ensure the highest levels of integrity and availability.
2. Only personnel that have previously been authorized are allowed to enter information into an information system. Inputs will be restricted according to granted permissions, though these restrictions may be lifted on a temporary basis based on pre-defined project responsibilities. In such circumstances, additional authorization is required and must be granted before restrictions are lifted.
3. Where possible, information systems will check entered information for accuracy, completeness, validity, and authenticity. These checks will be performed as close to the point of information entry as possible and will attempt to ensure that data corruption does not occur or that entered information cannot be interpreted as system commands by the information system.
4. Information systems will be configured such that they prevent unauthorized and unintended information transfer. Further, information systems will protect the integrity and confidentiality of transmitted information using [indicate controls – suggest session authentication, session encryption, data encryption].

**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.

**Procedure 1**

Configure systems to store confidential and sensitive data in a secure manner:

* + - * + Where possible, data encryption should be used for all confidential data at rest.
        + Data encryption solutions should be centrally managed with key escrow.

**Procedure 2**

Positively dispose of data that is no longer required:

* + - * + Use software or hardware delete functions to remove non-confidential data from systems once that data is no longer required.
        + Use dedicated media wiping solutions to permanently remove confidential data from systems once that data is no longer required.

**Procedure 3**

Configure systems to transmit confidential and sensitive data in a secure manner:

* + - * + Where possible, encrypted tunnels should be used for all electronic data transmissions.
        + Whether encrypted tunnels can or cannot be used for electronic data transmissions, data should be directly encrypted prior to transmission.
        + Message digest hashes should be created and supplied for all electronic data transmissions.

**Procedure 4**

Configure systems to restrict and validate data input:

* + - * + Data should only be input by those with appropriate accounts and account permissions.
        + Data should only be input according to established syntax parameters.
        + Inputted data should be checked for accuracy, authenticity, completeness, and validity by the system.

# 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 ABC]. 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 ABC] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.