Data Classification Policy

|  |  |
| --- | --- |
| Policy Area | IT Policy Library |
| Approved Date | December 31, 20XX |
| Approved By | Policy Committee |
| Effective Date | January 1, 20XX |
| Current Version | 1.0 |

# I. Overview

Data Classification provides a framework for managing data assets based on value and associated risks and for applying the appropriate levels of protection as required by state and federal law as well as proprietary, ethical, operational, and privacy considerations. All ABC Company data, whether electronic or printed, should be classified. The data owner, who is responsible for Data Classification, should consult with legal counsel on the classification of data as Public, Sensitive, or Confidential. Consistent use of data classification reinforces with users the expected level of protection of ABC Company data assets in accordance with ABC Company security policies.

# II. Purpose

The purpose of this policy is to provide a foundation for the development and implementation of necessary security controls to protect information according to its value and/or risk. Security standards, which define these security controls and requirements, may include: document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures.

# III. Scope

This policy applies to all Staff that use ABC Company Information Resources.

# IV. Policy

Data shall be classified as listed below.

Public. Information intended or required for public release. Disclosure of such information does not adversely impact ABC Company’s business operations, financial well-being, or our image and reputation.

Sensitive. Sensitive data that requires additional levels of protection. Examples of sensitive data include but are not limited to:

* Operational information
* Personnel records
* Information security procedures
* Research
* Internal communications
* Log records (firewall logs, audit trails, etc.).

Confidential. Sensitive data that must be protected from unauthorized disclosure or public release based on state or federal law, and other constitutional, statutory, judicial, and legal agreements. Examples of “Confidential” data may include but are not limited to:

* Personally Identifiable Information, such as: a name in combination with Social Security Number (SSN) and/or financial account numbers
* Employment Records
* Intellectual Property, such as: Copyrights, Patents and Trade Secrets
* Medical Records

Controlled Unclassified Information (CUI). Information, excluding Classified Information, that requires safeguarding or dissemination controls required by laws, regulations, or Government-wide policies.

Access to authentication data shall be restricted to authorized personnel through the use of encryption, file access controls, or both encryption and file access controls.

# V. Enforcement

Any Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination.

# VI. Distribution

This policy is to be distributed to all ABC Company Staff.

**Policy History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description | Approved By |
| 1.0 | 1/1/20XX | Initial policy release |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**References:**

COBIT EDM01.01, EDM03.02, APO01.11, APO14.01-02, APO14.07, APO14.10, BAI02.05

GDPR Article 9, 10

HIPAA 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E)

ISO 27001 A.8.2

NIST SP 800-37 P-10

NIST SP 800-53 PM-29, RA-2

NIST Cybersecurity Framework ID.AM-2-3, ID.AM-5

PCI 3.1, 12.2