Data Marking 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

ABC Company’s Information Systems contain sensitive information that must be protected from unauthorized access throughout all phases of the information lifecycle. By properly marking data, ABC Company helps ensure that it can be properly protected.

# II. Purpose

Failure to protect sensitive information can lead to fraud, waste, abuse, and other negative outcomes that ultimately damage both the business and our relationships with customers, suppliers, and other critical entities. This policy also helps manage risks related to legal and compliance requirements and our ability to continue business operations.

# III. Scope

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

# IV. Policy

Staff in both IT and business roles shall use physical and technical mechanisms to ensure secure handling, transfer, and storage of data via electronic and paper documents, printouts, backup media, electronic storage, and removable media. Staff must also consider sensitive information that may be saved on media and equipment slated for disposal.

All hardware, output, and media that contain Sensitive Information shall be clearly marked.

A. General

All Sensitive Information and material shall be marked to clearly convey to the holder the level of classification assigned, the portions that contain or reveal Sensitive Information, the period of time protection is required, and any other notations required for protection of the information.

* Hardware Components. All components of an information system, including input/output devices that have the potential for retaining information, terminals, stand-alone microprocessors, or word processors used as terminals, shall bear a conspicuous, external label that states the highest classification level and most restrictive classification category of the information accessible to the component in the Information System. This labeling may be accomplished using permanent markings on the component, a sign placed on the terminal, or labels generated by the IS and displayed on the screen.
* Hard Copy Output and Removable Media. Output (paper, fiche, film, and other printed media) and removable media shall be marked with visible, human-readable, external markings to the level of the information.
* Unclassified Media. In the approved areas where classified and non-classified information are processed on collocated information systems, unclassified media shall be so marked.

B. Identification markings

All classified material shall be marked to show the name and address of the party responsible for its preparation, and the date of preparation.

* Files, Folders, or Groups of Documents. Files, folders, binders, envelopes, and other items containing Sensitive Information, when not in secure storage, shall be conspicuously marked.
* E-mail and other Electronic Messages. Electronically transmitted messages shall be marked in the same manner required for other documents except as noted. The overall classification of the message shall be the first item of information in the text. A "Derived From" line is required on messages. Certain departments may also require that messages contain a "Classified By" and a "Reason Classified" line in order to identify the derivative classifier and the specific reason for classification. Instructions for the use of such lines will be included in the security classification guidance provided with the contract documents. When messages are printed by an automated system, all markings may be applied by that system, provided the classification markings are clearly distinguished from the printed text. The last line of text of the message shall include the declassification instructions.
* Derivative. A new document or copy shall be marked with the same classification markings as applied to the information or document from which the new document or copy was prepared.
* Not classified. If the information was not previously classified, the information shall be protected as though classified at the appropriate level and submitted to the appropriate department for a classification determination. In such a case, the following marking, or one that clearly conveys the same meaning, may be used and shall conspicuously appear on the material:

CLASSIFICATION DETERMINATION PENDING

Protect as though classified as Confidential

Electronic output to be released outside the security boundary shall be verified by a comprehensive review (e.g. in human readable form) of all data on the media including embedded text (e.g., headers and footer) before being released. Information on media that is not in human-readable form (e.g., embedded graphs, sound, video, etc.) shall be examined for content using the appropriate software application. Random or representative sampling techniques may be used to verify the proper marking of large volumes of output.

C. Inadvertent Release

The following steps shall be performed if Sensitive Information is inadvertently distributed outside the company without the proper classification assigned to it, or without any markings to identify the material as classified:

* Determine whether all holders of the material are cleared and authorized access to it.
* Determine whether control of the material has been lost.
* If recipients are cleared for access to the material, promptly provide written notice to all holders of the proper classification to be assigned. If control of the material has been lost, if all copies cannot be accounted for, or if unauthorized personnel have had access to it, report the compromise to management.
* Media shall be protected until an appropriate classification review has been conducted. An appropriate sensitivity and classification review shall be performed on human readable output before the output is released outside the security boundary to determine whether it is accurately marked with the appropriate classification and applicable associated security markings.

D. Responsibilities

The Chief Security Officer shall be responsible for approving documented processes that:

* Ensure security during reproduction of sensitive data files.
* Ensure security during receipt or sending of media that contains sensitive data.
* Log transmittal and transport records related to media that contains sensitive data.
* Investigate and resolve any discrepancies between internal records and transmittal and transport logs.
* Defines in the security plan disposition procedures for media no longer used to process or store sensitive information.

Department heads shall:

* Train employees on security requirements for equipment and media containing sensitive information.
* Monitor employee activities to ensure compliance with security policies and procedures.
* Work with System Administrators to ensure that only authorized software runs on automated information systems.
* Approve, as needed, reproduction of sensitive data files.
* Sign for, or delegate authority to sign for, receipt of registered, certified, or express mail which can contains sensitive data.
* Review transmittal logs and transport records on a weekly basis to account for all removable media that contains sensitive information.
* Investigate and resolve any discrepancies between internal records and transmittal and transport logs.
* Work with the Chief Security Officer to define disposition procedures for media no longer used to process or store sensitive information.
* Establish and communicate requirements for protecting systems and data
* Ensure that sensitive data is not stored on personal computers.
* Track sensitive data from creation through destruction.

Staff shall:

* Adhere to security requirements for the protection of sensitive data and systems.
* Appropriately identify, date, and mark sensitive information they are responsible for originating, producing, or processing.
* Ensure that media containing sensitive data is appropriately labeled.
* Ensure that media containing sensitive data is stored in secure locations and/or containers.
* Ensure that media does not contain both sensitive and non-sensitive information.
* Ensure that sensitive information is not left on output devices after printing.
* Sign for all data sent, received, or transported.
* Shred sensitive printed documents and follow secure disposition procedures for media.

# 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, APO13.07, APO14.01-02, APO14.07, APO14.10

GDPR Article 32

HIPAA 164.308(a)(7)(ii)(E)

ISO 27001 A.8.2.2, A.8.2.3, A.8.3

NIST SP 800-37 3.2, 3.3

NIST SP 800-53 AC-16, MP-3, PE-22

NIST Cybersecurity Framework ID.AM-2, ID.AM-3, PR.PT-2, DE.DP-2, DE.CM-2

PCI 9.9.2