**Cybersecurity Templates**

**Dat Classification Policy**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Data Classification Policy** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy No:** | [Assign Number] | **Effective Date:** | [Insert Date] |
| **Owner:** | [CISO / IT Security Manager] | **Review Cycle:** | [Annual / Biennial] |

Contents

[Data Classification Policy 3](#_Toc207016823)

[1. Purpose 3](#_Toc207016824)

[2. Authority 3](#_Toc207016825)

[3. Scope 3](#_Toc207016826)

[4. Policy Statements 3](#_Toc207016827)

[4.1 Classification Principles 3](#_Toc207016828)

[4.2 Data Classification Levels 4](#_Toc207016829)

[5. Roles and Responsibilities 4](#_Toc207016830)

[6. Data Classification Process 5](#_Toc207016831)

[7.Handling & Control Matrix 5](#_Toc207016832)

[8. Labeling Guidelines 5](#_Toc207016833)

[9. Third-Party Data Sharing 6](#_Toc207016834)

[10. Training and Awareness 6](#_Toc207016835)

[11. Compliance and Exceptions 6](#_Toc207016836)

[12. Metrics and Review 6](#_Toc207016837)

[13. Definitions 6](#_Toc207016838)

[14. Related Documents 6](#_Toc207016839)

[15. Revision History 7](#_Toc207016840)

[Appendix A – Always Restricted Data Types 7](#_Toc207016841)

[Appendix B – Data Inventory Register (Sample Fields) 7](#_Toc207016842)

# Data Classification Policy

# 1. Purpose

This policy establishes a standardized framework for classifying organizational data based on sensitivity, value, and criticality. Its goal is to ensure that sensitive, confidential, and regulated information is consistently protected, while enabling appropriate use, sharing, and compliance with legal, contractual, and regulatory obligations.

# 2. Authority

This policy is issued under the authority of [Organization Name]’s Information Security Program and is aligned with applicable regulations (e.g., GDPR, HIPAA, PCI DSS, state/federal laws).

# 3. Scope

This policy applies to:

* All forms of data: electronic, paper, voice recordings, images, and backups.
* All systems, applications, networks, and services owned, leased, or managed by the organization.
* All employees, contractors, consultants, interns, and third parties with authorized access.

# 4. Policy Statements

## 4.1 Classification Principles

* All information assets must be classified according to **Confidentiality, Integrity, and Availability (CIA)** requirements.
* The **highest rating** across CIA dimensions determines the overall classification level.
* Classification must be applied at creation and reviewed periodically.
* Information retains its classification throughout its lifecycle, including storage, transmission, sharing, and disposal.

## 4.2 Data Classification Levels

**a. Public**

* Definition: Information approved for public release with no adverse impact if disclosed.
* Examples: Press releases, published reports, website content.
* Controls: No restrictions, but accuracy and integrity must be maintained.

**b. Internal (Sensitive)**

* Definition: Information intended for internal use; unauthorized disclosure could cause limited harm.
* Examples: Internal memos, operational procedures, non-sensitive project data.
* Controls: Access restricted to employees/authorized users.

**c. Confidential**

* Definition: Information requiring strong safeguards; unauthorized disclosure could cause significant financial, legal, or reputational harm.
* Examples: Customer contracts, HR records, intellectual property.
* Controls: Encryption in transit and at rest, strict access control, and monitoring.

**d. Restricted / Regulated**

* Definition: Highly sensitive data regulated by law or contractual agreement; disclosure could cause severe harm.
* Examples: PII/PHI, PCI data, authentication secrets, legal case files.
* Controls: Strong encryption, MFA access, logging, DLP, contractual protections.

# 5. Roles and Responsibilities

* **Executive Management**: Approves policy, provides resources, and enforces compliance.
* **Data Owners**: Assign classifications, ensure controls, and review classification annually.
* **Data Custodians (IT/Operations)**: Implement technical and physical safeguards.
* **Users**: Follow classification and handling rules; report violations.
* **CISO/ISO**: Oversees classification program, conducts audits, approves exceptions.

# 6. Data Classification Process

1. **Identify** information assets (via inventory or system documentation).
2. **Assess CIA Impact**: Determine Low/Moderate/High per asset.
3. **Assign Classification**: Map CIA score to classification level.
4. **Label and Record**: Apply labels (e.g., headers, metadata, stamps). Maintain a central register.
5. **Apply Controls**: Implement baseline and enhanced controls based on classification.
6. **Review and Update**: At least annually or upon significant business/technical changes.

# 7. Handling & Control Matrix

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Classification** | **Access Control** | **Storage** | **Transmission** | **Sharing** | **Retention & Disposal** |
| Public | Open | Standard systems | No restrictions | Freely shareable | Archive or dispose of per schedule |
| Internal | Authenticated staff only | Secure drives, business apps | Internal email, intranet | Internal sharing only | Dispose securely (shred, wipe) |
| Confidential | Role-based access, MFA | Encrypted storage, secured apps | Encrypted email, VPN | NDA required for third parties | Shred paper, secure wipe digital |
| Restricted/Regulated | Need-to-know, strict logging | Strong encryption, HSM/KMS | End-to-end encryption, secure file transfer | Only with legal/contractual safeguards | Approved secure destruction only |

# 8. Labeling Guidelines

* **Electronic documents**: Metadata tags, document headers/footers.
* **Paper documents**: Stamps, cover sheets, watermarking.
* **Emails**: Classification label in subject line or banner.
* **Systems**: Automated classification tools where feasible.

# 9. Third-Party Data Sharing

* Data shared externally must have a risk assessment.
* Contracts must specify handling, access, and disposal requirements.
* Data Protection Agreements (DPA) required for Restricted/Regulated data.

# 10. Training and Awareness

* Employees must receive training on classification and handling at hire and annually.
* Awareness campaigns must reinforce labeling, secure sharing, and incident reporting.

# 11. Compliance and Exceptions

* Compliance is mandatory.
* Exceptions require written approval from the CISO/ISO.
* Violations may result in disciplinary action, termination, or legal penalties.

# 12. Metrics and Review

* Coverage: % of assets classified.
* Audit: Number of compliance violations per quarter.
* Review cycle: Annual or upon regulatory/operational changes.

# 13. Definitions

* **Data Owner**: Person accountable for the data’s classification and use.
* **Data Custodian**: Person responsible for implementing controls.
* **CIA Triad**: Confidentiality, Integrity, Availability.
* **DLP**: Data Loss Prevention.

# 14. Related Documents

* Information Security Policy
* Access Control Policy
* Secure Disposal Standard
* Incident Response Plan

# 15. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Approved By** |
| 1.0 | [Insert Date] | Initial Release | [Approver] |

## Appendix A – Always Restricted Data Types

* Authentication data (passwords, private keys).
* Payment Card Information (PCI).
* Personally Identifiable Information (PII).
* Protected Health Information (PHI).
* Legal privileged communications.

## Appendix B – Data Inventory Register (Sample Fields)

* Asset Name
* Owner / Custodian
* Classification (Public, Internal, Confidential, Restricted)
* CIA Impact (Low/Moderate/High)
* Location / System
* Retention Requirement
* Disposal Method