

Data Classification Policy Template

This data classification policy template should be customized according to your company's information assets and specific requirements.

Purpose

This policy aims to create a framework for classifying data according to its sensitivity, value, and importance to the organization, ensuring that sensitive corporate and customer information is adequately protected.

Scope

This policy covers all classes of data, including physical documents and digital data on any storage medium. It applies to all employees and authorized third-party agents associated with the organization.

Data classification guidelines:

Information asset type	Definition
Confidential	Data with high sensitivity and criticality require the highest level of protection.
Public	Data with low sensitivity and criticality can be shared openly.
Internal	Data with moderate sensitivity and criticality accessible to authorized personnel within the organization.
Restricted/Private	Data with the highest sensitivity and not accessible without authorization.
Private	Data is limited to only few individuals in the organization.

Impact level determination:

Security Objective	Description of impact	Impact Level
Confidentiality	Unauthorized access or disclosure causing financial/legal liability	High
Integrity	Unauthorized access or alteration causing incorrect decision-making	Medium
Availability	Disruption of access/Data unavailability causing operational disruption	Low

- Data owners assess each data piece for sensitivity.
- If it matches predefined restricted types, assign "High" impact.
- If not, determine the impact using the provided guidelines and NIST 800-600 Volume 2.
- If unsure, collaborate with data custodians to resolve the issue.
- Based on the overall impact level, assign a classification label:
 - High: Restricted
 - Moderate: Confidential
 - Low: Public
- Record the classification label and impact level for each data piece in the official data classification table.



Roles & Responsibilities

- **<Role>**: Responsible for overseeing the data classification process and ensuring compliance with this policy.
- **<Role>**: Responsible for classifying data according to its sensitivity and assigning appropriate security measures and making category decisions.
- **<Role>**: Responsible for implementing security controls based on the classification of data and auditing data access.

Appendix A: Types of Information Classified as “Restricted”

- **Authentication Information:** Passwords, cryptographic keys.
- **Payment Card Information (PCI):** Credit card number with cardholder name, expiration date, etc.
- **Personally Identifiable Information (PII):** Name combined with driver’s license number, financial account number, etc.

Exceptions must be documented and approved by <Role> and the organization, detailing the nature, rationale, risks, and evidence of approval.

This policy will be reviewed annually by <Role>.

Next review date: <DATE>

 **Exceptions**

 **Review**



To make things easier, you can use **Sprinto's unified policy library** with pre-built templates. You can share the policies organization-wide and ensure all employees have acknowledged them in the platform.

With **Sprinto**, you can map policies according to your chosen compliance frameworks. The periodic policy endorsement can be easily shared with auditors during automated evidence collection.

Sprinto is a compliance automation platform that helps organizations much like yours get compliance-ready in as short a time as possible.

[Get Demo](#) →

✉ sales@sprinto.com

🌐 www.sprinto.com

