Title: Data Classification Policy (Draft for review)	
Department: IT	**Version:** Original
Approved by:	**Approval date:**
Senior management approval:	
Effective date:	**Last updated:**
Author:	

Scope

This policy applies to the offices of <company name> at <enter address>.

The scope of this policy is all data generated by or in use by the company that is deemed necessary for the conduct of the company's business.

Objectives

The objective of this policy is to protect the confidentiality, integrity and availability of <company name> data through a data classification process. This process is part of the company's overall data management program.

Responsibility

The IT department of <company name> is responsible for managing, upgrading and maintaining a data classification process that applies to the company's computing and business environments, including but not limited to all data, databases, files and information the company generates, uses, stores and disposes.

Custody of data is managed by the IT department in coordination with business unit leaders who are responsible for their unit's data.

The IT department is responsible for maintaining and updating this policy with the approval of the CIO, COO and CEO.

The IT department is responsible for identifying the standards and regulations applicable to this policy and ensuring that the company and its activities comply fully with the requirements specified in such statutes.

Identifying data to be classified

The IT department is responsible for coordinating with all relevant business units in the company to inventory the data each business unit needs to conduct its business. It will perform this inventory using tools and technologies specifically designed for this task.

Data classification categories

The IT department will define the following categories, as a minimum, for classifying data:

- Publicly available data -- Data with no restrictions on who can view it.
- Internal data with limited access -- General business information not meant for public use.
- Confidential data -- Business data whose release could cause harm to the business, e.g., litigation.
- Restricted data -- Highly sensitive data whose release could cause severe and irreparable harm to the company and its reputation if released.

Regulatory requirements

This data classification policy will comply with relevant provisions of the following statutes:

- GDPR.

- CCPA.
- HIPAA.
- FIPS.

The IT department is responsible for establishing a process for ensuring and documenting that the company complies with the relevant parts of the above statutes.

Policy for data handling

The IT department will establish guidelines for the classification of data. It will also establish guidelines for the use, storage, transmission, retention and disposal of data.

It will also define how data is to be protected, including but not limited to encryption, access controls, authentication and other security techniques. These activities will be coordinated with the company's cybersecurity department to ensure that cybersecurity policy requirements are addressed.

The following are required data classification processes:

- The IT department will define data classification processes and procedures; use specialized software and systems, whether on-site or outsourced, as needed; and document all data classification procedures and controls.
- The IT department will use specialized software and systems, whether on-site or outsourced, to reduce the threat of security breaches that could damage data.
- The IT department will periodically conduct a risk assessment of internal and external threats and vulnerabilities of the IT environment as applicable to data classification.
- The IT department will provide education, training and awareness programs to all employees.
- The IT department will define the consequences of violations of this data classification policy.
- Data in use at <company name>, whether at rest or in motion, must be encrypted.
- <Company name> employees must sign an employee contract agreeing to accept and comply with IT policies, including data classification, at the time they are hired and on a regular basis, e.g., annually, through the employee handbook and/or in contract renewals to account for policy changes over time.
- All proposed changes to data classification activities are to be documented in detail and will use the company's change management process.

Additional policies

Additional policies that are part of the company's overall data management policy might include, at management's discretion, the following:

Acceptable use. Describes the organizational permissions for the usage of IT and information-related resources.
End-user computing. Describes the parameters and usage of desktop, mobile computing and other tools.
Access Control. Describes the method for defining and granting access to various IT resources.

Applicability of other policies

This document is part of the company's suite of technology policies. Other policies might apply to the topics covered in this document, and as such, the applicable policies should be reviewed as needed.

Enforcement

This policy will be enforced by the HR department in coordination with the IT department, which is responsible for identifying and documenting noncompliant activities by employees and non-employees.

Management review IT management will review and update IT policies on a quarterly basis at <company name>. As changes to IT policies are indicated in the course of business, IT management might launch a change management initiative to modify or delete the policy(ies). All <company name> IT policies will be available for review in the course of scheduled IT audits.