[Company Name] Data Classification & Handling Policy

**Document Version:** 1.0 **Date:** March 11, 2025

## 1. Overview

This Data Classification and Handling Policy establishes a framework for classifying and protecting [Company Name]’s information assets based on their sensitivity and criticality. It defines how data should be handled, stored, transmitted, and disposed of to ensure its confidentiality, integrity, and availability. This policy applies to all employees, contractors, and vendors who handle company data.

## 2. Purpose

The purpose of this policy is to:

* Ensure that data is protected appropriately based on its sensitivity.
* Minimize the risk of data breaches and unauthorized disclosure.
* Comply with relevant data protection regulations and legal requirements.
* Establish clear guidelines for handling different types of data.
* Promote a consistent approach to data security across the organization.

## 3. Scope

This policy applies to all data created, received, stored, processed, or transmitted by [Company Name], regardless of its format or location. This includes:

* **Electronic Data:** Data stored on computers, servers, networks, mobile devices, cloud services, and removable media.
* **Paper Documents:** Printed documents, handwritten notes, and any other physical records.
* **Data Types:** Customer information, financial records, employee data, project plans, intellectual property, and any other information that has value to the company.

## 4. Policy

### 4.1. Data Classification Levels

[Company Name] will classify data into the following levels:

* **Public:** Information that can be freely disclosed to the public without any adverse impact on the company. Examples: Marketing materials, publicly available website content.
* **Internal Use Only:** Information that is intended for internal use within the company and is not meant for public disclosure. Unauthorized disclosure could cause minor inconvenience or embarrassment. Examples: Internal memos, company directories.
* **Confidential:** Sensitive business information that, if disclosed without authorization, could cause significant harm to the company, its customers, or its employees. Examples: Project bids, client contracts, financial reports, employee performance reviews.
* **Restricted:** Highly sensitive information that requires the highest level of protection. Unauthorized disclosure could have severe consequences, including legal penalties, financial losses, and reputational damage. Examples: Customer Social Security numbers, credit card information, trade secrets.

### 4.2. Data Handling Requirements

The following table outlines the minimum handling requirements for each data classification level:

| Data Classification | Storage | Transmission | Disposal | Access |
| --- | --- | --- | --- | --- |
| **Public** | No special requirements. | No special requirements. | No special requirements. | No special requirements. |
| **Internal Use Only** | Store securely to prevent unauthorized access. | Use reasonable precautions to prevent interception. | Dispose of securely (e.g., shredding). | Limit access to authorized personnel. |
| **Confidential** | Encrypt at rest and in transit. Store in secure locations. | Encrypt in transit. Use secure communication channels. | Securely shred or destroy. | Limit access to authorized personnel on a need-to-know basis. |
| **Restricted** | Encrypt at rest and in transit. Store in highly secure locations with access controls. | Encrypt in transit. Use highly secure communication channels. | Securely shred or destroy, with documented chain of custody. | Strictly limit access to authorized personnel on a need-to-know basis, with documented authorization. |

### 4.3. Data Owner Responsibilities

* Each data set or system will have a designated Data Owner. [This might be the department head or project manager responsible for that data.]
* The Data Owner is responsible for:
  + Classifying the data according to this policy.
  + Ensuring that the data is handled appropriately.
  + Reviewing and updating the data classification as needed.
  + Granting access to the data based on the principle of least privilege.

### 4.4. Data User Responsibilities

* All data users are responsible for:
  + Understanding and complying with this policy.
  + Handling data according to its classification level.
  + Protecting data from unauthorized access, use, disclosure, modification, or destruction.
  + Reporting any suspected data security incidents or vulnerabilities.

### 4.5. Data Retention

* [Company Name] will retain data only for as long as necessary to fulfill its business purpose and comply with legal and regulatory requirements.
* A separate Data Retention Policy may be developed to provide more specific guidance.

### 4.6. Data Disposal

* Data must be disposed of securely when it is no longer needed, in accordance with the handling requirements for its classification level.
* Electronic data must be securely erased or destroyed using methods that prevent recovery (e.g., overwriting, degaussing, physical destruction).
* Paper documents must be shredded or destroyed using a secure method.

## 5. Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract, and potential legal action.

## 6. Revision History

| Version | Date | Author | Description of Change |
| --- | --- | --- | --- |
| 1.0 | March 11, 2025 | Shijie Yin | Initial Policy Creation |