# Information Classification and Handling Procedure

## 1. Introduction

This document outlines the Information Classification and Handling Procedure for [Organization Name], aligned with ISO 27001 standards. It defines the processes and responsibilities for classifying and managing information to ensure its confidentiality, integrity, and availability.

## 2. Purpose

The purpose of this procedure is to establish a standardized approach to classifying and handling organizational information based on its sensitivity and criticality. This ensures that appropriate controls are applied to protect information assets and comply with legal, regulatory, and contractual requirements.

## 3. Scope

This procedure applies to all employees, contractors, and third parties who handle or process [Organization Name]'s information. It covers all forms of information, including electronic, paper-based, and verbal communication.

## 4. Policy Statement

1. Information assets must be classified into predefined categories based on sensitivity and criticality. For example:

- Public: Non-sensitive information intended for public dissemination, such as marketing materials or press releases.

- Internal Use Only: Information intended for internal operations, such as internal memos or procedural documents.

- Confidential: Sensitive information requiring controlled access, such as customer data or financial records.

- Restricted: Highly sensitive information that, if disclosed, could cause severe harm to the organization, such as trade secrets or regulatory filings.

2. Classification must be assigned by the information owner or custodian.

3. Information handling procedures, including storage, access, transmission, and disposal, must align with its classification level.

4. Unauthorized access, disclosure, or modification of classified information is prohibited and subject to disciplinary actions.

## 5. Roles and Responsibilities

- Information Owners: Responsible for determining and reviewing the classification of information assets.

- Employees and Contractors: Required to adhere to the classification and handling procedures.

- Information Security Team: Provides guidance on classification standards and monitors compliance.

- Compliance Officer: Ensures alignment with regulatory requirements.

## 6. Compliance and Monitoring

Adherence to this procedure will be monitored through regular audits, security assessments, and incident reviews. Non-compliance will result in corrective actions, which may include training, disciplinary measures, or system access restrictions.

## 7. Related Documentation

- [Information Security Policy]

- [Data Protection Policy]

- [Incident Management Procedure]

- [Access Control Policy]

## 8. Review and Revision

This procedure will be reviewed annually or following any significant changes to the organization’s structure, regulatory requirements, or business processes. The Information Security Team is responsible for initiating the review process and implementing necessary updates.

## Appendix A: Information Classification Levels

- Public: Information that is intended for public dissemination and has no restrictions.

- Internal Use Only: Information that is restricted to employees and authorized personnel within the organization.

- Confidential: Sensitive information that requires a higher level of protection and limited access.

- Restricted: Highly sensitive information with the strictest access controls and handling procedures.

## Appendix B: Handling Guidelines by Classification Level

| Classification Level | Storage Requirements | Access Control | Transmission Methods |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| Public | No restrictions | No restrictions | No restrictions |
| Internal Use Only | Secure drives or folders | Authorized personnel only | Encrypted email or secure transfer |
| Confidential | Encrypted storage | Limited to need-to-know | Encrypted email or secure transfer |
| Restricted | Encrypted storage with MFA | Strictly limited access | Encrypted transfer only |