## **ISO 27001 Information Classification and Handling Policy Template**

### **1. Introduction**

This document outlines the Information Classification and Handling Policy for [Organization Name], ensuring compliance with ISO/IEC 27001:2022 requirements. The policy provides a framework for classifying and protecting information based on its sensitivity and criticality to the organization.

### **2. Purpose**

The purpose of this policy is to:

1. Define a standardized approach to classifying and handling information.
2. Protect sensitive and confidential information from unauthorized access or disclosure.
3. Ensure compliance with ISO 27001 and applicable regulatory requirements.
4. Support the organization’s risk management objectives.

### **3. Scope**

This policy applies to all employees, contractors, and third-party vendors who handle [Organization Name]’s information assets. It encompasses:

* Physical and digital information.
* Information stored, processed, or transmitted through organizational systems.

### **4. Policy Statement**

[Organization Name] commits to implementing information classification and handling practices to safeguard its information assets. Key elements include:

1. Assigning classification levels to all information assets.
2. Ensuring information is handled according to its classification level.
3. Applying technical and procedural controls to protect sensitive information.

### **5. Classification Levels**

1. **Public:** Information that can be shared without restriction.
2. **Internal:** Information intended for internal use only.
3. **Confidential:** Information requiring access controls to prevent unauthorized disclosure.
4. **Highly Confidential:** Critical information requiring strict access restrictions and encryption.

### **6. Handling Guidelines**

1. **Storage:**
   * Store confidential and highly confidential information in secure locations.
   * Encrypt digital information at rest.
2. **Transmission:**
   * Encrypt sensitive information during transmission.
   * Avoid using personal devices for transmitting sensitive information.
3. **Access:**
   * Restrict access based on the need-to-know principle.
   * Use multi-factor authentication for accessing sensitive systems.
4. **Disposal:**
   * Shred physical records before disposal.
   * Use secure deletion tools for digital records.

### **7. Roles and Responsibilities**

1. **Information Owners:** Assign classification levels and define handling requirements.
2. **Employees and Contractors:** Handle information in accordance with its classification.
3. **IT Department:** Implement and manage technical controls for information protection.
4. **Information Security Officer (ISO):** Oversee compliance with classification and handling standards.

### **8. Compliance and Monitoring**

1. Conduct regular audits to ensure adherence to classification and handling policies.
2. Monitor for unauthorized access or misuse of sensitive information.
3. Address non-compliance through corrective actions or disciplinary measures.

### **9. Related Documentation**

1. Acceptable Use Policy
2. Data Protection Policy
3. Risk Management Policy

### **10. Review and Revision**

This policy will be reviewed annually or whenever significant changes occur in the organization’s information assets or regulatory requirements. Updates will be coordinated by the Information Security Officer.

### 

### **Appendix A: Classification Matrix**

| **Classification Level** | **Examples of Information** | **Handling Requirements** | **Access Controls** |
| --- | --- | --- | --- |
| Public | Marketing materials | No restrictions | Open access |
| Internal | Internal reports | Mark as "Internal Only" | Limited to employees |
| Confidential | Customer data | Encrypt during transmission | Limited to specific roles |
| Highly Confidential | Trade secrets | Strong encryption | Strict need-to-know basis |

### **Appendix B: Information Handling Incident Report**

| Incident ID | Date/Time | Affected Data Type | Description of Incident | Actions Taken | Resolution Status |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

### **Appendix C: Policy Acknowledgment Form**

I acknowledge that I have read and understood the Information Classification and Handling Policy and agree to comply with its requirements.

**Name:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_