**Security Policy:**

**Information Classification Policy**

This policy / procedure complies with the requirements of the ISO 27001:2013 International Standard

Annex A 5.12

[**Company Name]**

[Address]

[City, State Zip]

**1. Purpose**

This Information Classification Policy (ICP) establishes a system for classifying [Company Name]'s information assets based on their sensitivity and criticality. The ICP is designed to protect [Company Name]'s information assets from unauthorized access, disclosure, modification, or destruction.

**2. Scope**

The ICP applies to all information assets owned or controlled by [Company Name], regardless of where they are stored or processed. Information assets include, but are not limited to:

* Hard copy records
* Electronic records
* Software
* Databases
* Intellectual property
* Customer data
* Financial data

**3. Policy (A.5.12)**

All employees and contractors are responsible for classifying and protecting information assets in accordance with this ICP.

**Classification Levels**

[Company Name] uses the following classification levels to classify its information assets:

* **Confidential**: Information that is highly sensitive and could cause significant harm to [Company Name] if it were to be disclosed to unauthorized individuals.
* **Internal**: Information that is sensitive and could cause harm to [Company Name] if it were to be disclosed to unauthorized individuals but is not as sensitive as confidential information.
* **Public**: Information that is not sensitive and can be shared with the public.

**Classification Process**

All information assets must be classified at the point of creation or acquisition. The classifier must consider the following factors when classifying an information asset:

* The sensitivity of the information.
* The criticality of the information to [Company Name].
* The legal and regulatory requirements that apply to the information.

**Marking and Handling of Classified Information**

All classified information must be marked with its classification level. The classification level must be prominently displayed on all hard copy and electronic documents containing classified information.

Classified information must be handled and stored in a secure manner. Access to classified information must be restricted to authorized individuals on a need-to-know basis.

**4. Responsibilities**

* **Information Asset Owners:** Information asset owners are responsible for classifying their information assets and ensuring that they are handled and stored in a secure manner.
* **Information Security:** The information security department is responsible for developing and implementing the information classification program, as well as providing training and support to information asset owners.
* **System Administrators:** System administrators are responsible for implementing and maintaining the technical controls that protect classified information.
* **Employees and Contractors:** All employees and contractors are responsible for following the information classification program and protecting classified information.

**Information Asset Owners:**

* Classify their information assets.
* Develop and implement security procedures for handling and storing classified information.
* Conduct regular security reviews of their information assets.

**Information Security:**

* Develop and implement the information classification program.
* Provide training and support to information asset owners on the information classification program.
* Monitor and enforce compliance with the information classification program.

**System Administrators:**

* Implement and maintain the technical controls that protect classified information, such as access control systems and data encryption.
* Monitor and respond to security incidents involving classified information.

**Employees and Contractors:**

* Follow the information classification program.
* Protect classified information from unauthorized access, disclosure, modification, or destruction.
* Report any suspected security incidents to their manager or to the information security department.

**5. ENFORCEMENT**

Violations of this ICP may result in disciplinary action, up to and including termination of employment. [Company Name] may also investigate and prosecute any suspected violations of the law.

The ICP complies with ISO Annex A control 5.12 by:

* Defining the classification levels that [Company Name] uses to classify its information assets.
* Establishing a process for classifying information assets.
* Requiring that classified information be marked and handled in a secure manner.
* Enforcing the ICP through disciplinary action.

Organizations can help to ensure compliance with ISO Annex A control 5.12 by implementing a comprehensive information classification program. This program should include the following elements:

* A written ICP that is communicated to all employees and contractors.
* Training on the ICP for all employees and contractors.
* Technical and organizational controls to protect classified information.
* A process for reviewing and updating the ICP on a regular basis.

By implementing a comprehensive information classification program, organizations can help to protect their information assets from unauthorized access, disclosure, modification, or destruction.