**Security Policy:**

**Acceptable Use Policy**

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

Annex A.8.1.3

[**Company Name]**

[Address]

[City, State Zip]

**1. Purpose**

This Acceptable Use Policy (AUP) sets forth the rules for the acceptable use of [Company Name]'s information and technology resources. All employees, contractors, and other third parties who access or use [Company Name]'s information or technology resources are subject to this AUP.

**2. Scope**

This AUP applies to all [Company Name]'s information and technology resources, including but not limited to:

* Computer systems and networks
* Mobile devices
* Software
* Data
* Cloud services
* Internet access

**3. Policy (A.8.1.3)**

It is the policy of [Company Name]'s information and technology resources are to be used for business purposes only. Any personal use of [Company Name]'s information or technology resources must be incidental and must not interfere with business operations.

Prohibited Use

The following activities are prohibited when using [Company Name]'s information and technology resources:

* Accessing or using pornographic, obscene, or offensive materials.
* Engaging in illegal activities.
* Violating the intellectual property rights of others.
* Transmitting malicious code or viruses.
* Engaging in unauthorized access to or use of [Company Name]'s information or technology resources.
* Disclosing confidential information to unauthorized individuals.
* Using [Company Name]'s information or technology resources for personal gain.

Enforcement

Violations of this AUP 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.

**4. Responsibilities**

Roles and responsibilities regarding specific access assignments are as follows.

* The Information Security department is responsible for enforcing this AUP.
* Violations of this AUP may result in disciplinary action, up to and including termination of employment.
* Reporting Violations.
* Employees who suspect that someone is violating this AUP should report it to their manager or to the Information Security department.

**5. PROCEDURES**

Implementation note: the following requirements may be met using any combination of automated and/or manual systems if compliance with the requirements can be clearly evidenced by the system(s).