**Information Security Policy**

**1. Purpose**

This Information Security Policy outlines the principles and guidelines to ensure the confidentiality, integrity, and availability of the organization's information assets. This policy applies to all employees, contractors, and third-party users.

**2. Scope**

This policy covers all information assets, including but not limited to data, software, hardware, networks, and intellectual property. It applies to all information systems and processes owned or operated by the organization.

**3. Roles and Responsibilities**

* **Executive Management**: Ensure adequate resources are allocated for information security and approve the policy.
* **Information Security Officer (ISO)**: Develop, implement, and maintain the information security program.
* **IT Department**: Implement technical controls and monitor compliance with the policy.
* **Employees and Contractors**: Follow information security policies and report any security incidents.

**4. Information Classification**

All information must be classified into one of the following categories:

* **Public**: Information that can be freely shared with the public.
* **Internal**: Information intended for internal use only.
* **Confidential**: Sensitive information that requires protection due to regulatory, contractual, or other obligations.
* **Restricted**: Highly sensitive information that requires stringent controls due to its critical nature.

**5. Access Control**

* Access to information must be granted based on the principle of least privilege.
* Authentication mechanisms, such as passwords and multi-factor authentication, must be used to verify user identities.
* Regular reviews of user access rights must be conducted to ensure appropriate access levels.

**6. Data Protection**

* Encryption must be used to protect sensitive data in transit and at rest.
* Regular backups of critical data must be performed and stored securely.
* Data retention policies must be established, ensuring data is retained only as long as necessary.

**7. Network Security**

* Firewalls, intrusion detection/prevention systems, and other network security controls must be implemented to protect against unauthorized access.
* Regular network security assessments and vulnerability scans must be conducted.
* Wireless networks must be secured using strong encryption and authentication mechanisms.

**8. Incident Response**

* An incident response plan must be established and regularly tested.
* All security incidents must be reported to the ISO immediately.
* A post-incident review must be conducted to identify root causes and implement corrective actions.

**9. Physical Security**

* Physical access to sensitive areas must be controlled and monitored.
* Security measures, such as access cards and surveillance cameras, must be implemented to protect physical assets.
* Visitors must be escorted and monitored when accessing sensitive areas.

**10. Training and Awareness**

* Regular information security training must be provided to all employees and contractors.
* Awareness programs must be conducted to educate users about current security threats and best practices.

**11. Compliance and Audit**

* Compliance with this policy must be regularly audited.
* Non-compliance with the policy may result in disciplinary action.
* Regular reviews and updates to the policy must be conducted to ensure its continued relevance.

**12. Policy Review**

This policy must be reviewed annually and updated as necessary to reflect changes in legal, regulatory, or organizational requirements.

**13. Approval**

This Information Security Policy is approved by the Executive Management and is effective as of [Date].

**Executive Management:**

**Information Security Officer:**

**Date:**