ISO 27001 LEAD IMPLEMENTER
DOWNLOADABLE TEMPLATE

Sample Information Security Policy

[Organization Name] Information Security Policy

1. Scope: This Information Security Policy applies to all information assets and related processes within [Organization Name]. It encompasses electronic and physical information, regardless of the format or location, and is applicable to all employees, contractors, and third-party entities accessing or handling organizational information.

2. Applicability: This policy is applicable to all personnel, including employees, contractors, and third-party vendors, who have access to [Organization Name]'s information assets. It extends to all information systems, networks, and processes within the organization.

3. Responsibilities: Every individual and department within [Organization Name] is responsible for ensuring the security of information. Specific responsibilities include safeguarding information assets, reporting security incidents promptly, and adhering to established security protocols and procedures.

4. Compliance: [Organization Name] is committed to compliance with all relevant legal and regulatory requirements related to information security. This includes, but is not limited to, data protection laws, industry-specific regulations, and contractual obligations with clients and partners.

5. Confidentiality, Integrity, and Availability (CIA): Confidentiality, integrity, and availability are fundamental principles of [Organization Name]'s information security. All personnel must adhere to these principles:

- **Confidentiality:** Protecting sensitive information from unauthorized access or disclosure.
- **Integrity:** Ensuring the accuracy and completeness of information and preventing unauthorized alteration.
- **Availability:** Ensuring timely and reliable access to information and information systems.

6. Acceptable Use: All users of [Organization Name]'s information systems, assets, and resources must adhere to acceptable use policies. This includes using information systems for authorized purposes only, refraining from unauthorized access, and reporting any suspicious activities promptly.

7. Risk Management: [Organization Name] employs a risk-based approach to information security. This involves:

- Identifying and assessing information security risks regularly.

- Developing and implementing risk treatment plans to mitigate or manage identified risks.
- Periodically reviewing and updating risk assessments based on changes in the organizational landscape.

Review and Revision: This Information Security Policy will be reviewed regularly to ensure its ongoing relevance and effectiveness. Any necessary revisions will be made in response to changes in the organization's operations, applicable laws, or the information security landscape.

Acknowledgment: All personnel are required to read, understand, and acknowledge their commitment to this Information Security Policy. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract.

Date of Policy Approval: [Insert Date]

Signature: [Authorized Signatory]