

Information Security Policy Template

Table of Contents

01	Purpose	01
02	Scope	01
03	Policy statement	02
04	Information security requirements	02
05	Information security objectives	03
06	Segregation of duties	03
07	Contact with special interest groups	04
08	Contact with authorities	04
09	Information security in project management	04
10	Reporting of security incidents	04
11	Maintenance of policy	04
12	Supporting policies	05
13	Document security classification	07
14	Non Compliance	07
15	Responsibility	08
16	Schedule	08
17	Version history	08

1. Purpose

In the course of providing [COMPANY_NAME]'s service to clients, [COMPANY_NAME]'s staff members and vendors have access to the client's privileged and sensitive information. Each of [COMPANY_NAME]'s clients places enormous trust in that their data is created, stored, shared, and transmitted securely.

The loss of any client data or services due to unauthorized access, intrusion, theft, natural or cyber disasters, or cyber-attacks, will diminish the client's trust as well as significantly damage [COMPANY_NAME]'s reputation as an advocate for companies to develop, implement and maintain systems to prevent the loss of intellectual property and other confidential information.

The purpose of this policy document is to define the direction, principles, and basic rules for information security management within [COMPANY_NAME]. This document describes the management's vision and commitment to effectively protect "confidentiality", maintain "integrity" and ensure "availability" of its information assets, including PII, and to respond and recover from information security incidents when they arise.

Information security is deemed to safeguard three main objectives:

- ◆ **Confidentiality** - Data and information assets must be confined to people authorized to access and not be disclosed to others.
- ◆ **Integrity** - Keeping the data intact, complete, and accurate, and IT systems operational.
- ◆ **Availability** - An objective indicating that information or a system is at the disposal of authorized users when needed.

2. Scope

This policy applies to:

- ◆ All staff members working for [COMPANY_NAME] who have access to the organization's and/or client's information.
- ◆ All staff members, vendors, and third-party employees who have access to [COMPANY_NAME]'s information processing systems and the data contained in them. This includes the data accessed by licensed third parties, which is, in turn, deployed to and used by their clients.

- ◆ All stakeholders and interested parties who are relevant to the operations of [COMPANY_NAME].
- ◆ This policy covers all digital and non-digital assets that contribute to the creation, storage, transmission, and disposal of information.

3. Policy statement

[COMPANY_NAME] shall establish, implement, and maintain a holistic and robust Information Security Management System (ISMS), putting in place adequate and appropriate arrangements which shall enable it to effectively protect "confidentiality", maintain "integrity" and ensure "availability" of its information assets including PII and to respond and recover from information security incidents when they arise.

While planning the ISMS, [COMPANY_NAME] shall consider its internal and external issues along with the requirements of the interested parties and determine risks and opportunities that could affect the activities supporting the provision of its products and services. The top management shall provide the required resources and sufficiently contribute towards the ISMS ,ensuring it achieves its intended outcome(s).

4. Information Security Requirements

Information and supporting technology - including hardware and software systems are critical business assets. Confidentiality, integrity, and availability of information are essential to maintaining a better competitive edge, profitability, legal compliance, and reputation.

Organizations and their information systems and networks increasingly face security threats from a wide range of sources, including external hacking and intrusion, computer-assisted fraud, espionage, sabotage, vandalism, or damage from natural disasters. Due to the dependence on information systems and services, organizations are now more vulnerable to security threats.

Designing security controls and implementation requires careful planning and attention. Management policies and administrative controls are needed to supplement technical controls that are implemented to protect data. Information Security Management needs, as a minimum, participation from all employees in the organization. It may also require involvement from suppliers, vendors, service providers, customers, and external specialists.

5. Information security objectives

- ◆ To create a coherent system for information security management that is aligned with [COMPANY_NAME]'s business strategy.
- ◆ To protect and safeguard information that is important to [COMPANY_NAME] and its clients, licenses, and their clients.
- ◆ To reduce risk related to the use of technology & technology outsourcing.
- ◆ To ensure that all [COMPANY_NAME]'s information assets are accounted for and adequately protected from damage, alteration, loss, and unauthorized use or access.
- ◆ To ensure that information and information systems are always available to authorized users whenever they need to access them.
- ◆ To ensure that [COMPANY_NAME] provides its customers with the means to enable them to fulfil their obligation to facilitate the exercise of the 'right to access, correct, and/or erase PII about them, defined by contract.
- ◆ This ensures that PII is processed under a contract and should not be processed for any purpose independent of the instructions of [COMPANY_NAME]'s customer.
- ◆ To comply with all information security-related regulatory and statutory requirements about information collection, storage, processing, transmission, and disclosure.
- ◆ To set aside resources to establish, implement, operate, monitor, review, and maintain information security safeguards.
- ◆ To create awareness of information security and ensure that all employees understand their responsibilities for maintaining it.
- ◆ To create detailed information security best practices and guideline documents, and ensure compliance with such documents.
- ◆ To assess and update the information security policy objectives on a timely basis as per the business need and ensure continual improvement.

6. Segregation of duties

Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization's assets. While assigning responsibilities, conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of

the organization's assets. Care shall be taken that no single person can access, modify or use assets without proper authorization or detection. The possibility of collusion should be considered while designing the controls.

7. Contact with special interest groups

Based on requirements, and proper validation of the vendor, specialist advice shall be sought whenever required. This could be by way of having a Security Consultant on a contractual or on a per-call payable basis. The same could also be sought from non-profit agencies like [SECURITY_AGENCIES like CIS, CERT, NIST].

8. Contact with authorities

Where required, appropriate contacts with law enforcement authorities, regulatory bodies, fire department, emergency services, telecommunication providers and other service providers shall be maintained by the organization. These contacts shall ensure help can be availed of and is accessible during a crisis situation.

9. Information security in project management

Information security should be integrated into the organization's project management method(s) to ensure that information security risks are identified and addressed as part of a project. This applies generally to any project regardless of its character, e.g., a project for a core business process, IT, facility management, and other supporting processes.

10. Reporting of security incidents

The person witnessing an information security incident should report the incident in accordance with [COMPANY_NAME]'s Incident Management Policy.

11. Maintenance of policy

The compliance with this policy and supporting policies shall be audited on a yearly basis; exceptions identified during the audit shall be immediately and appropriately addressed and

logged in the version history.

The security policy shall be reviewed annually unless there is a major change in the organization or the environment affecting the organization, in which case it should be reviewed after the change is implemented.

The security policy shall be reviewed and revised whenever a major security risk or an incident is identified.

12. Supporting policies

The following policy documents will support the information systems security policy at a minimum:

Code of Conduct

The purpose of this policy is to define the expected behavior of employees, contractors, and third parties in alignment with [COMPANY_NAME]'s values and security objectives. It outlines standards for ethical conduct and integrity in handling company assets and information.

Asset Management Policy

The purpose of this policy is as follows:

- ◆ To identify [COMPANY_NAME]'s assets and define appropriate protection responsibilities.
- ◆ To ensure that information receives an appropriate level of protection in accordance with its importance to [COMPANY_NAME].
- ◆ To prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

Risk Management Policy

The purpose of this policy is to ensure guidelines related to identifying, assessing, and managing Information Security Risks that may prevent <COMPANY_NAME> from achieving its business objectives.

Human Resources Security Policy

The purpose of this policy to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

Physical and Environmental Policy

The purpose of this policy is to prevent unauthorized physical access, damage, and interference to [COMPANY_NAME]'s information and information processing facilities.

Access Control Policy

The purpose of this policy is as follows:

- ◆ To limit access to information and information processing facilities.
- ◆ To ensure authorized user access and to prevent unauthorized access to systems and services.
- ◆ To make users accountable for safeguarding their authentication information.

Acceptable Usage Policy

It is to ensure that all employees at [COMPANY_NAME] are aware of acceptable use of assets and formal cybersecurity guidelines to ensure best security practice.

System and Services Acquisition and Development Policy

The purpose of this policy is as follows:

- ◆ To ensure that information security is an integral part of information systems across their entire lifecycle — including planning, development, implementation, maintenance, and decommissioning.
- ◆ To enforce security-by-design principles during system design and development.
- ◆ To ensure third-party software and services used in development are assessed for supply chain security risks.
- ◆ To maintain documentation and change control processes to support secure development and acquisition practices.

Vendor Management Policy

The purpose of this policy is to ensure the protection of [COMPANY_NAME]'s assets that are provided by third-party suppliers.

Privacy Policy

The purpose of this policy is to ensure that [COMPANY_NAME] collects, processes, stores, and shares personal data in a manner that respects individuals' privacy and complies with relevant data protection regulations.

Operations Security Policy

The purpose of this policy is to ensure the protection of information through the secure management of technical and operational processes directly supporting systems that process customer data. This includes, but is not limited to:

- ✦ IT operations such as change management, patching, system monitoring, logging, backup, and recovery activities.
- ✦ Operational procedures that ensure the secure and consistent functioning of [COMPANY_NAME]'s information systems and services relevant to customer data processing.

Incident Management Policy

This policy helps management of any information security incidents that may compromise confidentiality, integrity or availability of data and services by [COMPANY_NAME].

Business Continuity Management and Disaster Recovery Policy

The purpose of this policy is to

- ✦ Ensure that business continuity is embedded in [COMPANY_NAME]'s scope of operations.
- ✦ Establish procedures for responding to and recovering from major disruptions to IT services and infrastructure, ensuring the continuity of critical business functions at [COMPANY_NAME].

Compliance Policy

The purpose of this document is to ensure [COMPANY_NAME] is in compliance with all Information and cybersecurity legislation and regulations to ensure the proper functioning of all business domains.

13. Document security classification

[CLASSIFICATION_LEVEL]

14. Non-Compliance

[COMPANY_NAME] staff who violate this policy may face repercussions in proportion to the

impact of their violation. [COMPANY_NAME] management will determine how severe a staff member's offense is and decide the appropriate penalty. Penalties may include a Reprimand. Demotion. Suspension or termination for more serious crimes. Detraction of benefits for a definite or indefinite time.

15. Schedule

Activity	Frequency
Review of the document	On an annual basis, or earlier as deemed necessary due to required updates or changes

16. Version history

Version	Log	Log
[VERSION]	[CHANGE_DESCRIPTION]	[DATE]
[VERSION]	[CHANGE_DESCRIPTION]	[DATE]

About Sprinto

Thousands of ambitious tech companies trust Sprinto to streamline their GRC program, automate management, and maintain security best practices. Sprinto supports over 20 security standards, including SOC 2, ISO 27001, GDPR, HIPAA, and PCI-DSS, as well as custom frameworks. Featuring a smart, adaptive and scalable architecture, Sprinto ensures security best practices without getting in the way of your growth ambitions.

For more information visit sprinto.com

[View Sprinto Trust Center](#) ↗



Get in touch

 sales@sprinto.com  support@sprinto.com

© Sprinto 2025 All Rights Reserved. THIS DOCUMENT HAS BEEN PREPARED FOR GENERAL INFORMATIONAL PURPOSES ONLY. IT IS PROVIDED IN GOOD FAITH, HOWEVER, WE MAKE NO REPRESENTATION OR WARRANTY INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, COMPLETENESS, OR ACCURACY. THE INFORMATION PROVIDED IN THIS DOCUMENT IS ONLY ILLUSTRATIVE AND DOES NOT DIRECTLY OR INDIRECTLY CREATE ANY CONTRACTUAL OBLIGATIONS. THIS DOCUMENT SHALL NOT BE DISCLOSED TO ANY THIRD PARTY IN ANY FORM OR BY ANY MEANS, ORALLY OR IN WRITING, FOR ANY PURPOSE, WITHOUT OUR PRIOR WRITTEN CONSENT. WE RESERVE THE RIGHT TO CHANGE THE CONTENTS OF THIS DOCUMENT, WITHOUT NOTICE. UNDER NO CIRCUMSTANCE SHALL WE BE LIABLE FOR ANY LOSS OR DAMAGE INCURRED BY ANY PARTY IN CONNECTION WITH THE USE OR RELIANCE OF INFORMATION PROVIDED IN THIS DOCUMENT.