COMPANY policy template instructions

This COMPANY policy template represents a complete, compliance-ready policy with placeholders for company specific text. Each policy section represents a policy-specific topic that you should consider and/or modify to match your company’s practices.

For each policy section

* Consider if this section and its corresponding risks apply to you. If it does not, remove it and/or replace it with your organization’s corresponding practices.
* Replace any highlighted text in angled brackets < > with your own language
* Rewrite the policy language such that it reflects the practices of your organization

Policy completion checklist

1. Use Find to make sure that all text in angled brackets is replaced
2. Proofread your policy for spelling and grammar mistakes
3. Confirm that the policy’s content reflects your organizations practices
4. Add any company-specific letterhead, branding, and formatting
5. Remove this instructions page
6. Export this document as PDF — File > Save As > Change “File Format” to PDF
7. Upload the PDF to COMPANY at https://app.COMPANY.com/policies

More questions?

A good rule-of-thumb is to keep your language at a high enough level such that it stays representative for at least a year. If you have more questions about how to use this template, please reach out to support@COMPANY.com or your auditor for additional guidance.

Document Name: Scope of the ISMS

Document Number: 01-ISMS

| Company Name: | <Company Name> |
| --- | --- |
| Policy Owner(s): | <Policy owner(s)> |
| Effective Date: | <Effective date> |

# Purpose

<Company Name> has established an Information Security Management System (“ISMS”) in accordance with ISO/IEC 27001 (“ISO 27001”) that governs the processes required to protect company and information assets. This document specifies the scope of the ISMS at <Company Name>.

# Introduction

<Company Name> utilizes the ISO 27001 Information Security (“InfoSec”) frameworks in order to identify and maintain the assets, technologies, and processes needed to protect customer information and to help ensure the confidentiality, integrity, availability, and privacy of customer data and supporting services.

To enable this, <Company Name>:

1. Aligns its InfoSec policies and procedures to the global industry standard ISO 27001
2. Maintains a robust InfoSec framework for the efficient functioning of the organization

All locations identified including departments and assets are included in the scope of the ISMS as detailed in the following sections.

# Scope of the ISMS

<{remove after use} Please select one of the following:>

<Company Name> one or more specific processes

<Company Name> one or more specific functions

<Company Name> one or more specific services

<Company Name> one or more specific sections or locations

<Company Name> entire legal entity

<Company Name> entire administrative entity and one or more of its suppliers

## General

The following statement defines the Scope of Services for <Company Name>:

<Description of service(s) provided by your company>

The scope of <Company Name> ISMS includes the assets, technologies and processes for the secure provision of <Include services, product or activities performed by the company>. Additionally, the scope is defined with consideration of the external and internal context of the organization (Appendix A), requirements of interested parties (Appendix B), such as customers and regulatory bodies, and boundaries with third parties (Appendix C).

## Assets

The assets of the ISMS are further categorized as information, application, database, cloud services, and personnel. The details of the assets can be found in Appendix D.

## Locations

The following locations are in scope for the ISMS:

| **Office Locations** | |
| --- | --- |
| <Address> | <Address> |
| <Address> | <Address> |

## Departments

The following departments are in-scope for the ISMS:

* Information Technology (“IT”)
* Software Development (“Dev”)
* Human Resources (“HR”)
* Information Security (“InfoSec”)
* Legal
* Finance

## Personnel

All personnel belonging to the above departments are in-scope for the ISMS.

### Scope Exclusions and Boundaries

* <Company Name> <uses Amazon Web Services (“AWS”) for cloud computing and storage services. Amazon is responsible for managing logical access to the underlying network, system management, and storage devices for its cloud service hosting> <Company Name> <data.>
* <Amazon is responsible for the physical security and environmental controls at data center facilities hosting> <Company Name> <systems. Therefore, physical security and environmental controls are out of scope for those facilities>.
* <Amazon is responsible for the secure deletion of data and disposal of equipment used to support> <Company Name> <customer operations.>
* <Company Name> <information, application, database, facility, and personnel assets that are not related to the identified in-scope components are out of scope for the ISMS.>

# ISO 27001 Coverage

ISO 27001 4.1; 4.2; 4.3; 4.4; A.7.1

# Version History

| **Version** | **Date** | **Description** | **Author** | **Approved by** |
| --- | --- | --- | --- | --- |
| <1.0> | <Date of change> | <Initial policy> | <Author of changes> | <Approver of changes> |
|  |  |  |  |  |
|  |  |  |  |  |

# Appendix A - Context of the Organization

By establishing the organizational context, <Company Name> is able to articulate its objectives, define the external and internal parameters to be considered when setting scope and risk criteria and managing risks to the objectives of the ISMS.

# Internal Context

<Company Name> established the internal context by analyzing the internal components that support the ISMS as documented below:

| **Internal Factors** | **Description** |
| --- | --- |
| Governance | Decision making and power to define expectations and manage performance |
| Organizational structure | Establishment of internal hierarchy and lines of authority |
| Roles and accountabilities | Assignment of roles and responsibilities for the establishment, operation, maintenance, and continual improvement of the ISMS |
| Policies, objectives, and strategy | Processes, requirements and activities developed to achieve business objectives |
| Capabilities | Company resources and knowledge (e.g., intellectual property, capital, time, people, processes, systems and technologies) |
| Internal stakeholders | Management of perceptions, values and relationships with interested/invested parties |
| Organizational culture | Company values, mission statement, and employee perceptions |
| Information management | Information systems, information flows and decision-making processes (both formal and informal) |
| Contractual relationships | Requirements established with third parties |

# External Context

<Company Name> established the external context through consideration of the local, regional, national, and international factors below:

| **External Factors** | **Description** |
| --- | --- |
| Social | The communities and customs of the environment with which <Company Name> operates |
| Cultural | The shared beliefs and values of the environment with which <Company Name> operates |
| Political | The governmental system(s) and practices of the environment with which <Company Name> operates |
| Legal, regulatory, and compliance | Laws, regulations, and compliance standards that may impact <Company Name>’s objectives:   * <23 NYCRR 500 (NYCS)> * <Americans with Disabilities Act (ADA)> * <California Department of Insurance Code (CIC)> * <California SB 1121 Consumer Privacy Act of 2018 (CCPA)> * <California SB 1386 Security of Non-encrypted Customer Information of 2003 (State of California) and progeny> * <CAN-SPAM Act of 2003 Computer Fraud and Abuse Act (CFAA) of 1986 (FTC – Federal Trade Commission)> * <Electronic Signatures in Global and National Commerce Act (E-SIGN) (Public Law 106-229)> * <General Data Protection Regulation (GDPR)> * <Gramm-Leach-Bliley Financial Modernization Act of 1999 (GLBA)> * <Health Insurance Portability and Accountability Act (HIPAA)> * <ISO/IEC 27001 and 27701 Frameworks> * <New York State Information Security Breach and Notification Act of 2005> * <PCI Data Security Standard> * <The Californian Online Privacy Protection Act of 2004 (CalOPPA)> * <Uniform Electronic Transactions Act (UETA)> |
| Financial | Allocation, management, acquisition and investment of resources in <Company Name> |
| Technological | Changes in the mechanisms, processes, communications and systems used in the environment with which <Company Name> operates |
| Economic | The conditions of the production, distribution, and consumption of goods of the environment with which <Company Name> operates |
| Natural | The physical environment and landscape of the environment with which <Company Name> operates |
| Competitive | The impact made by other companies that perform similar services |
| Key drivers and trends | Changes in the market that have an impact on <Company Name>’s objectives |
| External stakeholders | Perceptions, values relationships with key external interested parties |
| Contractual relationships | Requirements established with third parties |
| <Data Controller and/or Processor>[[1]](#footnote-8) | <Compliance as a Data Processor> |

# Appendix B – Interested Parties and Their Requirements

<Company Name> defines the ISMS key interested parties and their requirements, as well as which of these requirements will be addressed through the information security management system:

| **Interested Party** | **Type** | **Requirements** | **Addressed by ISMS** |
| --- | --- | --- | --- |
| Customers | External | Protection of customer information (confidentiality, integrity, availability, and privacy) and compliance with contractual agreements | <”Yes, this requirement is addressed by the ISMS as per our SOA” or “No, this will not be addressed in the ISMS because … <provide explanation>”> |
| Regulators | External | Compliance with regulations and other applicable privacy laws | <”Yes, this requirement is addressed by the ISMS as per our SOA” or “No, this will not be addressed in the ISMS because … <provide explanation>”> |
| Business Partners and Stakeholders | Internal | Protection of <Company Name>’s reputation, meeting customer expectations, and continuous generation of revenue | <”Yes, this requirement is addressed by the ISMS as per our SOA” or “No, this will not be addressed in the ISMS because … <provide explanation>”> |
| Employees | Internal | Information security training and awareness that can help employees align their daily operations with <Company Name>’s information security goals and objectives | <”Yes, this requirement is addressed by the ISMS as per our SOA” or “No, this will not be addressed in the ISMS because … <provide explanation>”> |
| Auditors | Internal & External | Compliance with certification framework requirements | <”Yes, this requirement is addressed by the ISMS as per our SOA” or “No, this will not be addressed in the ISMS because … <provide explanation>”> |
| Management & Board of Directors | Internal | Protection of customer information (confidentiality, integrity, availability, and privacy) and compliance with contractual agreements and external regulations.  Integrity of financial reporting | <”Yes, this requirement is addressed by the ISMS as per our SOA” or “No, this will not be addressed in the ISMS because … <provide explanation>”> |
| <PII Principles (i.e. Data Subjects and Consumers)> [[2]](#footnote-10) | <External> | <Data subjects and consumers whose PII is collected, stored and processed expect that the confidentiality, integrity and availability of their data is maintained. In addition, they expect that data processing and sharing will be limited to the purposes and parties about which they’ve been informed and consented to.> | <”Yes, this requirement is addressed by the ISMS as per our SOA” or “No, this will not be addressed in the ISMS because … <provide explanation>”> |

# Appendix C – Interfaces and Dependencies

The interfaces and dependencies between activities performed by <Company Name> and other organizations are listed below and are considered while determining the scope of ISMS. The organizations listed below are critical to <Company Name>’s operations. However, since the company does not have direct control over these organizations, inherent risks are reduced via signed contractual agreements which comply with <Company Name> standards.

| **Other Organizations** | **Description of the Interfaces and Dependencies** |
| --- | --- |
| <Salesforce (“SFDC”)> | <Responsible for Availability of hosting platform required for managing customer relationships, sales opportunities, market access, financial accounting, reporting, business processes, and policy and benefits administration. Physical and Environmental Security, Secure Data Deletion and Device Disposal are the responsibility of Salesforce.> |
| <Google Suite (“G Suite”)> | <Availability of email, office tools, and identity and authentication platform. Physical and Environmental Security, Secure Data Deletion and Device Disposal are the responsibility of Google.> |
| <Zoom> | <Cloud-based communications> |
| <ZeroTier> | <Network management and monitoring> |
| <Sophos> | <Centralized endpoint threat detection and monitoring, and managed threat response, for malware> |
| <Customers> | <Responsible for securing their own email and account credentials> |

# Appendix D – Assets

Below is a detailed description of the all assets in-scope for the ISMS:

| **Asset Category** | **Asset Name** | **Description** | **Location(s)** |
| --- | --- | --- | --- |
| <Information assets> | <System infrastructure> | <System infrastructure / Data Centers / Cloud Infrastructure> | <SITE NAME> |
| <Information assets> | <Customer data> | Data stored by <Company Name> customers | <SITE NAME> |
| <Information assets> | <User and organization information> | User information of <Company Name> employees and customers | <SITE NAME> |
| <Information assets> | <Intellectual property> | <Source code and company intellectual property> | <SITE NAME> |
| <Information assets> | <Operational / support procedures / system documentation> | <Documents that detail the operations of the ISMS> | <SITE NAME> |
| <Information assets> | <Task management system (Clubhouse)> | <Task management system utilized to centrally track, maintain, and manage internal requests (e.g., access requests) and change management activities> | <SITE NAME> |
| <Information assets> | <Microsoft VPN> | Access to Microsoft services | <SITE NAME> |
| <Application assets> | <Application website> | Website used for customers to access <Company Name>’s service | <SITE NAME> |
| <Database assets> | <Epic Database> | <E.g., Contains PII> | <SITE NAME> |
| <Database assets> | <SQL Databases> | <E.g., Contains public information> |  |
| <Cloud service assets> | <AWS> | <Cloud infrastructure> |  |
| <Personnel assets> | <InfoSec and IT> | <Personnel that are responsible for system and network infrastructure. Personnel that are responsible for cloud infrastructure. Personnel that are responsible for overseeing the security of laptops, interface with and respond to internal staff and interested third parties regarding security questions, and manage compliance.> | <SITE NAME> |
| <Personnel assets> | <Development> | <Personnel that are responsible for application development, bug fixes, and code management. Personnel that are responsible for overseeing the certification of code changes. Personnel that are responsible for implementing code and infrastructure changes and manage parts of the production application stack.> | <SITE NAME> |
| <Personnel assets> | <Human Resources> | <Personnel that are responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisition, employee retention, compensation, employee benefits, performance management, employee relations, and training and development.> | <SITE NAME> |
| <Personnel assets> | <Legal> |  | <SITE NAME> |
| <Personnel assets> | <Finance> |  | <SITE NAME> |

# Appendix E – External and Internal Issues

4.1 requires an organization to determine external and internal issues relevant to its purpose and affecting its ability to achieve the intended outcome(s) of the information security management system (ISMS). As part of the Management Review process <Company Name> continually analyzes itself and the world surrounding it in order to identify issues that in some way affect information security and how information security can be managed, insofar as they are relevant to the organization’s objectives.

Analysis of external and internal issues serves three primary purposes:

— understanding the context in order to decide the scope of the ISMS;

— analyzing the context in order to determine risks and opportunities; and

— ensuring that the ISMS is adapted to changing external and internal issues.

The following table represents the external and internal issues that have been identified as relevant to <Company Name>’s security and objectives:

| **External Issues** *(defined as those outside of the organization’s control* | |
| --- | --- |
| **Issue** | **Description <SAMPLES PROVIDED - UPDATE>** |
| **Social and cultural** | <Reduced demand for the organization’s services> |
| **Political, legal, normative and regulatory** | <Insufficient analysis of legal implications of using an outsourced IT service>  <Changes to regulatory landscape> |
| **Financial and macroeconomic** | <Inflation, commodification> |
| **Technological** | <Inability to keep pace with hacking tools>  <Insufficient use of cryptography> |
| **Natural** | <Risk of disasters such as fire, flood and earthquakes> |
| **Competitive** | <Direct market competition, market oversaturation of similar product/services> |
| **Internal Issues** *(defined as those subject to the organization’s control)* | |
| **Organizational culture** | <No clear direction or mandates set to drive organization excellence or culture> |
| **Policies, objectives, and the strategies to achieve them** | <Lack of strategic direction related to organizational goals> |
| **Governance, organizational structure, roles and responsibilities** | <Lack of leadership and oversight for key areas> |
| **Standards, guidelines and models adopted by the organization** | <Lack of internal alignment with legal and regulatory standards and associated processes> |
| **Contractual relationships that can directly affect the organization’s processes included in the scope of the ISMS** | <Changes to contractual agreements impacting organizational goals> |
| **Processes and procedures** | <Insufficient or nonexistent policies, processes, procedures> |
| **Resources, knowledge, and technologies** | <Lack of capital, time, persons, processes, systems to support operations> |
| **Physical infrastructure and environment** | <Insufficient IT infrastructure to support operations> |
| **Information systems, information flows and decision making processes (both formal and informal)** | <Lack of IT direction and governance> |
| **Previous audits and previous risk assessment results.** | <Lack of remediation and oversight of findings arising from internal and external audits and assessments> |

# 27701 Privacy Information Management System (PIMS) Addendum

This addendum is automatically applicable for organizations implementing ISO 27701 and optional for organizations who are implementing ISO 27001 only.

* All references to “ISMS” in this document are changed to “IS&PMS”
* All references is ISO 27001 in this document are changed to “ISO 27001/27701”
* All references to “information security management system” are changed to “information security and privacy management system”

1. Define role as Data Controller, Processor, or Both [↑](#footnote-ref-8)
2. PII principles are defined as an interested party [↑](#footnote-ref-10)