COMPANY document template instructions

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

For each document section

* Consider if this section applies 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 document language such that it reflects the practices of your organization

Document completion checklist

1. Use Find to make sure that all text in angled brackets is replaced
2. Proofread your document for spelling and grammar mistakes
3. Confirm that the document’s content reflects your organization’s 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 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 your Customer Success Manager or your auditor for additional guidance.

Document Name: Relevant Laws, Regulations, and Contractual Requirements

Document Number: 12-ISMS

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

# Purpose

The purpose of this workbook is to identify, update, and maintain a current list of all relevant laws, regulations, and contractual requirements and <Company Name>'s approach to meeting these requirements.

# Relevant Laws, Regulations, and Contractual Requirements

| **Relevant Laws, Regulations, and Contractual Requirements** | **<Company Name> as Data Controller** | **Approach to Meeting Requirements** | **<Company Name> as Data Processor** | **Approach to Meeting Requirements** |
| --- | --- | --- | --- | --- |
| California SB 1386 Security of Non-encrypted Customer Information of 2003 (State of California) and progeny | Yes | See <Company Name>'s *Information Security Policy*. | No. All customer data is encrypted. | Not Applicable |
| The Californian Online Privacy Protection Act of 2004 | Yes | <Company Name> has a Privacy Notice on our website. We support DNT, our privacy notice covers all notice requirements under CalOPPA. <Company Name> ensures transparency and accountability in its use of PII. | Yes | <Company Name> has a Privacy Notice on our website. We support DNT, our privacy notice covers all notice requirements under CalOPPA. |
| California Consumer Privacy Act (CCPA) | Yes | To the extent that <Company Name> has PII belonging to CA residents, we will protect such PII in accordance with our Information Security Policies. | No | To the extent that <Company Name> has PII belonging to CA residents, we will protect such PII in accordance with our Information Security Policies. |
| Computer Fraud and Abuse Act (CFAA) of 1986 (FTC – Federal Trade Commission) | Yes | See <Company Name>'s Acceptable Use Policy. | Yes | Customers are contractually prohibited from using the services in violation of any law, see also <Company Name>'s Acceptable Use Policy attached to all contracts. |
| New York Data Security Law (Name: New York State Information Security Breach and Notification Act) | Yes | To the extent that <Company Name> has PII belonging to NY residents, we will protect such PII in accordance with our Information Security Policies and will notify the state AG in the event of a breach of such data. | No |  |
| 23 NYCRR 500 (NYCS) | Yes | To the extent that <Company Name> has PII belonging to NY residents, we will protect such PII in accordance with our Information Security Policies and will notify the state AG in the event of a breach of such data. | No |  |
| General Data Protection Regulation (GDPR) | Yes | In its role as a data controller, <Company Name> complies with the requirements of the GDPR. <Company Name> has appointed a DPO and our policies and procedures reflect our compliance efforts. | Yes | In its role as a data processor, <Company Name> complies with the requirements of the GDPR. <Company Name> has appointed a DPO and our policies and procedures reflect our compliance efforts. |
| GLBA | No | No personally identifiable financial information relating to individuals in scope | No |  |
| PCI DSS | No | <Company Name> has outsourced all PCI functions to PCI compliant 3rd parties. <Company Name> does not store, process, or transmit credit card data. | No |  |
| HIPAA | No |  | Yes |  |
| Customer contractual requirements | No. Customers are data controllers. | Not Applicable | Yes | <Company Name> has implemented administrative, technical, physical, and organizational controls to protect customer data. |

# Compliance Validation Process

At least annually, compliance with relevant information security and data privacy frameworks, laws, regulations, and contractual commitments shall be validated. Validation processes may include:

* Verifying that tests are passing in COMPANY
* Compliance, configuration, and vulnerability scanning
* Internal audits
* External audits
* Spot checks
* Control owner validation processes

# ISO 27001 Coverage

ISO 27001 A.5.31; A.5.32; A.5.34

# Version History

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

# 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”