# Compliance Policy

To use this template, simply replace the text in dark grey with information customized to your organization. When complete, delete all introductory or example text and convert all remaining text to black prior to distribution.

# Purpose

Describe the factors or circumstances that mandate the existence of the policy. Also state the policy’s basic objectives and what the policy is meant to achieve.

The purpose of this policy is to ensure proper measures are in place to avoid non-adherence to information security compliance requirements – legal, contractual, regulatory, or otherwise.

# Scope

Define to whom and to what systems this policy applies. List the employees required to comply, or simply indicate “all” if all must comply. Also indicate any exclusions or exceptions, i.e. those people, elements, or situations that are not covered by this policy or where special consideration may be made.

This Compliance Policy applies to all business processes and data, information systems and components, personnel, and physical areas of [insert Company’s name].

# Definitions

Define any key terms, acronyms, or concepts that will be used in the policy. A standard glossary approach is sufficient.

# Governing Laws & Regulations & Standards

If applicable, list any laws or regulations that govern the policy or with which the policy must comply. Confirm with the legal department that the list is full and accurate. If there are no pertinent governing laws or regulations, delete this section.

|  |  |
| --- | --- |
| **Guidance** | **Section** |
| ISO27001:2013 | A.18 (A.18.1, A.18.2) |
| NIST SP 800-53 v4 | XX-1 controls, CM-10, AC-3, AU-9, AU-11, CP-9, MP-4, SA-5, SI-12, Appendix J Privacy Controls, SI-12, AC-8, AU-6, CM-11, PL-4, PS-6, PS-8, IA-7, SC-13, CA-2, CA-7, RA-5, AU-1, AU-2, SI-4 |

# Policy Statements

Describe the rules that comprise the policy. This typically takes the form of a series of short prescriptive and proscriptive statements. Sub-dividing this section into sub-sections may be required depending on the length or complexity of the policy.

**Compliance with legal and contractual requirements:**

* + All applicable compliance requirements should be identified, documented, and well-maintained.
  + Any intellectual property rights requirements should be implemented and adhered to as necessary.
  + Records will be properly managed to avoid any destruction from natural disasters, unauthorized use, or loss.
  + Personally identifiable information will be properly protected.
  + Any cryptographic controls will be used appropriately according to relevant compliance requirements.

**Compliance with security policies and standards:**

* + At least annually, [insert Company’s name] should perform reviews or audits of users’ and systems’ compliance with security policies, standards, and procedures, and initiate corrective actions where necessary.
  + Results from compliance reviews or audits shall be documented and reported by [insert Company’s name] leadership.

**Information system audit considerations:**

* + [Insert Company’s name] should implement audit procedures to help ensure that activities involving reviews or audits of operational systems are carefully planned to minimize the risk of disruptions to business processes.
  + [Agency] shall implement security controls to help prevent unauthorized access and/or access abuse of audit tools.
  + [Insert Company’s name] information systems should be enabled to generate audit records containing details to help establish what type of event occurred, when and where the event occurred, the source and outcome of the event, and the identity of any individuals or subjects associated with the event.
  + [Insert Company’s name] should report findings of audit records reviews to information security personnel and [Agency] leadership.

**Information security reviews and continuous improvements:**

* [Insert Company’s name] will conduct an independent review of its information security practices, controls, policies, etc.
* Management team is responsible for regular reviews of their compliance with information security policies and procedures.
* A technical review of information systems will be conducted regularly.
* [Insert Company’s name] should develop a plan of action and milestones to document planned remedial actions to correct weaknesses or deficiencies identified as a result of internal/external risk assessments, security reviews, and/or audits.

**Relevant Procedures**

Consider creating formal procedure documents that reinforce and support the policy statements above. Note, it is best practice to house policies and procedures in separate documents to keep the content focused and reduce the number of times the policy must be reapproved by senior management.

# Non-Compliance

Clearly describe consequences (legal and/or disciplinary) for employee non-compliance with the policy. It may be pertinent to describe the escalation process for repeated non-compliance.

Violations of this policy will be treated like other allegations of wrongdoing at [Company Name]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [Company Name] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

.