**Cybersecurity Templates**

**Regulatory Compliance Management Policy**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Regulatory Compliance Management Policy** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Policy No:** | [Assign Number] | **Effective Date:** | [Insert Date] |
| **Owner:** | [CISO / Compliance Manager] | **Review Cycle:** | [Annual / Biennial] |

Contents

[1. Purpose 3](#_Toc207031435)

[2. Scope 3](#_Toc207031436)

[3. Objectives 3](#_Toc207031437)

[4. Regulatory Compliance Framework 3](#_Toc207031438)

[5. Roles and Responsibilities 4](#_Toc207031439)

[6. Compliance Processes 4](#_Toc207031440)

[6.1 Regulatory Obligations Register 4](#_Toc207031441)

[6.2 Statement of Applicability (SoA) 5](#_Toc207031442)

[6.3 Compliance Calendar 5](#_Toc207031443)

[6.4 Monitoring & Auditing 5](#_Toc207031444)

[6.5 Reporting 5](#_Toc207031445)

[7. Third-Party & Cloud Compliance 5](#_Toc207031446)

[8. Training and Awareness 5](#_Toc207031447)

[9. Exception Management 5](#_Toc207031448)

[10. Metrics and Key Performance Indicators (KPIs) 6](#_Toc207031449)

[11. Review and Continuous Improvement 6](#_Toc207031450)

[12. Related Documents 6](#_Toc207031451)

[13. Revision History 6](#_Toc207031452)

[Appendix A – Sample Regulatory Obligations Register 6](#_Toc207031453)

[Appendix B – Compliance Calendar (Sample) 7](#_Toc207031454)

[Appendix C – Compliance Metrics Dashboard (Sample) 7](#_Toc207031455)

# 1. Purpose

The purpose of this policy is to establish a governance framework for ensuring the organization’s compliance with applicable laws, regulations, and industry standards related to information security and data protection. This framework enables the organization to reduce regulatory risk, demonstrate accountability, and maintain trust with stakeholders.

# 2. Scope

This policy applies to:

* All organizational entities, subsidiaries, and business units.
* All employees, contractors, and third parties handling regulated data.
* All information assets, systems, and processes are subject to regulatory or contractual obligations.

# 3. Objectives

* Identify and monitor all regulatory obligations relevant to the organization.
* Translate regulatory requirements into actionable controls, policies, and procedures.
* Ensure periodic assessments, reporting, and remediation of compliance gaps.
* Provide evidence of compliance to regulators, auditors, and stakeholders.
* Foster a culture of compliance through training and accountability.

# 4. Regulatory Compliance Framework

1. **Obligation Identification** – Maintain a **Regulatory Obligations Register** that captures laws, regulations, standards, and contractual requirements (e.g., GDPR, HIPAA, PCI DSS, ISO 27001, NIST, local laws).
2. **Control Mapping** – Align obligations to internal policies, controls, and frameworks (e.g., NIST CSF, ISO 27002).
3. **Implementation & Evidence** – Assign responsibilities, implement controls, and retain supporting evidence.
4. **Monitoring & Assurance** – Conduct audits, risk assessments, and continuous monitoring.
5. **Reporting & Certification** – Provide compliance reports to management, regulators, and external parties.
6. **Remediation & Improvement** – Address findings, track corrective actions, and continuously update controls.

# 5. Roles and Responsibilities

* **Board of Directors / Executive Management**: Ensure oversight, approve compliance strategy, allocate resources.
* **Chief Information Security Officer (CISO) / Compliance Manager**: Own compliance program, maintain registers, coordinate audits, report compliance status.
* **Legal & Regulatory Affairs**: Interpret laws/regulations, review contracts, support compliance obligations.
* **Risk & Audit Teams**: Perform audits, assessments, and independent assurance.
* **Business Unit Heads**: Ensure compliance activities are implemented in their domains.
* **All Employees**: Follow compliance policies, participate in training, report potential non-compliance.
* **Third Parties & Vendors**: Comply with contractual and regulatory requirements; provide attestations/certifications.

# 6. Compliance Processes

## 6.1 Regulatory Obligations Register

Maintain a register with the following fields:

* Obligation ID
* Regulation / Standard / Contractual Clause
* Applicability (Business Unit / System)
* Control Mapping
* Responsible Owner
* Review Frequency
* Status

## 6.2 Statement of Applicability (SoA)

Document each control (Applicable / Not Applicable) with justification, aligned to frameworks such as ISO 27001 Annex A.

## 6.3 Compliance Calendar

Define a compliance calendar that includes recurring activities such as audits, assessments, certifications, awareness campaigns, and regulatory reporting deadlines.

## 6.4 Monitoring & Auditing

* Conduct internal audits at least annually.
* Perform control effectiveness testing.
* Maintain audit logs and compliance dashboards.

## 6.5 Reporting

* Quarterly compliance reports to senior management.
* Annual attestation to regulators or certification bodies.
* Immediate escalation of material non-compliance issues.

# 7. Third-Party & Cloud Compliance

* Vendors must provide compliance certifications (e.g., SOC 2, ISO 27001).
* High-risk third parties must undergo cybersecurity due diligence.
* Cloud providers must meet contractual regulatory obligations, with shared responsibility models clearly defined.

# 8. Training and Awareness

* Mandatory compliance training for all employees annually.
* Targeted training for roles with regulatory responsibility (e.g., HR, Legal, IT).
* Awareness campaigns to reinforce compliance culture.

# 9. Exception Management

* Exceptions must be documented, risk-assessed, and approved by the Compliance Manager.
* Exceptions must have compensating controls and expiry dates.

# 10. Metrics and Key Performance Indicators (KPIs)

* % of obligations mapped to controls.
* % of controls with evidence of effectiveness.
* Number of compliance findings (open/closed).
* Time to remediate compliance gaps.
* Vendor compliance certification coverage.

# 11. Review and Continuous Improvement

* This policy and associated registers must be reviewed at least annually.
* Emerging regulations must be incorporated into the compliance framework.
* Lessons learned from audits and incidents must drive continuous improvement.

# 12. Related Documents

* Cybersecurity Risk Management Policy
* Data Protection Policy
* Third-Party Risk Management Policy
* Incident Response Plan

# 13. Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Approved By** |
|  |  |  |  |

## Appendix A – Sample Regulatory Obligations Register

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Obligation ID** | **Regulation / Standard** | **Requirement** | **Business Unit** | **Control Mapping** | **Owner** | **Status** |
| REG-001 | GDPR | Data subject access requests within 30 days | All | Incident Response & Privacy Policy | Data Protection Officer | In Progress |
| REG-002 | PCI DSS | Encrypt cardholder data in storage & transit | Finance | Encryption Standard | IT Security | Compliant |

## Appendix B – Compliance Calendar (Sample)

|  |  |  |  |
| --- | --- | --- | --- |
| **Activity** | **Frequency** | **Responsible Party** | **Next Due Date** |
| Internal Compliance Audit | Annual | Internal Audit | [Insert Date] |
| GDPR Record of Processing Update | Quarterly | Data Protection Officer | [Insert Date] |
| Vendor SOC 2 Review | Annual | Vendor Risk Manager | [Insert Date] |

## Appendix C – Compliance Metrics Dashboard (Sample)

* Obligations Coverage: 85% mapped
* Control Effectiveness: 78% validated
* Open Findings: 6 (4 high, 2 medium)
* Average Remediation Time: 45 days