Compliance Management Policy

Effective Date: 06/01/2025

Introduction

IntelliBoard Inc. mandates a structured compliance management program to ensure adherence to regulatory, contractual, and client requirements, including ISO 27001:2022 (A.18.1, A.18.2), FedRAMP CA-2, SOC 2, GDPR, PCI DSS, CCPA, FERPA, and NIST 800-171. This policy establishes guidelines for managing compliance obligations, complementing the **Risk Assessment Policy**, **Cloud Services Policy**, **Privacy Policy**, and **Awareness Management Policy**.

Objectives

- Maintain continuous compliance with regulatory and client standards.
- Identify, assess, and mitigate compliance risks.
- Ensure audit readiness through documentation and monitoring.
- Foster a culture of compliance through training and oversight.
- Enhance client trust through transparent compliance practices.

Scope

This policy applies to all IntelliBoard employees, contractors, consultants, and third-party vendors involved in operations, covering SaaS, on-premises, and cloud environments.

Definitions and Acronyms

- **Compliance**: Adherence to laws, regulations, standards, and contractual obligations.
- **Compliance Register**: A centralized record of compliance obligations and controls.
- **Audit**: Independent review of compliance status and controls.
- **Non-Conformance**: Failure to meet compliance requirements.

Policy Standards

Compliance Framework

- A compliance register is maintained, documenting obligations (e.g., GDPR Article 32, FedRAMP CA-2), controls, and responsible roles, integrated with the **Risk Assessment Policy**.

- Compliance requirements are mapped to policies (e.g., **Access Management**, **Privacy**) and verified annually.
- The Board of Directors oversees compliance via a dedicated subcommittee, per the **Information Security Policy**.

Risk Assessment and Mitigation

- Compliance risks are assessed annually, per the **Risk Assessment Policy**, with findings integrated into the compliance register.
- Mitigation plans address non-conformances, with timelines and ownership assigned by the CISO.
- Third-party compliance (e.g., CSPs) is verified per the **Third-Party Risk Management Policy**.

Audit and Monitoring

- Annual internal and external audits verify compliance, using AWS CloudTrail and GuardDuty for log analysis.
- Quarterly reviews assess control effectiveness, with findings reported to the CISO and Board subcommittee.
- Non-conformances trigger corrective actions, tracked in the compliance register.

Documentation and Reporting

- Compliance documentation (e.g., policies, audit reports) is stored securely, per the **Asset Management Policy**, with access restricted via Azure Entra.
- Compliance status is reported quarterly to the Board and annually to clients, per the **Communication Procedure and Plan**.
- Regulatory notifications (e.g., GDPR breaches) are coordinated per the **Crisis Management and Communication Policy**.

Training and Awareness

- Annual training covers compliance obligations, risk management, and audit processes, integrated with the **Awareness Management Policy**.
- Role-specific training addresses client requirements (e.g., FERPA for educational data), tracked via HR records.

Incident Reporting and Response

- Compliance violations must be reported within 15 minutes to privacy@IntelliBoard.net, per the **Communication Procedure and Plan**.
- The Information Security Team investigates, implements corrective actions, and notifies regulators as required.

Roles and Responsibilities

- **Chief Information Security Officer (CISO)**: Oversees implementation of the Compliance Management Policy, approves mitigation plans, monitors compliance operations, maintains the compliance register, coordinates with clients and regulators on audits, and reports compliance status to the Board (Eugene Vereshagin, eugene@intelliboard.net).
- **Information Security Team**: Updates the compliance register, conducts audits using AWS CloudTrail and GuardDuty, investigates non-conformances, and implements corrective actions.
- **HR Team**: Coordinates annual training on compliance obligations, per the **Awareness Management Policy**, and tracks compliance via HR records.
- **Employees and Contractors**: Adhere to compliance requirements, report violations within 15 minutes to privacy@IntelliBoard.net, per the **Communication Procedure and Plan**, and participate in audits.
- **Board of Directors**: Provides strategic oversight through a dedicated subcommittee, ensuring alignment with compliance objectives, per the **Information Security Policy**.

Compliance Requirements

This policy aligns with ISO 27001:2022, FedRAMP, SOC 2, GDPR, PCI DSS, CCPA, FERPA, and NIST 800-171, ensuring lawful operations. Non-compliance may lead to disciplinary actions, per the **Human Resources Security Policy**.

Monitoring, Audit, and Continuous Improvement

- Continuous monitoring uses AWS CloudTrail and GuardDuty, with quarterly audits ensuring compliance.
- Policy is reviewed annually, with updates communicated per the **Communication Procedure and Plan**.

Communication and Coordination

Guidelines are communicated through training, client agreements, and reminders, per the

Communication Procedure and Plan. Compliance updates are shared via secure channels.

Non-Compliance Implications
Violations (e.g., ignoring regulatory requirements, falsifying audit data) may result in retraining, termination, or legal action, per the **Human Resources Security Policy**.

Contact Information
Report violations or inquiries to privacy@IntelliBoard.net.