Security Documentation Request Policy

Effective Date: 06/01/2025

Introduction

IntelliBoard Inc. mandates secure, controlled, and auditable handling of security documentation requests to ensure regulatory compliance, protect sensitive information, and uphold contractual obligations. This policy supports ISO 27001:2022 (A.5.32, A.18.1.3), FedRAMP RA-5 and IR-6, SOC 2, GDPR, PCI DSS, CCPA, and FERPA, and complements the Documents and Records Policy, Access Management Policy, Privacy Policy, and Communication Procedure and Plan.

Objectives

- Ensure secure and traceable fulfillment of security documentation requests.
- Restrict access to authorized internal and external parties.
- Maintain audit-ready logs of all request activities.
- Protect confidentiality and integrity of distributed materials.
- Promote awareness of request handling procedures and compliance requirements.

Scope

This policy applies to all IntelliBoard employees, contractors, consultants, clients, and third-party vendors involved in requesting, reviewing, approving, or distributing security-related documentation, including but not limited to SOC 2 reports, FedRAMP documentation, audit logs, risk assessments, and security architecture diagrams.

Definitions and Acronyms

- **Security Documentation:** Official records, policies, diagrams, certifications, and compliance evidence related to IntelliBoard’s security and privacy posture.
- **Requester:** An internal or external party authorized to submit a formal request for security documentation.
- **Sensitive Security Information (SSI):** Documentation that includes confidential architecture, controls, assessments, or credentials requiring protection.
- **Formal Request Process:** Documented request workflow initiated via HelpDesk, including approval and audit tracking.

Policy Standards

Request Initiation and Approval

- All security documentation requests must be submitted through IntelliBoard's HelpDesk system.
- Requests must include the purpose, recipient, justification, and requested retention period.
- External requests must be reviewed by the Information Security Team and approved by the CISO.
- Confidential materials may require execution of a Non-Disclosure Agreement (NDA) prior to release.

Review and Validation

- All requests are reviewed to ensure the requester has a legitimate business or regulatory need.
- Requests for Sensitive Security Information (SSI) are subject to stricter access controls and may be redacted where applicable.
- The Information Security Team ensures the most recent, approved version of the documentation is shared.

Secure Distribution

- Approved documentation is distributed only through secure, encrypted channels (e.g., SharePoint with RBAC or secure document portals).
- Files must be encrypted in transit and at rest (e.g., AES-256, TLS 1.2 or higher).
- Access is time-bound and revoked after the approved retention period or purpose expiration.

Access Controls and Logging

- Distribution systems must enforce role-based access control (RBAC) and Multi-Factor Authentication (MFA), per the Access Management Policy.
- All access and activity related to the documentation must be logged and monitored using audit tools such as AWS CloudTrail.
- Logs are retained for a minimum of 1 year, or longer per contractual or regulatory requirements.

Retention and Revocation

- Shared documentation must be deleted by the recipient after the retention period or at the request of IntelliBoard.
- Access may be revoked at any time if misuse is suspected or upon change in the recipient's status.
- Revocation requests are handled within 24 hours by the Information Security Team.

Incident Response

- Any suspected unauthorized request, access, or distribution must be reported within 15 minutes to privacy@IntelliBoard.net.
- The Information Security Team will investigate and take immediate action, including notification of affected parties and regulators as required.

Training and Awareness

- Annual training covers procedures for requesting and handling security documentation.
- Employees and contractors are required to complete training, tracked via HR systems in accordance with the Human Resources Security Policy.

Roles and Responsibilities

- **CISO:** Oversees implementation, approves documentation releases, and ensures compliance (Eugene Vereshagin, eugene@intelliboard.net).
- **Information Security Team:** Reviews requests, configures access, ensures secure distribution, audits activity, and investigates incidents.
- **HR Team:** Tracks training completion.
- **Employees and Contractors:** Submit requests through formal channels, handle documents securely, and report incidents.
- **Clients and Partners:** May receive approved documentation under NDA, and must protect shared materials as contractually required.

Compliance Requirements

This policy aligns with ISO 27001:2022, FedRAMP, SOC 2, GDPR, PCI DSS, CCPA, and FERPA, ensuring lawful and secure distribution of security documentation. Non-compliance may lead to disciplinary actions, access revocation, or legal enforcement.

Monitoring, Audit, and Continuous Improvement

- Quarterly audits verify request logs, access controls, and distribution channels.
- The policy is reviewed annually, with updates communicated per the Communication Procedure and Plan.

Communication and Coordination

- Guidelines are communicated through onboarding, annual training, and security awareness initiatives.
- External parties are informed of approved request procedures and access conditions during onboarding or contracting.

Non-Compliance Implications

Violations (e.g., bypassing formal requests, sharing documents without approval) may result in retraining, access termination, or legal action.

Contact Information

Report suspected violations or inquiries to: privacy@IntelliBoard.net