Artificial Intelligence (AI) Policy

Effective Date: 06/01/2025

Introduction

This policy establishes governance and controls over the responsible use of Artificial Intelligence (AI) within IntelliBoard Inc., including its integration in product development and internal productivity tools. It ensures AI usage aligns with regulatory, security, privacy, and ethical standards, including ISO 27001:2022 (A.5.10, A.8.30), FedRAMP, SOC 2, GDPR, and CCPA.

This policy complements the Access Management Policy, Change and Configuration Management Policy, Privacy Policy, and Secure Development Lifecycle (SDLC) Procedures.

Part 1: Use of AI in Product Development and Technology

Objectives

- Ensure responsible, secure, and transparent integration of AI in IntelliBoard products.
- Protect customer data and maintain alignment with data privacy and compliance standards.
- Prevent misuse of AI models that may introduce bias, security vulnerabilities, or regulatory risk.

Scope

This section applies to all engineers, data scientists, product managers, contractors, and third parties involved in designing, developing, training, deploying, or maintaining AI/ML capabilities within IntelliBoard products or services.

Standards

1. Data Protection and Privacy

- AI/ML models must not be trained using personal data (e.g., PII, educational records) unless expressly permitted by contract and regulatory authority (e.g., FERPA, GDPR).

- Synthetic or anonymized data must be used where training requires human-derived datasets.
- Data used in model training must adhere to the Data Classification and Privacy Policy.

2. Security and Access Controls

- AI infrastructure must be deployed using secure DevOps and Infrastructure as Code (IaC) practices.
- Access to models, APIs, and training data must be restricted by RBAC, protected by MFA, and logged via audit tools (e.g., AWS CloudTrail, Azure Monitor).
- Models must be evaluated for adversarial vulnerabilities (e.g., prompt injection, data poisoning) before production deployment.

3. Model Governance

- All AI models must be registered with version history, provenance, purpose, and risk classification.
- Model outputs used in decision-making (e.g., learner analytics, recommendations) must include human oversight or controls for interpretability.
- Third-party AI services (e.g., OpenAI, Azure Cognitive Services) must undergo vendor risk review per the Third-Party Risk Management Policy.

4. Ethical Use

- AI features must not promote discriminatory outcomes, misinformation, or opaque automation that impacts users' rights (e.g., grading, admissions, or employment decisions).
- High-impact AI use cases must undergo an AI risk assessment and ethical review prior to launch.

5. Audit and Compliance

- AI model use is subject to quarterly review by the Information Security Team.
- Any AI-enabled features used in FedRAMP systems must adhere to FedRAMP baselines and receive SSP documentation updates prior to ATO submission.

Part 2: Use of AI by Employees for Productivity

Objectives

- Enable employees to responsibly use AI tools to improve individual productivity while protecting company data, intellectual property, and customer confidentiality.
- Set boundaries for use of public AI services versus approved internal tools.

Scope

Applies to all IntelliBoard employees, contractors, interns, and consultants using AI tools in the course of their job duties, including AI writing assistants, coding copilots, chatbots, or internal IntelliBoard-developed tools.

Standards

1. Approved AI Tools

- Only AI tools explicitly approved by the Information Security Team may be used for work purposes.
- Public generative AI (e.g., ChatGPT, Gemini, Copilot) may be used for general assistance (e.g., summarizing public data, code suggestions) but must not be used with:
  - Customer data
  - Proprietary code
  - Confidential documents
  - Regulated data (e.g., FERPA, CCPA, GDPR-covered content)

2. Data Handling Restrictions

- Do not paste or input sensitive or confidential information into public AI tools.
- Use internal tools integrated with IntelliBoard systems when handling customer or proprietary data.
- All AI queries and generated content must follow the Acceptable Use Policy and the Communication Security Policy.

3. Content Validation

- Employees must review and validate any AI-generated output before sharing, publishing, or integrating it into client-facing materials or codebases.

- AI must not be used to impersonate clients, coworkers, or executives in communications.

4. Copyright and Attribution

- Content generated by AI must be treated as IntelliBoard-generated content, subject to copyright standards.
- When using AI-assisted outputs in external materials, include disclaimers or approvals when required by legal or marketing teams.

5. Logging and Monitoring

- Use of AI tools may be monitored for policy compliance, security violations, and misuse patterns.

6. Training and Awareness

- All employees must complete annual AI usage awareness training.
- Departments must request approval from the Information Security Team before deploying new AI tools.

Roles and Responsibilities

Role	Responsibilities
CISO	Approves AI-related systems and tools, ensures policy compliance, and reviews AI risk.
Information Security Team	Conducts AI model reviews, vendor risk assessments, access control enforcement, and audits.
Engineering & Product Teams	Implement AI securely and ethically in product development.
All Employees	Use AI responsibly, follow usage boundaries, and report suspected violations.

Enforcement and Violations

Non-compliance with this policy may result in disciplinary action, including revocation of access or termination. Suspected misuse must be reported within 15 minutes to privacy@IntelliBoard.net.