Collective Data AI Policy

Effective Date: January 1, 2025
Last Updated: January 1, 2025

Purpose

This AI Policy establishes Collective Data's standards for the ethical and secure use, development, and deployment of artificial intelligence (AI) tools and technologies. The policy ensures that AI aligns with our organizational values, complies with legal and regulatory requirements, and maintains the trust of customers, employees, and other stakeholders.

Scope

This policy applies to all employees, contractors, and third-party service providers who engage in the design, development, use, or oversight of AI technologies at Collective Data. It also governs the use of AI in any customer-facing products or internal processes.

Key Principles

Collective Data adheres to the following principles for AI development and use:

1. **Ethical Use of AI:** All AI technologies must be used ethically, avoiding harm, discrimination, or bias. AI must not be used to exploit vulnerabilities or cause harm to individuals or groups.
2. **Transparency:** Collective Data commits to transparency in the development and use of AI, ensuring customers and employees are informed about how AI is used, how it impacts them, and their choices regarding its use.
3. **Security and Privacy:** AI systems must comply with Collective Data's **Data Management Policy**, ensuring that data used in AI tools is protected through encryption, access controls, and other safeguards. Customer data will not be used for AI model training or shared with third-party vendors for this purpose.
4. **Compliance:** AI tools must comply with applicable legal, regulatory, and industry standards. This includes alignment with Collective Data's SOC 2 Type 2 framework.
5. **Human Oversight:** AI must function as a tool to assist, not replace, human decision-making. Employees are expected to oversee AI outputs and ensure they meet required standards.
6. **Accountability:** Employees and teams working with AI are responsible for ensuring its ethical, secure, and compliant use. Violations of this policy will result in disciplinary actions in accordance with company policies.

Governance

AI Committee

The AI Committee oversees the development, deployment, and use of AI technologies at Collective Data. The committee consists of representatives from:

- Engineering
- Product Development
- Compliance
- Security

The committee is responsible for:

- Reviewing new AI initiatives to ensure compliance with this policy.
- Evaluating risks, ethical concerns, and security implications.
- Monitoring AI systems for bias, errors, or harmful outputs.
- Updating this policy as AI-related regulations and best practices evolve.

Employee Responsibilities

Employees engaging with AI tools or systems are required to:

1. Use AI in compliance with this policy and other relevant policies, such as the **Acceptable Use Policy**, **Data Management Policy**, and **Access Management Policy**.
2. Report any concerns or suspected issues with AI tools to their manager or the AI Committee.
3. Participate in required training sessions on the ethical use of AI and compliance with this policy.
4. Ensure that AI outputs are accurate, unbiased, and appropriate before using them in customer-facing or business-critical applications.

Prohibited Uses of AI

The following are strictly prohibited:

1. Using AI to violate any local, state, or federal law or regulation.
2. Using AI for malicious purposes, including but not limited to discrimination, harassment, fraud, or exploitation.
3. Sharing sensitive customer or company data with unauthorized AI tools or platforms.
4. Allowing AI tools to make autonomous decisions without adequate human oversight.

Data and Privacy Standards

1. **Data Use**: Customer data will not be used to train AI models under any circumstances. AI functionalities are strictly limited to supporting customer operations within their application instances.
2. **Sensitive Data**: Sensitive data will be handled in compliance with the **Data Management Policy**.
3. **Vendor Oversight**: All third-party AI tools or services used by Collective Data will be reviewed by the AI Committee and managed under the **Third-Party Management Policy**.

Training and Awareness

Collective Data will provide mandatory training for all employees involved in the development, deployment, or use of AI. Training will include:

- Ethical considerations and best practices for AI.
- Identifying and mitigating bias in AI systems.
- Understanding data security and privacy requirements related to AI.
- Reporting issues and incidents related to AI use.

Monitoring and Reporting

1. **Regular Monitoring**: The AI Committee will monitor AI technologies for compliance, security vulnerabilities, and ethical concerns.
2. **Incident Reporting**: Any suspected misuse or malfunction of AI tools must be reported immediately to the AI Committee or the Information Security Team. Incidents will be investigated in accordance with the **Incident Response Policy**.

Violations and Disciplinary Actions

Violations of this policy, whether intentional or accidental, may result in disciplinary action, up to and including termination of employment or contract. Collective Data may also pursue legal remedies for violations involving malicious intent or significant breaches of trust.

Policy Review

This policy will be reviewed annually by the AI Committee or when changes in technology, regulation, or business needs warrant updates. Any updates will be communicated to all employees.
