Generative Artificial Intelligence Policy

Effective April 24, 2023

Table of Contents

Introduction

Ironclad, Inc. (“Ironclad” or the “Company”) recognizes that large language model-based, generative AI applications (collectively, “AI” or “generative AI”), such as OpenAI’s ChatGPT, have the potential to be incredibly useful and time-saving on a variety of tasks. We anticipate a growing interest in the use of AI in Ironclad’s business operations. At the same time, Ironclad also recognizes that AI technologies are still being refined, are known to produce inaccurate or distorted information, and that the use of AI can create significant risks for the Company. We believe it is essential to establish clear guidelines for the responsible use of AI. This Policy provides guidelines for using AI in a way that protects Ironclad’s proprietary information and complies with applicable laws, regulations, ethical standards, and Ironclad’s company values.

As AI is a rapidly evolving technology, Ironclad will review and update this Policy to reflect technological advancements, legal developments, and industry best practices.

Scope

This Policy applies to all Ironclad employees, executives, consultants, agents, vendors, and other third parties who have access to Company Data. For purposes of this policy, these individuals will be referred to as “**Ironclad Staff**.”

This Policy applies to the direct use of generative AI tools by Ironclad Staff members, separate from any generative integrations that Ironclad has embedded in its products. Although Ironclad may partner with companies offering AI (e.g., Ironclad’s integration with OpenAI), Ironclad Staff’s direct use of AI tools offered by these same companies is not covered by the partnership or services agreements with those companies, but is instead subject to the companies’ terms of use for their AI tools.

Definitions

The term “**Company Data**” should be interpreted broadly for purposes of this Policy, and includes, but is not limited to, at least the following: All Company business information and all personal data (whether of employees, executives, contractors, consultants, Customers, consumers, users, or other persons) that is accessed, collected, used, processed, stored, shared, distributed, transferred, disclosed, destroyed, or disposed of by any of the Company systems; all proprietary information and intellectual property (including, but not limited to, source code, designs, schematics, product roadmaps, product plans, product specifications, market analyses, white papers, strategy documents, financial information, internal communications, Customer lists, Customer files, Customer contact information, Customer contracts, Customer’s proprietary data, and any non-public Company information. Company Data includes information in written, electronic, audio, video, or any other form or medium. Company Data can include any level of information covered by Ironclad’s Data Classification Matrix.

The terms “**Ironclad Customer**” or “**Customer**” refer to any unique contracting entity listed within an active order form with Ironclad, including all individuals acting on the entity’s behalf.

The term "**Customer Data**" refers to any and all data that the third parties who contract as Customers with Ironclad provide to Ironclad to use, store, transmit, or process.

Principles for the Use of AI

Ironclad Staff should observe the following principles when using AI:

Compliance with Legal and Regulatory Requirements
Ironclad Staff must comply with all applicable laws and regulations governing the use of AI. This includes compliance with data protection and privacy laws, intellectual property laws, and anti-discrimination laws.

Protection of Data Privacy and Security
Ironclad Staff must ensure that they protect data privacy and security when using AI. The use of AI tools and applications must comply with the Company's data privacy and data security policies.

Human Backstop
Ironclad Staff must carefully review AI-generated material for inaccurate or incomplete information and potential infringement of third-party rights. You are ultimately responsible for all content produced with the assistance of AI, as if you were the original creator. The source of AI-generated material should be disclosed when appropriate.

Guidelines for the Use of AI

Required Actions

- Before using any generative AI tool for any Company business, you must opt out of letting generative AI tools use any data you feed the tool to train their AI models (Opt out for OpenAI via this link).
- Before using any generative AI tool for any Company business, consult Ironclad's Data Classification Matrix to determine the classification of the data you intend to feed into the tool, to determine if it is too sensitive to share.
- Carefully review AI-generated material for accuracy, completeness, and protection of both third-party rights and Ironclad's proprietary information.

How You May Use Generative AI

- If you use AI for authorized, Company-related activities, you must use accounts created with Ironclad email addresses/credentials.

- Your usage of AI must comply with this Policy, Ironclad's Code of Business Conduct and Ethics, and the confidentiality obligations in employment documentation signed by Ironclad Staff at the time of hire.
- You may only use data with generative AI tools that is legally obtained and used with the necessary permissions.
- You may only use data with generative AI tools that is not confidential, highly confidential, or restricted, as defined by Ironclad's Data Classification Matrix.
- You may only use vendor integrations or products featuring generative AI that have been approved by the Legal and Security teams.
- You must report any security incidents or suspected breaches immediately to security@ironcladhq.com and legal@ironcladhq.com.

Prohibited Use of AI

- Do not use personal accounts with AI tools for Company-related purposes.
- Do not use Customer Data with generative AI tools.
- Do not use any Company Data classified as confidential, highly confidential, or restricted information (as defined in our data classification matrix).
- Do not use personally identifiable information (e.g., people's names, addresses, emails) with generative AI tools.
- Do not use generative AI tools for Company-related purposes if you have not opted out of letting generative AI tools use any data you feed to the tool to train their AI models.

Enforcement

The Chief Information Security Officer ("**CISO**") and Security Team will verify compliance to this Policy through various methods, including but not limited to, business tool reports, and internal and external audits. Any exception to the Policy must be approved by the CISO and General Counsel, or designees, in advance. Any Ironclad Staff member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or engagement, or legal action where appropriate.

Document Control

Document Owner

Chief Information Security Officer

Revision History

Effective Date	Version	Contributors	Notes
04-24-2023	1.0	CISO, Info Sec, Legal, IT	Created