AI Policy

Version Number	2.0
Last Approved	Feb 25, 2025
Classification	PUBLIC

Overview

This AI Policy establishes criteria for adoption and use of artificial intelligence (AI) and machine learning (ML) models and making proper use of their results. AI and ML tools and services may include but are not limited to Customer Support & Chatbots (such as ChatGPT and Sentiment Analysis tools), Predictive Analysis tools (such as Churn Prediction or Demand Forecasting), Personalization tools (such as content recommendations and dynamic AI market condition analysis), Data Security tools (such as anomaly detection or fraud detection), Automation or Generative AI tools (such as Zapier or Copilot), and Natural Language Processors (NLP) (such as voice assistants or text analysis tools that analyze customer feedback).

Applicability

The applicability of this policy falls under purview of the Security Documentation Overview.

Purpose

As AI emerges as a significant new factor, this Policy aims to ensure AI related considerations are incorporated into all relevant group processes and capabilities. These guidelines are intended to allow for use of AI in a responsible and ethical manner. The guidelines will also ensure we meet our contractual obligations with our customers regarding the use of their data.

Scope

This policy applies to all employees, contractors, vendors, internal and client-facing systems and services of the Company.

AI Policy

AI Principles

The Company is committed to the following responsible uses of AI:

Human Oversight

The Company believes that human oversight and accountability is essential to the reliable operation of artificial intelligence (AI) and machine learning (ML) models and making proper use of their results. Accordingly, ML- or AI-enabled solutions should provide data-based recommendations to human decision-makers, which they can then decide how to act upon.

Monitoring

Where AI is to be used, Company personnel should implement audit and risk assessments to test their ML models as the baseline of their oversight methodologies. The Company should also test their models for fairness, performance, and drift before deploying, but also continue to monitor those issues to ensure the models are operating as intended.

Privacy & Confidentiality

Where AI is to be used, Company personnel should provide adequate information about how the AI will be used to handle personal data in privacy statements made available to clients' employees, customers, and/or job applicants (as applicable). Any ML models used by Company and/or any of its business units should seek to minimize access to identifiable information to ensure that the AI only uses the personal data it needs to generate insights to the extent permitted.

When using AI, Company personnel should similarly define, monitor, and enforce appropriate handling of sensitive and confidential information to prevent unauthorized access, use, or disclosure.

Company personnel should also maintain a robust security program for their ML models, including designing them in line with appropriate security standards and protecting them against misuse or compromise.

Explainability and Transparency

Company personnel should strive to develop ML models that are explainable and direct, with clear purposes. Company personnel should provide clients with information about how their ML models operate, their proper use, and their limitations, so that clients can implement those models in accordance with their design and purpose, operate them effectively, and use their

outputs as intended. Company personnel should also provide disclosures to those who interact with and are impacted by the use of an AI tool.

Considerations of Impacts

The Company's approach to AI should include reflection upon requirements for fair, safe, and responsible use. Users should strive to identify new and unexpected sources of harmful outcomes, such as bias and then refresh and enhance the design of their products and services to address them.

AI Concepts in Policies

AI Topics	Related Policy and Process
Suppliers' / Vendors' Use of AI	Policy: Vendor Management Policy
Company Internal Use of AI	Policies: • Vendor Management Policy • Acceptable Use Policy (AUP) Process: For New Tool and/or New Usage of Tool Security Service Desk
Monitoring AI Use	Policy: • Vendor Management Policy • Internal Audit and Compliance Policy Process: • Employees / Contractors - IT tool and activity monitoring process • Vendors - Vendor Risk Assessment process • Company Products - Secure Software Development (SDLC) Policy and product development process

AI Policy Administration	Policy: Information Security Statement
AI Bias	• Built into Secure Software Development (SDLC) Policy phases including but not limited to Phase 2: Systems and Requirement Analysis & Phase 4: Documentation and Testing, ensuring products function as designed • Transparency and disclosure inside product documentation
AI Training	Policy: Information Security Statement Process: Annual Security Awareness Training, Using AI Securely Training, Data Protection Training
Product Design and Testing of/with AI	Policy: Secure Software Development (SDLC) Policy
AI Policy Noncompliance	Policies: • Security Documentation Overview • Internal Audit and Compliance Policy Process: • Disciplinary Actions, Exceptions and Questions (within above policy) • Internal audits
Privacy and AI	Policy: • Vendor Management Policy

	• Client Data Privacy Compliance Policy • Privacy Notice

Usage of AI

The use of personal user accounts for company business or involving Company or customer data in any way is prohibited.

Free plans and subscriptions do not generally meet our security and privacy requirements. Enterprise/business plans that include additional safeguards are required unless specifically cleared via the vendor risk assessment process.

Only approved AI tools may be used; these are assessed via the Vendor Management Policy and approved for a specific use case (including the specific classifications of data that are allowed for each use case). Changes in the intended use of AI must be reassessed as discussed in the Vendor Management Policy to broaden the scope/use case.

AI Governance

The Company has implemented an AI Management System that is aligned with ISO 42001 to embed a standard, internationally recognised governance framework over the Company's relevant processes. The requirements of our AI Management System have been integrated into our existing management systems certified to ISO 27001 (Information Security Management System) and ISO 27701 (Privacy Information Management System). The Company's internal audit program rigorously monitors adherence to the AI Management Systems control set.

Document control

This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	@Art Machado	
Author(s)	@angelina.kilmer , @Art Machado @Paul Gordon	
Required Approver(s) and Approval Date	@Art Machado - VP of Information Security	Feb 25, 2025
Review cycle	ANNUAL	
Next review date	Feb 24, 2026	

Version History

Date	Author(s)	Version	Changes
Feb 25, 2025	@Art Machado @Paul Gordon @angelina.kilmer	2.0	Annual review
Nov 1, 2024	@angelina.kilmer	1.2	Changed Policy classification from Confidential to Public
Jul 15, 2024	@Wasim Khan @Val Brunson (Unlicensed)	1.1	High level review and updates on AI Principles
Jun 4, 2024	@Sarah Zwicker (Unlicensed) @angelina.kilmer @Art Machado	1.0	Original Version