KNIGHT TRANSPORTATION SWIFT TRANSPORTATION

INFORMATION TECHNOLOGY

Artificial Intelligence Acceptable Use Policy

20231109

PURPOSE

AI technology is a powerful tool that can be used to create a wide range of content, including text, images, audio, and source code. Tools can also be conversational in nature and provide answers on a wide variety of topics. As a company that utilizes this technology, we have a responsibility to ensure that its use is legal, ethical, and in compliance with our corporate values and policies.

This document will be reviewed at least annually to ensure that it remains relevant and effective.

SCOPE

This document outlines the acceptable use policy for the appropriate use of proprietary and third-party AI technology by our employees and contractors, on company-provided hardware and tools, as well as on contractor devices that are used for accessing, storing, or processing Company data.

DEFINITIONS

- Artificial Intelligence (AI) - AI refers to technology that can mimic human behavior or go beyond it.
- Generative Artificial Intelligence (GenAI) – GenAI is a type of AI technology that can produce various types of content (e.g., text, image, video, synthetic data, source code) based on input prompts.
- Confidential Information – KNX information including but not limited to passwords, certificates, personally identifiable information (PII), asset names, company trade secrets or other intellectual assets outside the company.
- Machine Learning - This subcategory of AI uses algorithms to automatically learn insights and recognize patterns from data, applying that learning to make increasingly better decisions.

POLICY

KNX does not want to discourage employees from interacting with new and innovative technology; the Company asks that employees and contractors follow the following standards when using these tools on Company provided IT equipment:

- Use the technology only for legitimate business purposes that are in line with our corporate values and policies.
- CIO or Department VP shall consider, review, approve/disapprove, and document as appropriate all GenAI systems requested for use to ensure that only authorized applications are applied by the business. Anyone desiring to use GenAI systems associated within Knight-Swift should submit an IT HelpDesk ticket for approval consideration.
- Ensure that the content generated by AI technology is accurate, reliable, and appropriate for its intended purpose.
- Take appropriate measures to prevent the misuse or abuse of AI technology, including but not limited to, securing access to the technology, monitoring its use, and reporting any suspicious activity.
- Respect the intellectual property rights of others and ensure that the content generated by AI technology (i.e., AI generated source code, images, audio, text) does not violate any third-party copyrights, trademarks, etc.
- All systems, within or outside of immediate company control, that use GenAI are considered part of this policy. This includes all third-party systems that may consume prompting from, train with, or provide inputs to, Knight-Swift

systems using GenAI systems. KNX cannot control the actions of third parties but shall control how such systems interact with Knight-Swift.

Bias Prevention in AI Usage:

- AI technology is powerful and efficient, but it can pick up biases from the data it's trained on. This hidden bias might affect different AI applications, leading to decisions and results that might not always be fair or equal.
  - Be aware of the potential for bias in AI interactions, especially when AI is utilized in decision making processes.
  - Seek approval from the KNX Legal Department before using AI tools for employment-related decisions, including but not limited to: hiring, discipline or compensation.

Prohibited Uses:

- The Company requires that its valued and trusted employees and contractors use their best judgement to ensure that they are not partaking in illegal activities or other prohibited uses, including but not limited to, cybercrime, fraud, distribution of malicious content, identity theft, and phishing scams.
- Inputting Personally Identifiable Information (PII), customer data or financial data into an AI tool is strictly prohibited.
- Individuals with concerns about the usage of AI should talk to their department head, IT leadership or Internal Audit.

EXCEPTIONS

Exceptions must be approved by the Company CIO on a case-by-case basis and shall be granted for limited duration with an accompanying plan for mitigating potential risks. Approvals and accompanying plans must be documented on Helpdesk tickets.

COMPLIANCE

Enforcement, communication, and monitoring of this Policy is the responsibility of applicable department VP's. This Policy is ultimately under the jurisdiction of the Company and the Company may revoke or remove this privilege at any time. Each authorized user of any Company IT system, server, service, and/or software application is required to comply with this Policy and related documents. This policy may at times be subject to special evaluation and interpretation in terms of compliance adherence. Conclusions regarding policy interpretation will be supported by Department Heads, Compliance, and Internal Audit.

Incidents determined to be in non-compliance with this Policy will be assessed for severity and will carry a possible range of sanctions or disciplinary actions, up to and including termination.

POLICY OWNERS	Knight and Swift: VPs of IT and Business Department Heads		
EFFECTIVE DATE	01/01/2024	**NEXT REVIEW**	Quarterly