



Artificial Intelligence Policy Statement

Albireo Energy is a leading independent building controls and energy services provider recognized by customers for creating intelligent, high-performance buildings. We help building owners and their teams make decisions about building automation that achieves operating performance, decarbonization and sustainability goals.

Purpose and Scope

The purpose of this statement is to establish the framework for managing risks associated with Artificial Intelligence (AI) systems within Albireo Energy. It aligns with the National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF) and applies to all AI systems developed, deployed, or used by Albireo Energy. This includes internally developed models, third-party AI solutions, and AI-driven decision-making systems. Additional procedures and guidelines may be developed to address specific AI use cases and regulatory requirements.

Guiding Principles

Albireo Energy adheres to the following core principles in its AI governance and risk management practices:

- **Trustworthiness:** AI systems must be valid, reliable, safe, secure, resilient, accountable, transparent, explainable, privacy-enhanced, and fair—with harmful biases actively identified and managed.
- **Human-Centeredness:** AI systems shall augment human decision-making and uphold human rights, dignity, and autonomy.
- **Socially Responsible and Sustainability:** AI systems will be developed and deployed with consideration of societal impacts, environmental sustainability, and long-term ethical implications.
- **Compliance:** AI practices align with applicable laws, regulations, standards, and internal policies.

Governance Structure

The Office of the CIO leads our management policies and controls, with all work in line with the company's risk management register led by the Office of the CFO. Clear roles and responsibilities have been outlined for AI developers as well as employees, and third parties to ensure that all AI initiatives adhere to ethical and legal standards.

Office of the CIO | AI Responsibilities

The Office of the CIO is responsible for the following scope of work:

- Ensuring that AI systems are fair, transparent, and accountable.
- Implement bias mitigation strategies to prevent discrimination.
- Confirming that AI decisions must be explainable and auditable.
- Ensuring that all AI development and deployment complies with NIST AI RMF, GDPR, EU AI Act, and other applicable laws.
- Conducting risk assessments for all AI projects before deployment



- Maintaining an AI inventory and classify systems based on operational, ethical, security, and compliance risks.
- Conducting AI performance and behavior monitoring and response plans.
- Reviewing AI policies annually in alignment with evolving regulations.

Employee Responsible Use Policy

In March 2025, Albireo Energy implemented this AI responsible use policy that all employees are required to certify. The policy includes the banning of:

- The usage of non-Microsoft AI meeting note taking software.
- The usage of the Chinese generative AI tool, DeepSeek.
- The uploading of sensitive company information into any generative AI tools.
- The uploading of personally identifiable information into any generative AI tools.

As a supplement to the company's robust data management and cybersecurity training protocols, Albireo Energy is implementing required Responsible AI training as part of our learning management system to track completion. It includes all elements of this policy and a knowledge check to ensure understanding.

Third Party Responsible Use

Vendors, contractors, and third-party AI service providers are expected to comply with this policy. Due diligence and contractual obligations are enforced to ensure alignment with Albireo Energy's Code of Conduct and ethical standards.

Enforcement and Review

All employees and stakeholders must adhere to this AI RMF Policy. Non-compliance with this policy may result in corrective action, including suspension of AI projects or disciplinary measures. The Office of the CIO reviews and updates this policy annually.