Cybersecurity and Data Privacy Policy Statement

The purpose of this statement is to express Albireo Energy's commitment to the most stringent cybersecurity and data privacy protocols.

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.

Data Privacy and Security

Cybersecurity and Data Privacy

Keeping employee and customer data secure and private is a top priority and our vendor selection and compliance requirements are reflective of our commitment. Our cybersecurity and data privacy policy statement outlines specific protocols we follow. In 2025, there were zero enterprise systems impacted by cybersecurity incidents.

Governance and Oversight

Our IT organization provides central oversight with decentralized local implementation. Central management and oversight establish cybersecurity standards and strengthened security controls.

Our CIO provides updates on security and privacy to the Executive Team and Board as needed. The CIO's team includes a Security Administrator responsible for data security and IT engineers who manage day-to-day security operations across the Albireo Energy network.

We conduct ongoing reviews of our internal systems, resources, and employees to assess whether changes need to be made. All computer systems are monitored 24/7 by a leading global provider of Security Operations Center (SOC) services.

Employee Training

Albireo Energy's IT Security Awareness and Training Procedure helps prevent Internal information security breaches and includes. Training modules, covering both privacy and security, are designed to improve security culture, change behavior, and significantly lower security risk. KnowBe4 is our training provider, focusing on mitigating the top human error-related security risks using current trending data.

We supplement formal training modules with ongoing cybersecurity awareness, incorporating practical tips into key meetings, formally debriefing unsuccessful threats, and recognizing employees who actively prevent cyber threats during all-employee forums.

Specifically, our training procedures include:

- Employee onboarding training includes phishing and other data security threat avoidance.

- Monthly simulated phishing attacks. Employees who fail three simulated phishing attacks are assigned additional training.
- Quarterly cybersecurity training assignments. Supervisors are notified if training assignments are not completed within the allotted time.
- Cybersecurity updates during the quarterly all-employee meetings. Cyber Star of the Quarter Awards are presented where employees are recognized for their proactive response to real-world cyber threats.
- Cybersecurity Awareness Month education. Our Security Operations Center provides weekly learning topics to employees.

Call out: 100% of employees have completed required training.

Employee and Customer Data

Albireo Energy's employee data is managed by a third party in a SOC2 Type II data center that is tested annually for compliance. Customer data is stored within a Microsoft application operating platform spanning two data centers that are both annually certified as SOC2 Type II compliant.

We often monitor customer operational data that our building performance experts collect. When operating exceptions are detected within a customer's building, we provide the customer with configurable alerting services.