SciSure AI Statement

SciSure uses Artificial Intelligence (AI) within its products to enhance productivity, user experience, and scientific workflows. AI is implemented in a controlled and secure manner, with strong safeguards to protect customer and company data.

AI capabilities are available across the SciSure platform and include:

- AI assistants and chat capabilities;
- AI-powered content generation;
- AI-assisted data extraction and transformation;
- Customer-integrated AI models.

Core Principles

- **Human Oversight:** AI outputs are reviewed before use or implementation.
- **Data Minimization:** AI accesses only the data necessary to perform its intended function.
- **Transparency:** AI-powered features are clearly identified to users.
- **Security & Compliance:** AI capabilities are governed in alignment with ISO/IEC 27001, ISO/IEC 42001, GDPR, and applicable security and privacy requirements.
- **Customer Control:** Customers retain control over their data, AI integrations, and configuration.

AI Feature-Specific Safeguards

AI Chatbot (Astra Iris)

SciSure Research

An optional add-on that can be installed via the marketplace to support users in finding relevant product documentation. It does not process or access customer data and is strictly limited to publicly available content from https://support.elabnext.com/ .

- **Strict data limit access** by design to mitigate exposure risk;
- **Prompt filtering** to ensure appropriate and legitimate use;
- **Clearly identified as an AI-powered assistant**, with user awareness during onboarding;
- **User validation required** before acting on responses;
- **Powered by OpenAI language models.**

enquiries@scisure.com
3 Center Plaza, Suite 501
Boston, MA 02108 United States
scisure.com

AI Protocol Generator

SciSure Research

An optional add-on that can be installed via the marketplace to generate a written protocol based on the users prompt. It does not process or access customer data and is strictly limited to publicly available content from the internet.

- **Strict data limit access** by design to mitigate exposure risk;
- **User review required** before implementation;
- No autonomous execution without user validation;
- Operates under the same **data protection and access controls;**
- **Powered by OpenAI language models.**

ChemSnap

SciSure Health & Safety

An optional add-on that can be installed via the marketplace that enables users to photograph a chemical container label and automatically convert the label information into inventory records. The feature extracts relevant information such as chemical name, CAS number, quantity, units, and lot number, and maps it into the ChemTracker inventory format.

- Customer-identifying information (such as organization name, locations, and account details) is **not sent** to the AI model;
- Customer data **is not used to train** the AI model;
- Users review extracted information before it is committed to inventory records.
- **Powered by OpenAI language models.**

Procurement Connect

SciSure Health & Safety

An optional add-on that can be installed via the marketplace that uses AI to transform procurement and order data into standardized inventory records. It identifies inventory-relevant line items and normalizes information such as chemical identity, quantities, units, packaging, and container counts for import into ChemTracker.

- Uses **AWS Bedrock Nova**;

- Customer-identifying information (such as organization name, locations, and account details) is not sent to the AI model;
- Customer data is not used to train the AI model;
- AI-generated transformations are subject to user review before use.

Customer-Integrated AI Models

SciSure Research

An optional MCP-based integration that allows customers to connect their own Large Language Models (LLMs) to their data. While support for commercially available models is included, typical usage involves locally hosted, on-premises LLM deployments managed by the customer.

- Customers may connect their own AI models for research purposes;
- **Access control and scoped permissions are enforced** (e.g., OAuth 2.1);
- **Clear separation of responsibilities** between SciSure and customer-managed AI;
- Customers are responsible for the configuration and use of their AI models.

Data Protection & Security

- AI systems operate under restricted access controls;
- Customer data is not used for model training unless explicitly controlled and safeguarded;
- All AI outputs require human validation before use;
- Security monitoring and risk assessments are continuously performed.

Summary
SciSure ensures that AI is used responsibly, securely, and transparently, with feature-specific controls in place to protect data, maintain trust, and support safe innovation.