SciNote

Security and Compliance Whitepaper

Enterprise-Grade Security and Compliance for Modern R&D IT

Trace Every Step. Trust Every Result.

Introduction

This guide outlines the data protection, privacy, and compliance framework behind SciNote Premium plans, detailing the technical infrastructure, product features, and certifications we've put in place to help keep your work safe, traceable, and audit-ready. Whether you're an IT decision-maker, QA lead, or lab administrator, you'll find the information needed to confidently evaluate SciNote as your secure ELN of choice.

Need more details? We're always happy to provide additional documentation or schedule a technical consultation.

Table of Contents

In this guide, you will find information about:

Questions? Contact us at **premium@scinote.net** or **security@scinote.net** with any security or compliance inquiries.

1. Infrastructure Security

SciNote is a cloud-based lab management software, which means the application is available online. Users access SciNote with their username and password, allowing them to manage their research data and collaborate with others in real-time.

SciNote takes several approaches to ensure infrastructure security to our software.

1. 1. Cloud Hosting

SciNote is hosted on **Amazon Web Services (AWS)**, ensuring strong global infrastructure, automatic redundancy, and **a 99.99% uptime commitment**. Software updates and system maintenance are handled by SciNote – saving internal IT teams time and energy.

1. 2. Server Environment

Each SciNote instance is running on the AWS infrastructure where several approaches are taken to ensure data safety and availability, including: Autoscaling, Load balancing, Point-in-time database restoration, Cross regional backups and more.

Each SciNote Premium client (industry and academic plans) is hosted in a single-tenant environment and has its own application instance. Users of an organization will access SciNote via a unique URL.

1. 3. Server Locations

SciNote servers are located across North America, Europe, Asia, and Oceania, with daily backups securely stored in geographically separate regions (e.g., Ireland for EU clients). This ensures business continuity even in case of regional disruptions.

1. 4. Data Storage and Backup

SciNote stores and backs-up data in two ways:

PostgreSQL Relational Database
This database is backed up using automatic Amazon AWS tools on a daily, weekly, and monthly basis. For SciNote Premium, we keep the last 35 daily backups, weekly backups of the previous month and all monthly backups.

Files Database
For files that are uploaded into SciNote, we use Amazon AWS S3 service.

We replicate all files that are uploaded into SciNote into a separate S3 server at the separate back-up location, as mentioned previously. The mirroring is done with no deletion, so even if you (accidentally) remove files from SciNote they are still stored in the mirrored data center.

1. 5. Data Encryption

Your data is encrypted both when it is in transit between the client (e.g., the browser you use to access SciNote) and the server, and at rest (stored or backed up).

SciNote uses the following means of data encryption to ensure maximum security.

Encryption of data at rest to prevent unauthorized access:	Encryption of data in transit via secure symmetric cryptography to prevent third-party data breaches:
• The server-side encryption uses one of the strongest block ciphers available: 256-bit Advanced Encryption Standard (AES-256).	• All data between clients and SciNote are encrypted using strong HTTPS protocol (TLS 1.3), RSA SSL certificate and strong 256-bit key exchange. • SciNote also communicates with external services using safe connections (SSL technologies): Heroku PostgreSQL database (SSL) and Amazon S3 (HTTPS).

1. 6. Self-Hosted Option

For organizations requiring complete internal control (e.g., pharma manufacturing or government research), SciNote offers a locally hosted solution. In this setup, security responsibilities are shared. We assist with deployment, validation, and system updates.

"With the help of SciNote implementation specialists, we chose which features of the software worked best for us and defined a company-wide method for recording data. SciNote then trained all our staff."

Rita Cruz
Section Head (Strain Engineering) , Ingenza (UK)
Read the Ingenza case study

2. Software Development & Application Security

2. 1. Development Process

SciNote takes a compliance-first approach in our Software Development Life Cycle (SDLC) where we ensure we're meeting industry standards and regulatory commitments. In doing so, we also provide features to help meet customers' global requirements.

Each development sprint includes internal QA, security testing, and implementation of user feedback. Critical patches are prioritized for immediate release outside regular cycles.

More information regarding our quality management process can be found in the Operational Security section.

Figure 1. SciNote Software Development Life Cycle (SDLC) process phases.

2. 2. Accountability and Validation

SciNote enterprise-grade Platinum plan includes qualified Installation Qualification (IQ) and Operation Qualification (OQ) support, ideal for regulated teams working under GLP/GMP standards.

2. 3. Product Updates

SciNote software developers are constantly improving SciNote. These improvements, including data protection features and security updates, are based on both internal goals and objectives, and on the feedback from our users as shown in our SDLC.

All new features developed in a certain period are released together with each software update.

For cloud-based SciNote users, all updates are automatic and done by SciNote.

For Platinum plan users, there are two releases each year – one in spring, and one in autumn. Each release will include all the updates between the previous Platinum release till the new release. Hotfixes and patches are pushed for severe security issues when identified, in addition to the two releases.

For self-hosted users, updates are on average performed at least once every 3 months. Even though SciNote provides all necessary information, updates are done by the organization's internal IT personnel.

"We demoed a variety of different ELN software solutions over a period of around nine months with different teams within research. As well as being 'easy to use', we also had requirements such as single sign on, and being compliant with EU law in relation to GDPR etc.

SciNote provides a relatively easy to use interface considering the amount of functionality as well as our security requirements"

Nathan Adams
Senior Scientist, NanoTemper (CA, USA)

3. Product Data Protection and Security Features

SciNote ELN includes many data security and protection features, so you can be in full control of your data. These features will also help you meet data integrity requirements set internally by your organization or externally by regulatory agencies or other stakeholders. Additionally, data in SciNote ELN is backed up regularly on a daily, weekly, and monthly basis.

> **FDA definition of a "Closed System"**
> Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records on the system.
>
> SciNote is a closed system by design; customers are responsible for managing access to the content.

3. 1. User Roles & Permissions - Summary

Role-based access controls in SciNote can be **team-based (organization/workspace)** and **project-based**. Each role has a predefined set of permissions that determine whether a user can create, edit, delete, view, or manage data. Premium customers have an additional **Organization Administrator role** that can control permissions system-wide.

SciNote has three levels of roles:

Organization Level

Administrator – Manages organization settings, roles, and members.
User – Standard access without organization management rights.

Workspace Level

Owner – Manages workspace members and roles; can give themselves access to any project.
User – Creates, edits, and archives projects, inventory items, protocols, and reports.
Viewer – View-only access to items shared with them or the workspace.

Project / Experiment / Task Level

Owner – Full control over project data and members.
User – Similar to Owner but cannot manage members or archive projects.
Technician – Follows protocols, completes steps, and leaves comments in protocol steps.
Viewer – View-only access to project data.
Reviewer *(optional plan feature)* – Same as Viewer but can comment, sign off on tasks, and request/revoke their own task signatures.

For a detailed breakdown of SciNote's user roles and their associated permissions, please refer to the applicable tables here: **LINK**.

3.2. Identity and Access Management (IAM)

Premium plan clients can configure enterprise authentication using:

- 2-Factor authentication (2FA)
- Single Sign-On (SSO)
- Password protection policies
- IP restrictions
- LDAP/Active Directory integrations
- Session timeout controls

These tools integrate with your existing IT infrastructure and reduce password fatigue.

3.3. Audit Trail and Timestamped Actions

All actions within SciNote ELN are automatically timestamped and tracked, so users know exactly who did what and when. Activities can be filtered by several parameters, such as user, sample, date, and action.

Selected SciNote Premium plans have access to the additional audit trail function, which includes exportable timestamped records that display both old and new data values. This allows for full traceability of all customer data in SciNote ELN.

SciNote customers reported up to **70% less time spent preparing for audits** after enabling our audit trail and compliance monitoring tools.

3.4. Deleting and Archiving

When it comes to information that is no longer needed, data within SciNote ELN can only be archived, not deleted, with the exception of a few elements (individual protocol steps, their contents, and comments). This is to ensure the completion of your records and to support data integrity and traceability practices. Archived information can be restored at any point if the data is needed again in the future.

3.5. FDA Title 21 CFR Part 11 Compliance

Selected SciNote plans and add-ons offer features that support compliance of FDA 21 CFR Part 11 (or similarly, EU Annex 11), which outlines the requirements for validation, audit trail, legacy systems, copies of records, and record retention for electronic records.

Features supporting 21 CFR Part 11 include: detailed audit trail, advanced user management, electronic signatures, electronic witnessing, and security features such as password expiration settings and system log records.

For details of these features, and SciNote's compliance matrix showing how the software supports each 21 CFR Part 11 provision, **see our 21 CFR Part 11 overview.**

3.6. GLP and GMP Compliance

The core mindset of "good practice" - for example, Good Laboratory Practice (GLP) and Good Manufacturing Practice (GMP) - lies in traceability (the ability to follow along the history of the development process of a product or an experiment) and accountability (the ability to discern who has contributed to this process and when).

To this end, SciNote ELN enables GLP/GMP compliance and makes it more straightforward by ensuring all study-related documentation can be saved and structured in a systematic way.

- Protocols and inventories are organized within repositories and can be used (and reused) and linked to individual experiments. Repositories offer version control ability.
- Information within SciNote, such as samples, people, date, inventories, experiments, and results can be easily referenced and assigned.
- Entry format is unified throughout SciNote.
- Experiment templates can be set up and reused to ensure consistency.
- Product reports can be generated and exported in accessible formats by users.

For details on how SciNote can help you meet GLP/GMP requirements, **see our guide on GMP and GLP compliance.**

3.7. Software Validation

SciNote uses internal software design and software validation processes to ensure that the delivered product meets specifications.

Additionally, SciNote's Platinum plan offers quality assurance services, with installation qualification (to verify SciNote is installed correctly) and operation qualification (to ensure the application is operating as expected). It offers a dedicated separate validation instance, and controlled software updates and releases to ensure the application meets the organization's QA requirements.

For details on SciNote's QA services, **see the Summary of SciNote's Quality Assurance Services.**

3.8. Data Export

Data within SciNote ELN can be exported in several ways:

Reports - Users can create reports by selecting any piece of data within SciNote ELN and structure it in a report, which can be saved and downloaded in .pdf and .docx formats. All files which have been uploaded in SciNote ELN can simply be downloaded in the same way.

Protocol Export - All protocols can be exported in .eln format, which means they can be uploaded to another SciNote team or organization at any time.

Export All - This feature is available for all SciNote Premium plans, which lets customers export all of the project's data in a readable format with all relevant attachments neatly organized in folders.

Inventories Export - Users can export inventory items from SciNote inventories. Each user can export the data they have access to, based on the project user role permissions.

3.9. Data Portability

Although we strive for long-lasting business relationships with our customers, we understand the importance of exit freedom when it comes to switching between ELN vendors without compromising your data. This is why SciNote has a well-defined exit strategy for our customers, designed around data portability.

Upon subscription cancellation, Premium customers are offered a time period to export their data, using the reports and export all features described before.

Database Dump: All Premium customers receive a link with two directories.

- **The first ('database')** contains a database dump in SQL format, that customers can import into PostgreSQL database using psql command.
- **The second ('files')** contains all files within SciNote, that should be located on the filesystem.

There is also a third file 'variables.env' which contains necessary environmental variables for setting up a SciNote instance (if needed), and correctly interpreting the folder structure files within SciNote ELN, that should be located on the file system.

3.10. Deleting the SciNote Premium Instance

Since data for each SciNote Premium customer is hosted on separate instances, the instance is shut down upon cancellation with all data deleted.

4. Operational Security

A few key practices and processes related to operational security are incorporated into the quality management activities at SciNote, including but not limited to:

- **Routine internal auditing** to evaluate our quality management system and raise awareness about critical process management. This helps us identify areas in security for improvements so we can take proactive actions to address them.
- **CAPA (Corrective and Preventive Action) processes** to identify, resolve, and prevent issues of quality nonconformity (the failure to meet one or more of the existing requirements). These issues are considered urgent and are addressed immediately.
- **Ongoing security testing and validation** to ensure our software functions as intended and meets the required standards of quality and reliability. It also helps identify any potential bugs, errors, or vulnerabilities that will affect software security, allowing for timely resolution before the software reaches the end-users.
- **A streamlined bug reporting process** through each customer's dedicated customer success manager allows users to report any unexpected issues or flaws they encounter while using the software, enabling prompt investigation and resolution by the development team.

By adhering to these measures, SciNote endeavors to maintain a robust and proactive security framework that safeguards your valuable data.

"Data security was another motivating factor [to transition to an ELN]. We once had a faulty fire sprinkler go off and damage several notebooks. When this happened, we knew we had to find a better way to protect our data. "

Chris Landers
Senior Protein Chemist, Athens Research and Technology (GA, USA)

5. Organizational & Corporate Security

A security policy, which the SciNote and its members adhere to, is in place. The policy encompasses standards and protocols for the handling of physical space, data security, data encryption, data transmission, handling of security incidents (security incident response plan), reporting of security incidents, and security education. Highlights from our security policy includes:

- **Access to physical/digital spaces:** Access to our office space is restricted to employees only, with reception security guard; access to our digital files is controlled by single sign-on and security credentials.

- **Ongoing security training (including incident response):** All employees receive security training during their onboarding process to ensure they are familiar with privacy and security best practices, incident reporting mechanisms, and actions to prevent unauthorized access. Budget is allocated for the development team to receive annual education for security best practices in the industry.

If a third-party vendor service is utilized at SciNote, **the vendor assessment and management plan** comes into place, where all vendors go through a rigorous screening and selection process to ensure they meet not only business but also privacy and compliance requirements. All vendors will sign data processing agreements and non-disclosure agreements.

Additionally, we implement the following policies to ensure there will not be interruptions to your access to data even when changes happen within SciNote.

Change management policy: This policy establishes a formal framework for managing changes within SciNote, including changes to code and infrastructure, ensuring a controlled and efficient process while upholding key principles and facilitating effective communication:

- No Data Loss Principle
- No Access Loss to Data Principle
- Reversibility Principle
- Minimal Downtime Principle
- Traceability Principle

Disaster Recovery and Business Continuity Planning: This set of protocols and procedures will prepare SciNote for disruptive events, to minimize risks and impacts, and to ensure restoration of business operations quickly.

We are proud to maintain a **98% customer satisfaction rate**, thanks to the reliability, professionalism, and responsiveness of our technical support team.

6. Certification, Frameworks & Compliance

6.1. Industry Certifications and Declarations

SciNote is certified and regularly audited to meet the needs of regulated R&D:

- ISO/IEC 27001:2022 certified Information Security Management System
- SOC 2 compliance
- Cyber Essentials Certification (UK)
- Supports full compliance with 21 CFR Part 11, EU Annex 11, GLP, and GMP

View current certifications and documentation at: **SciNote Trust Center**

We understand the importance of covering all compliance angles, so everything's ready for your security, legal, QA, or leadership team to review.

6.2. GDPR, CCPA, and Users Privacy Policy

SciNote is committed to complying with the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) by making personal data protection across our company a priority.

A detailed, clear and transparent description of our handling of Users personal data can be found in our **SciNote Users Privacy Policy**. It describes every aspect of User's personal data - from how and why we process personal data to data protection rights and how they can be exercised.

Our terms and policies can be found on our website: **https://www.scinote.net/legal/**

6.3. SciNote's Commitment: CIA in Action

SciNote's security framework is built on the CIA (Confidentiality, Integrity, Availability) triad — the foundation of information security:

Confidentiality	Integrity	Availability
• Encryption at rest and in transit • Single-tenant architecture isolating customer data • Role-based permissions and confidentiality settings	• Immutable audit logs • Versioning and rollback capabilities • Cryptographic data validation • Secure file upload and manipulation practices	• AWS-backed 99.99% uptime • Auto-failover infrastructure • Point-in-time backups • Tested disaster response systems

This triad is what ensures your research is available, accurate, and only accessible by authorized individuals.

Let’s Talk - Welcome to the World of SciNote

A cloud-based lab management solution trusted by the FDA and USDA

If you'd like to verify our certifications, explore integrations, or conduct a data protection impact assessment (DPIA), we’re happy to help.

- General inquiries: **premium@scinote.net**
- Technical and security inquiries & documentation: **security@scinote.net**

Explore all our active certifications, policies, and downloadable documentation:
SciNote Trust Center

At SciNote, we celebrate science and its achievements to help humanity. We believe that science can provide solutions to better understand the challenges we are facing today and will be facing in the future to help save our planet.

We look forward to the journey together.

SciNote’s Security-First Ethos: