SciNote

Protecting Your Data – Data Security and Privacy at SciNote

Introduction

This guide for SciNote Premium plans will provide a clear overview of the data protection and security measures SciNote puts in place to ensure your data is secured and highlight the features available to help you safeguard your data. It will give you the information you need when choosing the right ELN for your lab, and help you gain an understanding of the efforts we make to protect your work. Additional resources and supporting documents are available upon request to provide further technical details, should you require them.

Table of Contents

In this guide, you will find information about:

Questions? Consult with one of our team members at premium@scinote.net. We are happy to answer any questions you might have for your organization.

1. Infrastructure Security

SciNote Electronic Lab Notebook (ELN) is a cloud-based software, which means the application is available online. Users access SciNote ELN 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; these approaches are limited to our cloud-based/hosted offering, and not for the self-hosted option.

1. 1. Cloud Hosting

SciNote utilizes the Amazon Web Services (AWS), one of the strongest platform providers available, to host your data. **We employ various mechanisms to store and backup your data securely - we are committed to 100% data persistence via multi-regional backups.**

An important security benefit to a cloud-based platform is that software installation, development and updates are all part of the service we offer; this means **you are always using the most up-to-date software version** and helps reduce the workload of the internal IT team if you have one. It is also especially convenient for organizations that don't have an internal IT team at hand, as you don't need to rely on individual users to make sure the software is up to date to meet your security requirements.

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.

It is important to emphasize:

- Cloud hosting does not affect secured access to your data – access to customer data on the AWS servers is available only to your SciNote application based on each user's individual permissions. This is similar to how others don't have access to your emails even if you host your emails using a cloud-based service such as Gmail.
- You maintain full rights and ownership over your data, as stated clearly in our Terms of Service: https://www.scinote.net/legal/

1. 3. Server Locations

SciNote utilizes data centers in North America, Europe, Asia, and Oceania; new data centers are added depending on needs and additional security purposes.

Backups for all SciNote instances are in Dublin, IRELAND, EU. **The original database and backups are kept at separate locations on purpose, to ensure data remains unharmed in the unlikely case of natural disasters at one location.**

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 1.2), 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. Local Installation

The previous sections describe the infrastructure security measures SciNote takes to safeguard the data hosted within its cloud-based software.

In the case where organizations have internal rules and policies that require them to store data on locally hosted servers instead, SciNote can offer local installation with our Premium plans – please contact us for additional information. Here, an internal member or team from the organization will be responsible for deployment, maintenance, and updates of the software. We will work closely with this internal member or team to facilitate the process.

As such, infrastructure security for the self-hosted SciNote will remain the responsibility of the customer.

"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. Software Development Life Cycle (SDLC)

SciNote takes a compliance-by-design approach in our 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

Additionally, SciNote has been developed using agile software development practices, allowing us to have frequent software releases. This offers more flexibility in terms of the product development roadmap, enabling us to quickly adapt to customers' needs and to deliver improvements. It also means that if any security issues do arise - whether discovered through regular internal processes or through user feedback - they can be addressed very quickly by our team.

Agile software development practices also prioritize software quality by design. Testing and debugging are a vital part of every software development cycle; they are incorporated in the process by default.

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

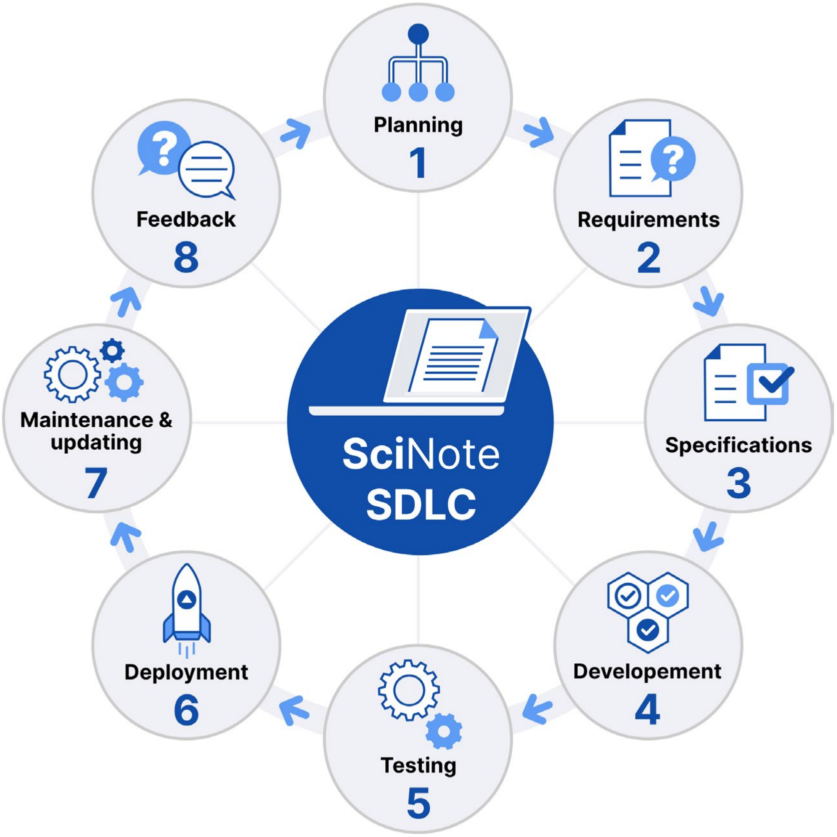


Figure 1. SciNote Software Development Life Cycle (SDLC) process phases.

2. 2. 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 local installation 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

User roles and permissions in SciNote can be team-based and project-based. Each user role in SciNote ELN has a pre-defined set of permissions that affects each user role's ability to create, edit, delete, view, and access data within SciNote ELN. These permissions are controlled by an additional user role called "Organization Administrator" that is available to Premium customers. See the VIDEO that explains user roles and permissions in detail.

User role	Access and permissions
Organization Administrator	has full authority when it comes to managing users and Teams within the Organization, i.e., the SciNote instance with a unique URL link.
Owner	has full authority when it comes to managing the people and the data on the projects.
User	has very similar rights as the Owner, with the exception of not having the privileges to manage its users. Furthermore, the User cannot archive projects. They can archive experiments, workflows, tasks, and results.
Technician	can view the task protocol and complete its steps. They can also leave comments. They cannot create, edit, or restore a task, nor can they create, edit, or delete the protocol steps.
Viewer	can only view the project's content. These roles are cascaded automatically to experiments and tasks from the project, but you can change the permission at any level.

3.2. Identity and Access Management (IAM)

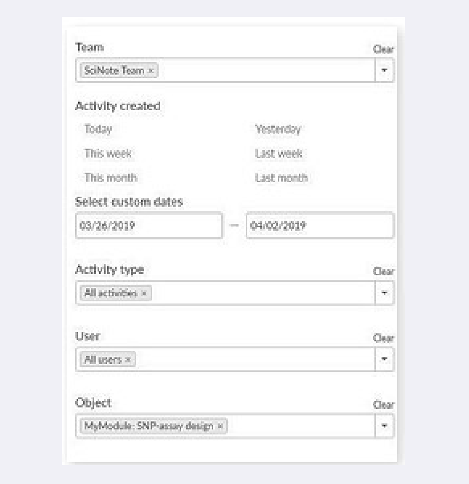
Several access security features are available through SciNote ELN, depending on the plans and add-ons subscribed to.

Available to all SciNote plans	Available to selected plans or as add-ons
• 2-factor authentication • Single sign-on • Enforced password change	• Enforced 2-factor authentication • Enforced single sign-on • Enforced password policy • IP whitelisting / blacklisting • Password complexity (require custom password length/complexity) • Password rotation

3.3. Timestamping, Activity Tracking, and Audit Trail

All actions within SciNote ELN are 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.



Team: SciNote Team ×

Activity created

Select custom dates: 03/26/2019 – 04/02/2019

Activity type: All activities ×

User: All users ×

Object: MyModule: SNP-assay design ×

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.

Want to know how SciNote helps protect your IP?

Download the IP whitepaper

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.

6. FedRAMP, Certification & Compliance

6.1 FedRAMP and Security Certifications

We are proud to announce that **SciNote is currently in the FedRAMP Authorization process as a part of our commitment to customer needs and the trust they place in our product.**

The Federal Risk and Authorization Management Program (FedRAMP®) is a United States federal government-wide compliance program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. It provides a standardized approach to security authorizations for Cloud Service Offerings.

SciNote is used at the FDA, USDA and other industry organizations.

Our security standards align with and go beyond the requirements of many security certifications. **Upon request, we will provide supporting documents to demonstrate our information security management system (ISMS), as defined by ISO/IEC 27001, is appropriately managed and maintained.**

For the up-to-date status of SciNote certifications, including SOC2, ISO/IEC 27001, NIST, and FedRAMP, please contact us directly as these processes are ongoing.

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.

If customers are acting as data controllers and wish to use SciNote for personal data processing, we are available for help and consultation on how to achieve that for your organization.

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

Questions? Consult with one of our team members at premium@scinote.net.
We are happy to answer any questions you might have for your organization.