Security Overview

How we protect sensitive biotech financial data.

Effective date: June 21, 2026 · Version 1.0
Provided by [Exigyn, Inc.] · exigyn.com

DRAFT — FOR LEGAL REVIEW

This Security overview is a working template for Exigyn. Statements about controls, certifications, and timelines below must be confirmed as accurate before publication — do not claim a certification (e.g., SOC 2) that is not yet in place. Items in [brackets] require confirmation. Remove this notice before going live.

Exigyn handles sensitive financial and operational data for life-sciences companies, and security is built into how we design, build, and run the platform. This page summarizes our security program and how to report a concern. It is provided for transparency and does not modify any contract.

1. Our Approach

We follow a defense-in-depth philosophy and the principle of least privilege across infrastructure, application, and operations. Security and privacy requirements are considered throughout our development lifecycle rather than bolted on at the end.

2. Encryption

- **In transit:** data is encrypted using TLS 1.2 or higher between your browser and the Service.
- **At rest:** stored data is encrypted using AES-256 or equivalent industry-standard encryption.

3. Infrastructure and Hosting

The Service runs on reputable cloud infrastructure providers [e.g., AWS / Google Cloud / Vercel — confirm] operating in secure, audited data centers. Production environments are logically segregated from development and testing, and access to production is restricted and monitored.

4. Tenant Isolation and Access Control

- Each customer's workspace is logically isolated so that one customer cannot access another's data.
- Access within an organization is governed by role-based permissions and least-privilege defaults.
- Authentication protects account access; [single sign-on (SSO) and multi-factor authentication (MFA) — available / on the roadmap; confirm].
- Internal administrative access to systems is limited to authorized personnel, granted on a need-to-know basis, and logged.

5. Application Security

- Secure development practices, including code review and version control.
- Dependency and vulnerability scanning of our software supply chain.
- Input validation and protections against common web vulnerabilities.
- [Periodic penetration testing by an independent third party — confirm cadence.]

6. AI and Connector Security

AI features and connectors (Excel, PowerPoint, and the Claude / MCP connector) are designed with data minimization in mind. Connectors authenticate using scoped credentials that you control and can revoke. Customer Content sent to AI sub-processors is processed under contractual terms that prohibit using your data to train third-party models, and we limit the data shared to what is needed to produce the requested output.

7. Sub-processors and Vendor Management

We evaluate the security and privacy practices of third-party providers before engaging them and put data-protection terms in place. A current list of sub-processors is available on request and, where applicable, under a Data Processing Addendum.

8. Logging, Monitoring, and Incident Response

We maintain logging and monitoring to help detect anomalous or unauthorized activity and operate an incident-response process for triage, containment, and remediation. In the event of a confirmed personal-data breach affecting you, we will notify affected customers without undue delay and consistent with our legal obligations and contractual commitments.

9. Resilience and Backups

Customer data is backed up on a regular schedule, with backups encrypted. We maintain business-continuity and recovery practices with target recovery objectives [RPO/RTO — confirm targets].

10. Personnel Security

- Personnel are bound by confidentiality obligations.
- Security awareness is part of onboarding and ongoing practice.
- Access to customer data is limited to those who need it to perform their role.
- [Background checks where permitted by law — confirm.]

11. Compliance

We align our practices with applicable data-protection laws, including the GDPR and the CCPA/CPRA, and support customers' compliance through our Privacy Policy and DPA. [SOC 2 Type II and any other certifications: state accurately whether achieved, in progress, or planned — confirm before publishing. Do not imply certifications that are not yet in place.]

12. Customer Responsibilities

Security is a shared responsibility. We ask that you use strong, unique passwords, enable available account-protection features, manage your Authorized Users and their permissions, safeguard data you export from the Service, and promptly report suspected issues.

13. Reporting a Vulnerability

We welcome reports from security researchers and the community. If you believe you have found a vulnerability, please email **security@exigyn.com** with details and steps to reproduce. We ask that you act in good faith, avoid privacy violations and service disruption, and do not access, modify, or delete data that is not yours. We will acknowledge your report, investigate, and work to remediate confirmed issues; we will not pursue good-faith research conducted in line with this policy. [A PGP key and any bug-bounty scope can be linked here — confirm.]

14. Contact

SECURITY CONTACTS

Security disclosures & vulnerability reports — **security@exigyn.com**

Privacy & data requests — **privacy@exigyn.com**

General support — **support@exigyn.com**