INFORMATION SECURITY CONTROLS AND TECHNICAL AND ORGANIZATIONAL MEASURES

The following sections define Exigyn's information security controls and technical and organizational measures to protect Client Data and are incorporated into the Master Services Agreement.

1. Physical Access Control

- Exigyn has architected its systems to eliminate physical access or security risk, as the software is a cloud-based installation hosted on Vercel and Supabase. No physical media containing Customer Data is maintained by Exigyn.

2. System Access Control

Data processing systems used to provide the software are prevented from being used without authorization through the following measures:

- Multi-factor authentication (MFA) is required to access production systems.
- All personnel access Exigyn's systems with a unique identifier (user ID). Shared credentials are prohibited.
- User access rights are granted on a least-privilege basis and revoked promptly upon separation.
- Exigyn maintains a password policy that prohibits password sharing, governs responses to password disclosure, and requires passwords to meet minimum complexity requirements. All passwords are stored in encrypted form.
- Production database and API access control lists are configured to deny all inbound connections unless from authorized sources.
- Endpoint security software is maintained on all devices used to access production systems or Customer Data.
- Security patch management is implemented to provide regular and periodic deployment of relevant security updates.

3. Data Access Control

Persons entitled to use data processing systems gain access only to the Customer Data they have a right to access. Customer Data must not be read, copied, modified or removed without authorization. Exigyn takes the following measures:

- Customer Data requires the same or higher protection level as “confidential” information according to Exigyn’s security classification standard.
- Access to Customer Data is granted on a need-to-know basis. Personnel have access only to information required to fulfill their duty.
- All Customer Data is isolated by organization at the database level via row-level security policies. No customer can access another customer’s data through the application.
- A retention and deletion standard governs how data and data carriers are securely deleted or destroyed once no longer required.

4. Data Transmission Control

Except as necessary for the provision of the software in accordance with the Agreement, Customer Data will not be read, copied, modified or removed without authorization during transfer. Exigyn takes the following measures:

- All data in transit is encrypted using Transport Layer Security (TLS) v1.2 or above and HTTPS.
- API endpoints do not accept unencrypted connections.

5. Data Input Control

It will be possible to retrospectively examine and establish whether and by whom Customer Data have been entered, modified or removed from Exigyn’s data processing systems. Exigyn takes the following measures:

- Only authorized personnel may access Customer Data as required in the course of their duty.
- Exigyn has implemented a logging system to record input, modification, or deletion of Customer Data within the software to the extent technically possible.

6. Personnel Control

Customer Data processed on behalf of the Client is processed solely in accordance with the Agreement and related instructions of the Client. Exigyn takes the following measures:

- Exigyn uses controls and processes to monitor compliance with contracts between Exigyn and its sub-processors or other service providers.
- All Exigyn employees and contractors are contractually bound to respect the confidentiality of all sensitive information, including trade secrets and Customer Data.

7. Availability Control

Customer Data will be protected against accidental or unauthorized destruction or loss. Exigyn employs regular backup processes to provide restoration of business-critical systems as necessary:

- Supabase-hosted databases are configured with automated daily backups and point-in-time recovery.
- The production environment is monitored through automated alerting tools. Alerts notify responsible personnel at predefined degradation thresholds related to performance and processing capacity.
- Critical and high-risk incidents are tracked through resolution.

8. Data Separation Control

Customer Data collected for different purposes can be processed separately. Exigyn takes the following measures:

- Multi-tenancy is enforced at the database level via row-level security policies, achieving data separation among customer data from multiple customers.
- Customers only have access to their own organization’s data.

9. Data Integrity Control

Customer Data will remain intact, complete and current during processing activities. Exigyn takes the following measures:

- Exigyn has implemented a multi-layered defense strategy as protection against unauthorized modifications.

In particular, Exigyn uses the following controls:

  - TLS encryption in transit; AES-256 encryption at rest
  - Row-level security and access control restrictions
  - Restriction of production access to authorized personnel only
  - Multi-factor authentication controls
  - Endpoint security software
  - Production data logging and monitoring
  - External and internal penetration testing
  - Regular internal audits to validate security measures