Terminal X Protects Your Data

We know how important your data is. Keeping your data secure isn't just a feature to us – it's core to how we operate. We've built our platform with industry-leading security measures and trusted infrastructure to safeguard the data you entrust to us.

WHAT IT MEANS TO: Our Users - Finance, Investment, Business Professionals

Our client universe consists of the most highly regulated institutions and they trust us with their Enterprise Data. We have tens of thousands of users on our platform using the service daily with their private data securely protected. We NEVER train on your data, or sell them to third parties.

Your Data Is Safe With Us: End-to-End Encryption

- Secure Connections: Anytime you interact with Terminal X, your connection is secured using HTTPS secure web protocol, encrypting data flowing between your device and our servers. Access always requires successful user authentication.
- Data Locked Down at Rest: Information you store in Terminal X, including content, database entries, and user data, is encrypted using the strong Advanced Encryption Standard (AES)-256 *before* it's written to disk.
- Infrastructure-Level Protection: We utilize Google Cloud Platform's built-in encryption for the underlying storage systems, adding another layer of defense.
- Database Encryption: Client specific DBs, Terminal X Web Index, Search Engine, Private Datarooms where your data is stored are directly encrypted

Google Is Our Data Security Partner

- Choosing the Right Partner: We run Terminal X entirely on Google Cloud Platform (GCP). We chose GCP for its world-class security posture and hardened global infrastructure.
- Physical Security is Google's Job: GCP manages the physical security of the data centers housing our servers. This includes 24/7 monitoring, strict access controls, background checks for staff, and multi-layered surveillance – things best handled by a dedicated infrastructure provider.
- Leveraging GCP Security Tools: We serve on GCP's best-in-class security services.
    - Identity & Access Management (IAM): To strictly control who and what can access specific resources within our cloud environment.
    - Virtual Private Cloud (VPC): To create isolated network segments, preventing unauthorized communication between different parts of our system and the public internet.
    - Firewalls: Configured to allow only necessary traffic (primarily HTTPS) to reach our application servers.

We Cannot Access Your Personal Information

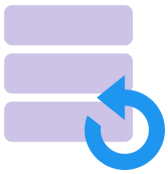
- The Terminal X agent systems have highly limited user info, such as your personal logins and password, email addresses, social security numbers, query logs, anything you input while using the platform
- Any other personal data including your research entitlements and associated username, passwords in our systems are protected in accordance with GDPR, CPRA regulations

WHAT IT MEANS TO: Compliance, Data Security, IT Officers

Security, compliance, privacy, and reliability are foundational to our approach to protecting our customers' data.

Terminal X Security Policies Comply With The Highest Global Standards

- Designing to High Standards: While we are a growing company, we've designed our security controls, policies, and procedures based on established frameworks like SOC 2.
- SOC 2-Compliant: We have all the procedures & policies in place for SOC 2 Type 2 certification. This is a rigorous, independent audit-validated certification, and we ensure that our systems and processes securely handle your data to this global standards.



Operational Security: Backups, Planning, and Training

- Resilience Through Backups: We perform regular data backups to ensure we can recover information in case of unexpected events.
- Planning for the Unexpected: We maintain disaster recovery plans and emergency protocols to ensure service continuity and data protection.
- Ongoing Risk Management: Security isn't static. We continually assess potential risks and adapt our defenses.
- Human Factor: Our team receives regular training on security best practices to minimize risks associated with human error.

We Constantly Monitor, Test, and Audit Our Security Systems

- Eyes on the System: We continuously monitor our systems, logging access and activity to detect potential anomalies or threats.
- Constant Vigilance at the Server Level: Service health and performance are tracked to spot issues like denial-of-service attacks.
- Putting Our Defenses to the Test: We conduct regular internal security reviews and vulnerability assessments. We also plan to engage independent, third-party security experts for penetration testing to proactively find and fix potential weaknesses.