Privacy And Security in Cloud App

Your privacy is important to us, and so is being transparent about how we collect, use and share information about you.

This policy aims to help you understand all these aspects which we will describe later in this article.

Secure Personnel

Kepler Technologies Inc. prioritizes the security of its data, along with that of its clients and customers. It ensures that only certified personnel have access to their resources.

- All employees, contractors, and others who require access to sensitive or internal information must sign Confidentiality or other types of Non-Disclosure Agreements (NDAs).
- We integrate security culture into our business by conducting employee security training and testing using current and emerging techniques and attack vectors.

Secure Development

- All development projects at Kepler Technologies Inc. follow secure development life cycle principles.
- To ensure security requirements are met, a design review is conducted on all new products, tools, and services, as well as major changes to existing ones.
- All team members who regularly participate in system development undergo annual secure development training in coding or scripting languages that they work with as well as any other relevant training.

Secure Testing

Kepler Technologies Inc. frequently employs third-party penetration testing and vulnerability scanning services to monitor all production and Internet-facing systems.

- Before deployment to production, all new systems and services are scanned.
- Internal security engineers conduct penetration testing on new systems and products or major changes to existing systems, services, and products to guarantee a comprehensive and real-world perspective of our products and environment from multiple viewpoints.
- As part of our software development process, we test both static and dynamic software application security for all code, including open source libraries.

Cloud Security

Kepler Technologies Inc. develops and implements the necessary and sufficient measures to ensure the Availability, Integrity, and Confidentiality of data.

Kepler Technologies Inc. Cloud provides maximum security with complete customer isolation in a modern cloud architecture.

Kepler Technologies Inc. Cloud leverages the native physical and network security features of the cloud service, and relies on the providers to maintain the infrastructure, services, and physical access policies and procedures.

- All customer cloud environments and data are isolated using Kepler Technologies Inc.'s patented isolation approach. Each customer environment is stored within a dedicated trust zone to prevent any accidental or malicious co-mingling.
- To ensure that data breaches and unauthorized access are prevented, all data is encrypted both at rest and during transmission.
- Our entire platform is constantly monitored by Kepler Technologies Inc. experts who are highly trained and dedicated.
- To protect and isolate data, we use unique encryption keys to separate each customer's data from our own.
- Our access controls are based on role-based controls and the principle of least privilege access, and we review and revoke access as required.