Security Policy

Last Updated: Dec 08, 2023

1. Security

1.1 Product Security

Product security is paramount at Luopaisi. Luopaisi performs continuous integrations, allowing us to rapidly respond to both functional and security issues. Well defined change management policies and procedures determine when and how changes occur. We employ many security practices, including:

Web server configured to prevent directory traversal and cross-site scripting

Argon2 password hashing

Query string layer preventing malicious code injection

HTTPS by default for everything

Secured Cloud Infrastructure in AWS

1.2 Physical Security

Our Luopaisi-as-a-service offerings are hosted in Amazon Web Services (AWS). Physical and environmental security related controls for production servers, which includes buildings, locks or keys used on doors, are managed by AWS. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors.

1.3 Corporate Security

Luopaisi leverages internal services that require Transport Layer Security (TLS/SSL) for network access and individually authenticate users, commonly by way of a central identity provider and leveraging two-factor authentication wherever possible.

2. Data

2.1 Secure Communication

All private data exchanged with Luopaisi is always protected using Transport Layer Security (TLS/SSL). If encrypted communication is interrupted, the Luopaisi application is inaccessible. Luopaisi does not “fail open.” Luopaisi is careful not to log sensitive values in clear text.

2.2 Protection of Data at Rest

Customer data at Luopaisi is encrypted using XChaCha20Poly1305IETF for secure storage of sensitive data and Data Backups are encrypted at rest using AES256.

2.3 Customer Data Storage Location

Luopaisi Service data currently resides in the United States of America.

2.4 Data Retention

For Service users, we will retain your personally identifying information (PII) for as long as your account is active or as needed to provide you access and use rights, which may include a limited 90-day tail period to allow for an orderly wind-down. Generally speaking, “full resolution” electronic information transmitted or received by you in relation to your use of the Service will be retained for a rolling 15-month look-back period, after which such information may be aggregated on the basis of a one-minute resolution for the duration of the Service period and

any tail period. In addition, we may retain and use your information as necessary to comply with our legal obligations, resolve disputes and enforce our agreements.

2.5 Gathering of Personally Identifiable Information (PII)

Certain visitors to the website and Service choose to interact with Luopaisi in ways that require Luopaisi to gather personally identifiable information (PII). The amount and type of information that Luopaisi gathers depends on the nature of the interaction. For example, when signing up for a trial of the Service, we may ask a user to provide the user's name and the name of the user's company, as well as an email address and telephone number where we may contact the user and/or another representative of the user's company. Each user is also expected to provide a username and password that, along with other information, we use to create and administer accounts. In each case, Luopaisi collects such information only insofar as is necessary or appropriate to fulfill the purpose of the visitor's interaction with Luopaisi.

Luopaisi does not disclose PII other than as described in the Luopaisi Privacy Policy. In addition, visitors can always refuse to supply personally identifying information, with the caveat that it may prevent them from engaging in certain activities.

2.6 Customer Data Access

A limited number of Luopaisi personnel have access to customer data via access controlled and logged mechanisms. Personnel engaged in customer support access a support application similar in structure to the Luopaisi end user web application that allows them to access customer data. Access to this system requires authenticating to our central identity provider and using two factor authentication. Access to the customer support portal is strictly logged. Technical operations personnel have access to the raw service data storage. This access requires using a secure access management proxy, authentication via SSO, and two factor authentication. Access to the staging and production management infrastructure is strictly logged. All other personnel are prohibited from accessing customer data.

Contact Us

If you have any questions or concerns about these Terms of Service, please email us at support@luopaisi.us.