DiliTrust

Security is our #1 priority

Security Policy

Physical infrastrusture

DiliTrust's servers are certified and comply with the strictest international security standards. The data hosted is not shared in the cloud, and is not subject (in any way) to the U.S. Patriot Act, thus providing a permanent control on the access to information. The servers are hosted in France by a French service provider.

ISO 27001 Hosting

In order to continuously improve data protection and ensure the confidentiality of all information, all DiliTrust systems and data are hosted on servers that have obtained the highest international certifications in the field of computer security.

The hosting is certified by the international standard ISO/IEC 27001:2013.

This standard guarantees the implementation of an Information Security Management System for data safety. ISO 27001 also specifies control measures to ensure the relevance of the system to provide our clients with the highest level of security requirements.

Physical security

Physical access is restricted by a security badge control system, video surveillance and on site security personnel 24/7.

- Rooms are equipped with smoke detection systems.
- Systematic double power supply.
- Generators with an initial autonomy of 48 hours.
- 2 network connections to and within the data centre.
- 2 network rooms capable of taking over from one another.

24/7 Monitoring

Our systems are monitored 24/7 for any attempted attack or technical event:

- Technical hardware monitoring, memory level, software performance...
- Automatic alerts in case of detection of suspicious activities.
- Firewall, IDS (Intrusion Detection System), anti-flood system and protection against brute-force attacks.

All servers have redundant storage and network access as well as a daily system of full backups.

Backups

Daily backups are performed and stored in a secondary location (geographically remote) that meets the same security requirements as the production servers.

Backups are stored for a maximum of seven days (7 sliding days) and then they are permanently destroyed (overwritten) with no possibility of recovery. For instance: Monday's backup file automatically overwrites the previous Monday's file.

DiliTrust

Security is our #1 priority

Security Policy

Encryption

« Data-at-rest »: AES 256

All confidential data at rest is encrypted using the Advanced Encryption Standard (AES, Rijndael) with a 256-bit key. On both servers and mobile devices (for the data stored locally).

« Data-in-motion »: HTTPS 256 bits

Our standard for all traffic (data in motion) in or out of our servers is a systematic TLS encryption (protocols TLS 1.0, 1.1 and 1.2 only) with the highest levels of encryption (256-bit). No unencrypted traffic is authorized. Only modern and secure browsers are allowed (IE9 +, Firefox, Chrome, Safari) and DiliTrust native mobile applications. Access is denied for outdated and insecure browsers (such as IE6).

Application level

2 levels of redundant safety controls: internal audits and regular external human audits. Upon discovery of a security vulnerability, it is corrected or patched as soon as possible. The recommendations and best practices are systematically applied whenever possible on a "best effort" basis.

Internal audits

DiliTrust has strict internal procedures to enforce the best security practices:
- Internal Procedures of "code review" and security tests before each release of new features.
- Internal security test and the use of various security audit tools. Mainly those available in the Linux Kali distribution (sqlmap, burpsuite, nmap… etc).

External audits by independent experts

At least once or twice a year, we perform a complete security audit by an external company specialized in information security ("human" penetration testing non-automated).

Passwords Policy

Each user is identified by a unique username and password. All users must choose their own secure password.

No password is emailed or apparent at any time or to anyone. Passwords are stored in hashed form, after a one-way encryption (injective).

The default minimum password policy is as follows:
- Must contain at least three different types of characters (lowercase, uppercase, numbers or punctuation).
- Minimum 10 characters length.

Password recovery procedure (or first access): email with secure single access link (invalid after 24 hours and once used).
Each and every request made to our servers is authenticated to verify the user's identity, and whether the user has the appropriate permissions to execute the requested action. Only if these checks successfully pass, does the request get passed to the main application for execution.

Two Factor Authentication (TFA) option by SMS: after the entry of the login and password, the user will receive an SMS with a code to enter to complete authentication. Each code is for a single use and is specific to a login attempt.