HOSTING SERVICE

TRAXESS SOLUTIONS

Traxess AG
Bleicherweg 10 - CH 8002 Zurich - T +41 43 505 1331 - E info@traxess.ch - UID CHE-109.083.955

INTRODUCTION

This document defines the standards applied to the Software Hosting Service for Software developed by Traxess and offered to clients as a Web Application in a software-as-a-service model.

It shall serve as information for stakeholders within the client's organisation and as an appendix to a Master Service Agreement.

1. HOSTING INFRASTRUCTURE

Hosting of Client Applications

- Data centre location: Nuremberg, Germany
- DC operator: Hetzner Online GmbH, Industriestrasse 25, 91710 Gunzenhausen, DE
- DC is operated according to the ISO 27001 standard.

Hosting of Back-up Client Applications and Recovery Site

- Data centre location: Helsinki, Finland
- DC operator: Hetzner Finland Oy, Huurrekuja 10, 04360 Tuusula, FI

Hosting of Traxess Backbone Functions

- Data centre location: Nuremberg, Germany
- DC operator: Hetzner Online GmbH, Industriestrasse 25, 91710 Gunzenhausen, DE

Server Infrastructure

- The software and data are hosted on encrypted containers dedicated to each client system on virtual servers, based on dedicated data centre hardware.
- Access to the containers is strictly limited to Traxess, therefore Hetzner personnel do not have any access to the software and data managed by Traxess.
- Deployment of the virtual server is done by container image, which is separately encrypted.

2. PHYSICAL SECURITY

- A video-monitored, high-security perimeter surrounds the entire data centre park. Entry is only possible via electronic access control terminals with a transponder key or admission card.
- All movements are recorded and documented. Ultramodern surveillance cameras provide 24/7 monitoring of all access routes, entrances, security door interlocking systems and server rooms.
- Due to the nature of server infrastructure, nobody has physical access to it.
- The uninterrupted power supply (USV) is ensured with a 15-minute backup battery capacity and emergency diesel generated power. All UPS systems have a redundant design.
- Direct free cooling allows the environmentally friendly cooling of hardware. Climate control is assured via a raised floor system.
- A modern fire detection system is directly connected to the fire alarm centre of the local fire department.

3. NETWORK SECURITY

- The WAF is deployed embedded within the webserver or as a proxy server in front of the web application. This allows the engine to scan incoming and outgoing HTTPS communications to the endpoint, enforcing OWASP, some PCI and DDoS rules.

- Multiple redundant connections to the largest German internet exchange point, DE-CIX, ensure smooth data transfer.
- All existing upstream and peering's are integrated in the backbone via state-of-the-art routers from Juniper Networks to boost the network's capacity.
- To safeguard servers, and IT infrastructure from DDoS attacks, Hetzner Online utilizes its automatic DDoS protection system.
- Each server is protected by Traxess with three-level firewalls.
- Automated security and safety check are in place.

4. SYSTEM SECURITY

- Security updates are continuously performed on the managed servers.
- There is a central back-up server to save backed-up data. The RAID-1 hard disk system reduces the likelihood of data loss.
- Other optional features provide the highest level of availability.
- Qualified experts are available 24/7 to provide individual support.
- The database and system-relevant files are encrypted using an RSA 4096-bit dynamic key.
- Access to web interface is possible only using the HTTPS protocol.
- Sensitive data are securely encrypted using the SHA-3 algorithm and stored in the dedicated environment. The environment is configured so that the system provides cryptographically secure access to the client's data. The environment for sensitive storage data has no access to the internet.
- Data retention in accordance with GDPR is applied to all systems elements. Anonymisation of data in accordance with data retention eliminates the possibility of tracing the original data.
- Access to the systems is protected by the SSL/TLS protocol for web access and various authentication methods in accordance with industry best practices.
- Double encryption methods are used for the connection to the database in accordance with PCI recommendations.
- Traceability of events and most critical user actions is assured by technical logs. The logs remain available upon agreement with the client.
- Cryptographic security measures are regularly audited according to industry best practices.
- The APIs to and from the system are secured with 2waySSL, oAuth2 etc.
- Penetration and security tests (OWASP, PCI, etc.) are performed four times a year. Test reports and remediation plans are shared with clients upon request.

5. DATA PROTECTION

- Traxess adheres to the EU's General Data Protection Regulation (GDPR), and transfers only the minimum amount of information necessarily saved and used exclusively for the contacted purposes.
- Traxess does not forward personal data to any third parties except it is explicitly agreed by the client and necessary, such as to provide assistance to clients in need in an emergency situation.
- Data is encoded using asymmetric cryptography algorithm.
- All data is being transferred exclusively via web transport. SSL TLS 1.2 encryption is implemented on the HTTPS protocol.
- All data transferred via web transport is using a publicly recognized CA. Public HTTPS certificates are generated by Traxess.
- Access to personal data is restricted based on access profiles and granted only by following a "Must Have" principle.

- A password policy (10 symbols at the minimum, at least one number, one uppercase letter and one special symbol) is enforced to assure strong passwords that must be updated at least every 6 months and a 2FA is available for admin roles to protect access of roles with access to sensitive data. Passwords are encrypted with SHA-3 algorithm.
- Personal data older than 6 months are encrypted on UI and removed from all storage media after one year. The data retention can be changed according to the customers preferences as agreed during the implementation phase. Processes for archiving and removal are fully automated.
- All Traxess employees sign confidentiality agreements and receive yearly training on data protection rights and regulations. External parties do not have access to personal data.
- The data processing agreement is signed as appendix of the contract between the parties according to GDPR requirements that specifies all measures in place according to the legal requirements.
- For any questions on data protection, please contact Traxess by sending an e-mail to info@traxess.ch.

6. DATA BACKUP AND RECOVERY PROCESS

- The back-up policy applies to the most critical components necessary for business continuity. The following systems are considered critical and are protected:
    - All data stored on file servers, mail servers, network servers, web servers, and database servers.
    - Domain controllers, firewalls, and remote access servers.
- The data backup and recovery are fully automated processes supported by own developed tool.
    - RPO (recovery point objective): 1 Hour
    - RTO (recovery time objective): 3 Hours
- Data are backed up daily, hourly for incoming files. Software back-up is updated upon new software versions are deployed.
- Roll-back of software functions and data are possible from back-up systems in case of an event.
- Test failures and recovery is simulated in a separate environment that is not accessible by clients.
- Consistency check is performed automatically after each restart.

7. SERVICE LEVEL AGREEMENT (SLA)

		Target value
1	**System Uptime** System is operational in percent per year. It includes downtime for maintenance.	99.7%
2	**System Accessibility** System is accessible by clients all over the world in percentage per year.	99.7%
3	**System Response Time** Average time to load the system depending on the content in the Browser when using 3G connection.	3 seconds
4	**First Response Time** Response time to critical issues like system down, system not accessible that impact core functions. Response time to any other requests with lower priority.	2 hours 8 hours
5	**Issue Resolution Time** Critical issues that limit use cases of the system.	8 hours

SLA Reporting Frequency: Reports are provided annually or upon request.