simplex Security Basics

contact xtendx:

support@xtendx.com

Table of Content

Security Levels

Datacenter & Hardware

The xtendx Cloud environment is built of the following suppliers:

1. Infrastructure Provider: **swissTXT**
2. Datacenter Operator: **Interxion**
   Interxion certification: **ISO-27001 & BSI ISO 22301**. Interxion manages its datacenters by FINMA-Standards and fulfills the strict requirements of the Swiss banking center.
3. Datacenter Supplier: **Equinix**
   Equinix certification: **ISO-27001, OHASAS-18001, ISO-9001**. The IBX® datacenters of Equinix are centrally located in Zürich.

Our above direct and indirect suppliers all maintain best practice industry standards for security control.

Additionally upon request, a global system of content distribution network nodes can be activated.

Virtual Machines & Operating System

Access rights on OS level are centrally managed and only available for specific xtendx DevOps personnel via personalized public key SSH VPN tunnel.

OS level hardening is a continual process at xtendx: Firewalls, Malware & Content Scanners are periodically updated.

Uptime related informations can be gathered from our xtendx SLA.

Application

Our shared cloud server fully satisfies Multi-Client capability (Mandantenfähig).

The different customers are separated and no possibility of data exchange between them exists.

A secure software development cycle in sprints with mandatory developer (i) and QA (ii) review steps for each activity allows technical and organizational platform security.

Network

The simplex network traffic is exclusively HTTPS end-to-encrypted. HTTP requests are being forced to HTTPS.

TLS v1.2 Certificate: 2048bit RSA Key with SHA-256 Signature Algorithm

Security Management

Communication Flow & Escalation

Xtendx follows a defined internal process upon incidents regarding information security & cyber security (external attacks, data loss, malware etc.) and proactively informs its customers.

The incident & escalation entrypoint is support@xtendx.com and our helpline. Further informations are defined in the xtendx SLA.

The IT Security responsibility lies with the xtendx CTO.

To provide the customer experience, xtendx relies on third party services like datacenter, CDN, Modules. In the event that xtendx decides to alter any third-party or supplier relation, our customers will be informed in a timely matter.

Contingency Management

See Backup Management. Our SLA covers contingency related requirements. However xtendx uses industry best practice approach and offers customer tailored solutions regarding availability & contingency requirements.

Data retention & Data deletion

Data storage is under the control of our customers. Upon request, the storage data can either be requested to be disabled or securely deleted.

Incident- & Problem Management

Xtendx uses state of the art application for incident & problem management using a configuration management database (CMDB) to maintain the relationships between different components configuration tracking.

Patch & Change Management

Xtendx employs a Security Patch Management und Change Management process that enables fast reaction times for critical releases.

The datacenter supplier owns relevant Business Processes by ITIL Standard.

Any Changes in Production with expected downtime will be announced to our customers according to our SLA.

Audits & Controlling

Each customer has the right to request & perform unhindered audits by involving trusted third parties. In 2017 two successful audits were requested and performed by different customers.

Xtendx tracks audit logs of every admin, customer & author user activity for a seamless backtracking of potential malicious activity or otherwise.

Penetration Tests & Load Tests

Periodically but at least once every year our infrastructure provider performs controls through desaster & emergency exercices, simulated attacks on both physical and technical level. Results can be presented upon request.

Backup Management

All Productive Cloud data (filestore & database) are daily & hourly respectively backed up onto a xtendx owned swiss local premise system and can be republished within hours in our desaster recovery scenario.

Portability & Interoperability

For operating the services (OS, Middleware & Applikationen) open and established application and data format standards are used so that customer data portability is ensured.

Specifically simplex is using **H.264, HLS & MPEG-DASH** video standards. We are continually evaluating and testing proposed future standards and will advance with the supported formats if and when they become beneficial to our customers.