# ZENNNN SECURITY

*Last updated: March 20, 2020*

Your security is very important to us! Here is a summary of what we do every day to guarantee that your data is safe with ZENNNN and that we apply best security practices on our hosted version, the ZENNNN Cloud.

## ZENNNN Cloud

### Backups / Disaster Recovery

- We keep 14 full backups of each ZENNNN database for up to 3 months: 1/day for 7 days, 1/week for 4 weeks, 1/month for 3 months;
- Backups are replicated in at least 3 different data centers on different continents;
- The actual locations of our data centers are specified in our Privacy Policy;
- You can also download manual backups of your live data at any time using the control panel;
- You can contact our Helpdesk to restore any of those backups on your live database (or on the side);
- Disaster recovery: in case of complete disaster, with a data center entirely down for an extended period, preventing the failover to our local hot-standby (never happened so far, this is the worst-case plan), we have the following objectives:

  1. RPO (Recovery Point Objective) = 24h. This means you can lose max 24h of work if the data cannot be recovered and we need to restore your latest daily backup.

  2. RTO (Recovery Time Objective) = 24h for paid subscriptions, 48h for free trials, education offer, freemium users, etc. This is the time to restore the service in a different data center if a disaster occurs and a datacenter is completely down.

  3. How is this accomplished: we actively monitor our daily backups, and they are replicated in multiples locations on different continents. We have automated provisioning to deploy our services in a new hosting location. Restoring the data based on our backups of the previous day can then be done in a few hours (for the largest clusters), with priority on the paid subscriptions.
  We routinely use both the daily backups and provisioning scripts for daily operations, so both parts of the disaster recovery procedure are tested all the time.

### Database Security

- Customer data is stored in a dedicated database — no sharing of data between clients;
- Data access control rules implement complete isolation between customer databases running on the same cluster, no access is possible from one database to another.

### Password Security

- Customer passwords are protected with industry-standard PBKDF2+SHA512 encryption (salted + stretched for thousands of rounds);
- ZENNNN Team does not have access to your password, and cannot retrieve it for you, the only option if you lose it is to reset it;
- Login credentials are always transmitted securely over HTTPS;
- Customer database administrators even have the option to configure the rate limiting and cooldown duration for repeated login attempts;
- Password policies: database administrators have a built-in setting for enforcing a minimum user password length.

### Staff Access

ZENNNN Team cannot sign into your account, It's impossible!

### System Security

- All ZENNNN Cloud servers are running hardened Linux distributions with up-to-date security patches;
- Installations are ad-hoc and minimal to limit the number of services that could contain vulnerabilities (no PHP/MySQL stack for example)
- Only a few trusted ZENNNN engineers have clearance to remotely manage the servers — and access is only possible using an encrypted personal SSH keypair, from a computer with full-disk encryption.

### Physical Security

ZENNNN Cloud servers are hosted in trusted data centers in various regions of the world (e.g. AWS, Google Cloud), and they must all exceed our physical security criterions:

- Restricted perimeter, physically accessed by authorized data center employees only;
- Physical access control with security badges or biometrical security;
- Security cameras monitoring the data center locations 24/7;
- Security personnel on site 24/7.

### Credit Card Safety

- We never store credit card information on our own systems.

- Your credit card information is always transmitted securely directly between you and our PCI-Compliant payment acquirers.

### Communications

- All web connections to client instances are protected with state-of-the-art 256-bit SSL encryption;
- Our servers are kept under a strict security watch, and always patched against the latest SSL vulnerabilities, enjoying Grade A SSL ratings at all times;
- All our SSL certificates use robust 2048-bit modulus with full SHA-2 certificates chains.

### Network defense

- All data center providers used by ZENNNN Cloud have very large network capacities, and have designed their infrastructure to withstand the largest Distributed Denial of Service (DDoS) attacks. Their automatic and manual mitigation systems can detect and divert attack traffic at the edge of their multi-continental networks, before it gets the chance to disrupt service availability;
- Firewalls and intrusion prevention systems on ZENNNN Cloud servers help detect and block threats such as brute-force password attacks;
- Customer database administrators even have the option to configure the rate limiting and cooldown duration for repeated login attempts.

## ZENNNN System

### Software Security

ZENNNN is open source, so the whole codebase is continuously under examination by ZENNNN users and contributors worldwide. Community bug reports are therefore one important source of feedback regarding security. We encourage developers to audit the code and report security issues. ZENNNN Team processes have code review steps that include security aspects, for new and contributed pieces of code.

### Secure by design

ZENNNN is designed in a way that prevents introducing most common security vulnerabilities:

- SQL injections are prevented by the use of a higher-level API that does not require manual SQL queries;
- XSS attacks are prevented by the use of a high-level templating system that automatically escapes injected data;
- The framework prevents RPC access to private methods, making it harder to introduce exploitable vulnerabilities.

## Independent Security Audits

ZENNNN is regularly audited by independent companies that are hired by our customers and prospects to perform audits and penetration tests. The ZENNNN Team receives the results and takes appropriate corrective measures whenever it is necessary.
We can't however disclose any of those results, because they are confidential and belong to the commissioners.
ZENNNN also has a very active community of independent security researchers, who continuously monitor the source code and work with us to improve and harden the security of ZENNNN. Our Security Program is described on our Responsible Disclosure page.

## Reporting Security Vulnerabilities

If you need to report a security vulnerability, please head over to our Responsible disclosure page. These reports are treated with high priority, the problem is immediately assessed and solved by ZENNNN Team, in collaboration with the reporter, and then disclosed in a responsible manner to ZENNNN's customer and users.