IT Security Policy

Date: May 23, 2018

We are committed to keeping our customer's data protected at all time. We take security and privacy seriously, adhering to enterprise-level security standards.

Product Development & Application Security

We have a strict agile development process that contains a structural flow:

- a best-practise branching model
- core-review process - all code is reviewed to enhance quality and security
- several testing methods and on separate environments
- we make use of Continuous Integration and Deployment
- we use rolling release strategy (Canary deployments) to avoid downtime and higher stability

Password and Encryption

We do encrypt sensitive data and hash all passwords (not irreversible).

Permissions and Levels

We do support level based roles. Customers can define users to what they have access to.

Access to customer data is limited to authorized employees who require it for their job.

Infrastructure Security

Data Hosting and Storage

All our services are hosted in Amazon Web Services (AWS) facilities (eu-central) in Germany.

We do not use cloud-based services for our internal infrastructure that supports our application development, testing or deployment.

Virtual Private Cloud & Network Security

All of our services are within our own virtual private clouds (VPC) with network access control lists (ACLs) that prevent unauthorized access. By default, we block all traffic at the network level and only allow specific ports that are required to deliver our services. Any escalated access to our infrastructures requires VPN connection combined with 2FA.

eSmiley supports HTTPS, which allows customers to use a secure channel for communication (default).

Inventory and Configuration

All our infrastructure is configured using orchestration tools (OpsWorks and Rancher). This allows us to scale and bootstrap new application servers and containers automatically and with ease.

Monitoring & Logs

We do extensive monitoring of both our infrastructure and application performance using several systems, such as Sysdig and Pingdom. All alerting is sent to our internal communication systems as well as e-mail and SMS. We do log all usage of our applications. All logs are pseudonymized and stripped for any sensitive or personal data. We use our logs to detect abnormalities, misbehaviours and being able to debug our services.

Backup

Server Backup

Due to the nature of our infrastructure architecture, we do not need backup of servers as we have "cattle/dumb" application servers that are bootstrapped automatically with our application and settings.

Database Backup

We have implemented multiple backup mechanisms, which are:

- point-in-time recovery (using AWS RDS)
- full database file-dumps on a daily basis

We do have a daily automated routine of loading yesterdays backup, which allows us to have a hot-standby setup with data integrity kept in place.

File Backup

All user content is stored en secure AWS S3 buckets (contains backup). We do snapshot all our S3 Buckets nightly as off-site backup.

Failover & Disaster Recovery

All our infrastructure is built with redundancy in mind. Our services are multi-region tolerant (using AWS), and we balance our load between our regions.

We do run a separate "cold" site setup, with delayed data loading process. This allows us to even have a failover at application failures and in case of complete unavailability (eg. AWS regions are completely unavailable).

Uptime

We do monitor our uptime - which is near ~99.99%.

Additional Security

Employees

All employees complete a Security and Awareness training, which is renewed annually, eSmiley does as well:

- perform a background check on all new employees in accordance with local laws.
- all employee contracts include a confidentiality agreement