Security Policy

Last Updated: 31/03/2021

Prelude

Our mission is to create software technologies to support industrial players in growing their additive manufacturing.
The way to get there is standardizing and optimizing information, it is at the heart of all our businesses and lives. This is why customer trust and data security is at the center of what we do. We strive to be transparent about our security program so you can feel informed and safe using our products and services.
We don't look at security as a destination to reach — it's an ongoing journey. We continually strive to improve our software development and internal operational processes with the aim of constantly increasing the security of our software and services.

Read more about our approach to security and learn about how customers can play a part in developing secure production solutions.

Our security and risk management objectives

We have developed our security framework using best practices in the SaaS industry. Our key objectives include:

Customer Trust and Protection – consistently deliver superior product and service to our customers while protecting the privacy and confidentiality of their information
Availability and Continuity of Service – ensure ongoing availability of the service and data to all authorized individuals and proactively minimize security risks threatening service continuity
Information and Service Integrity – ensure that customer information is never corrupted or altered inappropriately

This document consists of 3 sections:

Software Security / Product Security

In this section, you will find our measures to make and maintain our Product's Security and Reliability at the highest levels. This section is the most relevant for **on-premises installations.**

Infrastructure and Cloud Security (Operational Practices)

In this section, you will find everything that we do to make our **cloud installations** secure and reliable. If the software will be installed on on-premise servers, the topics in this section are not directly applicable - however, they can serve as guidance.

Office Security Practices

In this section, you will find everything that we do to make our daily work and routines secure. This section is relevant if you trust us with handling sensitive data and is therefore also most relevant for **cloud installations.**

Table of Contents

Software Security / Product Security

In this section, you will find everything that we do to make our Products Secure and Reliable. This section concerns ***on-premises installations.***

Security of Code Repository

The security of 3YOURMIND's code structure is a fundamental building block of our overall software security. We ensure code repository communication security through TLS encryption and identify any user connection by username/password and SSH keys. Code repository access is fully limited to 3YOURMIND developers and we use **GitLabs** "Merge Requests" to track any code changes.

Security Updates and Dependencies

The effort to provide high standards of security needs to be coordinated with constant product updates. Also, since dependencies are a major source of vulnerability of applications, we perform systematic and automatic dependency checking of our code using **trivy**. This allows us to identify when to update away from software packages with critical vulnerabilities.

Safe Coding

We follow strict rules to ensure safe coding processes. We use multi-layered static analysis tools (Bandit, SonarQube) for coding and every code created goes through a systematic internal peer review process. From a procedural point of view, every developer is given guidelines to mitigate common intrusion vectors. As for our tools security, our backends are built on stable and best in class frameworks like Django and Spring. Those frameworks lower the risk of introducing security risks accidentally (e.g.SQL injections). And to reduce the risk of XSS vulnerabilities, our frontends are built with Vue.js.
We also track and review any code change and use CI servers to test all changes both automatically and manually. Every change is documented in release notes.

Cryptography and Encryption

All data sent between the application and users are encrypted in transit and at rest. We use a wide range of peer-reviewed encryption methods, in compliance with our clients' specific security protocols. Also, we use unique encryption keys and passwords per server. Application and infrastructure secrets are stored in a dedicated secret management solution, where they can be accessed from the application based on per-customer roles.

Authentication and Authorization

3YOURMIND's platform enforces a uniform password policy and only authenticated profiles can access our resources. For password and token-based authentication, we rely on methods provided by Django REST Framework.
We use layered platform authorizations to allow specific roles to access specific product resources (E.g. admin, Service, Manager, User etc.).

Product Vulnerability Management

We use a structured and systematic approach to designing quality applications. We enforce a continuous improvement code review system and developed a "Security Board" process for handling and tracking vulnerabilities when discovered. We allow all our developers to take part in this Security Board and facilitate a culture of responsibility and cooperation on security topics.

User input validation

Since User input can not be trusted we have multiple validation levels in place:

1. **Automatic validations provided by Backend Frameworks**
   The Django Rest Framework comes with a set of default validation methods which protect from both processing the wrong data type and also shield against SQL Injections and Cross Site Vulnerabilities
2. **Permission Checks**
   Every time a user calls an endpoint, it is checked first, if the user has the right permission to do so. Mostly the Django Rest Framework Permission System is used for that.
3. **Custom Business Logic Validation**
   On top of the automatic validation checks, we added a logic to the validation in the backend. Especially during order creation, we deeply check for the validity of the inserted data. For example, we check if the total

price that the user sees in the frontend while ordering is indeed the price to be charged.

4. **Frontend validation**
   For a smooth user experience, most data is additionally validated directly in the frontend to give users an immediate feedback.

Product Testing

Product testing is performed by both internal and external sources.

Internally: we regularly and automatically test our product functionalities with Unit-, Integration and End To End Tests. We also occasionally implement internal Bug Bounties programs.
Regarding external testing: when a vulnerability is identified by users, we promptly respond to it. We are also available for any specific client audit program.

Availability and Reliability

Platform Availability and Reliability highly depends on local infrastructure and server setup. Therefore, our software is designed to run on stateless servers to enable the installation into a highly available environment (See Availability and Reliability in the next section).

External Penetration Tests

3YOURMIND pays external companies to perform penetration tests to the application. It is ensured that there is at least one test per week running.

Chain of Trust

The Platform depends on various (Open Source) Packages and Base Images that are included in the deployable artifacts. Those packages originate from trusted community resources like https://hub.docker.com/, https://pypi.org/ and https://www.npmjs.com/.

3YOURMIND has high standards when choosing the best supported and secure packages. We believe that using the original community sources results in the highest possible security since new Security fixes are published there first.

While building the artifacts, we download dependencies with https from the sources. Our CVE scanner, Trivy, scans all dependencies for known vulnerabilities.

Infrastructure and Cloud Security (Operational Practices)

*This section concerns mainly our policies to maintain secure and reliable **cloud installations**. This section can still serve as guidelines for on-premises installations. In addition to cloud installation, our application architecture and our operational model allows us to store our software on customer dedicated cloud servers.*

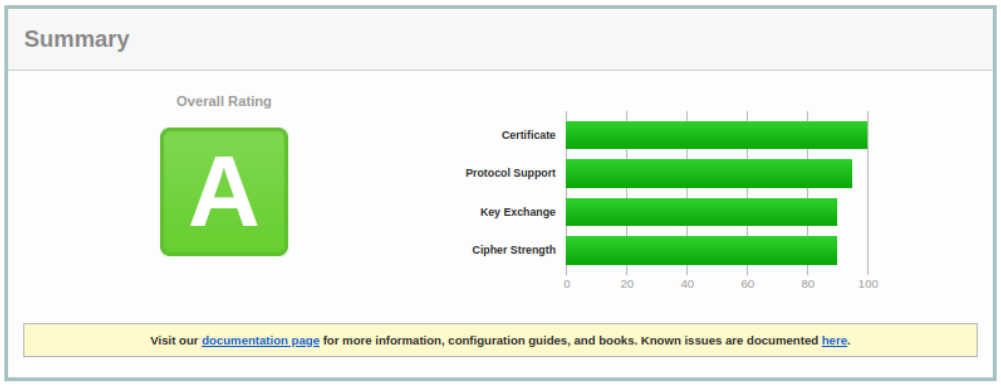
Encryption of Stored Data

Our platform's data are stored and encrypted at Amazon's data centers. We rely on trustworthy physical controls and management at AWS, as well as transit-level encryption to protect customer data. The encryption used by Amazon is one of the strongest block ciphers available in the market: 256-bit Advanced Encryption Standard (AES-256).

Data	**Storage System**	**Encryption**
User Uploaded 3D Files	AWS S3	SSE-S3
User Uploaded Attachments + Images	AWS S3	SSE-S3
Other Data (Users, Passwords, Orders, Configuration)	AWS RDS	AES-256

Encryption of Transferred Data to End Users

Non-encrypted data transfer represents a high-security risk. That is the reason why we encrypt transferred data by default by using SSL secured connections to end-users. For verifying our SSL configuration, we are using https://www.ssllabs.com, which gives us an A-level grading for all our connections to end users.



(https://www.ssllabs.com/ssltest/analyze.html?d=demo.3yourmind.com&latest)

Internal Encryption of Transferred Data

External (customer) data transfer is not the only risk for data security. Our own internal operations must follow high standards of encryption. To do so, we use a panel of several encryption methods:

- Employee -> AWS EC2 SSH, VPN
- Employee -> Admin Configuration SSL
- Employee -> AWS RDS VPN, SSH, SSL
- AWS EC2 -> AWS S3 SSL
- AWS EC2 -> AWS RDS SSL

Intrusion Prevention (Firewall)

We control access to our sensitive production networks through the use of strict firewall rules. In addition, we apply the principle of least privilege for all our inbound firewall rules as well as all files on our servers. Also, our backend servers are protected in non-public subnets.

Infrastructure as Code

Security is a primary focus when designing our applications, networks, and business processes. Our whole cloud infrastructure is described as a code (we use Terraform and Ansible in Combination with Docker). We apply modern IaC practices to ensure more robust, secure, readable, reliable, revertible, transparent, testable and configurable Infrastructure. We also allow smoke-testing for new parts of the infrastructure.

Availability and Reliability

As the continuity of your operating model matters to us at the highest level, we are committed to providing you with a maximum accessibility to your data and processes, at any time. To ensure availability in case of load increase, all our Servers are operating behind a Load Balancer. In addition to that, we use New Relic for Availability Monitoring and our databases are multi-availability zone deployments, ensuring high-availability requirements and to reduce the risk of an unplanned outage
As for new deployments, we test all database migrations prior to it and use blue-green deployment (zero-downtime deployment) to roll-out new versions of our system. As for data Availability and Reliability (3D Files, Attachments, Metadata), we trust in the competency and industry validated AWS S3 and AWS RDS.

Monitoring and Logging

We use a self-hosted version of Sentry, Prometheus, Loki and Grafana to monitor and investigate bugs in the production environment.

Key Management and Rotation

Due care is given to managing encryption keys within 3YOURMIND. Our credential cannot be accessed on volition by our teams, and we rotate credentials regularly. Secret management is also enforced internally with strong cryptographic methods on a minimum amount of critical credentials.

Data Loss Prevention

Our data loss prevention policy is designed to keep track of all your operations data in cases of unpredicted shut downs. We create automatic backups across all our storage backends:

- AWS S3 uses redundancy and stores the data multiple times to prevent data loss (See AWS S3 FAQ)
- RDS databases create snapshots once per day
- Infrastructure as code increases software reliability

We automatically create a “last snapshot” prior to shutting down any service. We also systematically obfuscate sensitive data prior to granting access to our developers.

Access to Customer Data for Developer and Support

The access to production system is strongly regulated within our organization. Only a fixed number of employees (DevOps + Support) have the possibility to access customer data. These employees are selected thoroughly and operate under bilateral customer non-disclosure agreements. Customer data is only to be accessed in specific situations such as bug inspection or upon customer request.

Office Security Practices

Systems security are also highly tied to flawless daily office security practices.

Responsibility for Security

We acknowledge that there is always a margin for error in applications, processes and infrastructures. Security is an everyday endeavour that not only relies on technology but also on people. As security is a central driver of our company culture we strive to hire the best engineers to conduct these critical guidelines. In 3YOURMIND, a team of expert engineers are dedicated to all security related topics and all our developers are sensitized to security issues from initial training to regular internal information campaigns.

Employee Trainings

Regularly, all our employees receive Security Awareness Trainings, regardless of their function. These trainings concern secure development, architecture and behaviour principles. We believe in a culture of transparency and collaboration on security topics and promote any individual initiatives toward increasing our security culture.

Hiring and Employee Onboarding

Just like any top tier tech company, we want to attract and hire the best engineers. We perform systematic and in-depth technical assessments with our applicants and have them go through advanced, use-case based, test days in our office. This recruiting process allows us to back our hiring ambition and decision making with accurate sets of evaluation.

Security Policy for Computers (and all digital devices)

We strive to keep our employees devices updated and safe. Indeed, all Windows/MacOS machines enable automatic updates and we provide detailed devices security guidelines to our employees:

- No device is left without locking the screen
- All employees are instructed to use strong login passwords
- All employees are instructed to not install untrusted software

Safe Use of Smartphone

We are aware that along with increasing mobility, smartphones provide additional security risks. This is the reason why no employee can access sensitive operational secrets or data that is stored on our cloud servers on their smartphones

Protection of Office Space

Our office space is secured by certified security professionals, office doors are systematically locked with digital systems and confidential documents are removed from desks and stored securely after using. Guests are systematically accompanied by one of our employees.

WIFI

Office WIFI keys rotate regularly, and we grant a Guest WIFI with a strong, rotating password.

Password Management

We mitigate the risk of leaked credential reuse or password guessing by malicious parties with strict password policies. We generate strong and hardly memorable passwords and all our employees are using password safe applications to manage their credentials. In addition, we use Vault for the most sensitive operational secrets - like passwords for databases and servers - this allows us to easily rotate passwords on incidents and cases of employee leave.

Multi-factor Authentication

We enforce multi-factor authentication for both our primary business (email, data) and operational accounts (AWS).