Security Report

V1.0

10.06.2021

1. Our Company

Safee is a leading provider of GPS vehicle tracking services, fleet management, and assets management solutions. Since its founding, Safee has been on the main mission of empowering the communities with the best and most user-friendly fleet management web application. Today, thousands of businesses and non-profit organizations in 25+ countries use our cloud-based vehicle tracking and fleet management services.

Safee is introduced to the customers as a SaaS Software-as-a-Service solution. Customers can easily access the web application of Safee via the internet browser. Safee users can benefit from the advanced features such as:

- Comprehensive real-time monitoring and controlling dashboards.
- Powerful filtering and customizable listing.
- Instant alarming system for more effective fleet management operations.
- Dynamic reports capabilities to reduce reporting time to the minimum.
- The most reliable fuel consumption management and weight tracking tools.

Safee also offers its powerful application programming interface API for development and business integration purposes.

2. Security and Risk Governance at Safee

Our top priority is to protect the data of our customers and the privacy of the platform users. We have big investments in the most suitable data protection resources and we implement the most advanced security measures and controls to ensure that we are always able to serve our customers and protect their data without any interruption.

At Safee, we established highly skilled application security and operational security teams with the main responsibility of developing and managing the entire security and risk governance program, across the whole company hierarchy and its products and services infrastructures.

3. Objectives

To develop our security framework, we have applied the best web application security practices in the cloud services industry.

The main objectives of the development process are:

- **Service and data integrity.** protect customer data from any corruption or alteration.
- **Business continuity and service availability.** defend and protect our systems against all security threats that could cause data loss or service interruption.
- **Business trust and data protection.** deliver high-quality services ensuring that the data privacy and confidentiality of the customers are protected.
- **Standardization and data law compliance.** design and develop our security and risk management procedures and controls to meet exactly the data protection regulations and practices of the cloud security industry. Our security program complies with the GDPR General Data Protection Regulation of the European Union and leverages the standards ISO 27001 and NIST SP 800-53, it also aligns with standards like COBIT and CCM.

4. Safee Security Controls

Here is a subset of security controls Safee has implemented to secure customers' data and business operations and to reduce the risk to the minimum across the entire company.

4.1. Service Infrastructure

4.1.1. Data Center Security

Basically, Safee does not host its data management services on servers located in the company headquarter or any of its offices. The hosting of our data management web application is outsourced, Safee leverages the two leading cloud infrastructure providers Microsoft Azure and Google Cloud Platform for product hosting.

Microsoft Azure and Google Cloud Platform provide high levels of operational, physical, and network security. Our cloud infrastructure providers' data centers which we use to host our cloud services and to store our customers' data are located both in the European Union and in the United States.

Both Microsoft and Google datacenters have their own robust security programs that comply with SOC 2 and ISO 27001 standards.

Our cloud infrastructure providers have the most sophisticated infrastructure capabilities from power supply grids, data networking, and operational and physical security:

- Service uptime is above 99.95%.
- Minimum redundancy of N+1 to the power grid, data network, and HVAC services.
- Highly restricted access to the sites for both physical and electronic access.
- SOC 2 Type II and ISO 27001 certified business continuity and recovery plans.

Certificates are available on the Microsoft Azure and Google Cloud Platform compliance and security website pages.

4.1.2. Network Security

Safee applies a set of the most advanced network security protections designed specifically to prevent unauthorized access to the product internet network and within the intranet network of the service infrastructure. Safee protection controls apply corporation-level routing, firewalling, and traffic logging and monitoring.

4.1.3. Configuration Management

Our process of scaling the product infrastructure and service operations to meet the changing needs of the customers is completely automated. Servers' configurations are embedded in images and puppet files. Configuration management is accomplished by these images and scripts when the server is built. Configuration and image changes are managed via strictly controlled changing management processes. The patching management process is handled by replacing server instances that are no longer compliant with the provisioned and fully compliant new instances.

4.1.4. Alerting and Monitoring

Safee made big investments in establishing a fully automated alerting and monitoring system and developed high-tech response procedures in order to address all the potential risks earlier and solve the problems as fast as possible.

The strong product infrastructure of Safee fleet management system was built to trigger alarms to the specialized security team when any problem occurs, such as:

- Failure Rates Increasing.

- Unexpected or Malicious Activities.
- Misuse Scenarios.
- Application Cybersecurity Attacks.

The security team is responsible for investigating the situation, developing the right solution and correcting the issue instantly and in real-time.

Safee system is able to protect itself against undesirable situations by leveraging a number of powerful automated protection techniques:

- Real-time Logging and Monitoring.
- Pre-defined Thresholds.
- Instant Traffic Blocking.
- Quarantining.
- Immediate Process Termination.

One of our system's strongest points is the ability to log and monitor every single activity at the application layer and at the infrastructure backend layer. The events monitoring system is linked with an immediate response system that alerts security professionals in real-time to develop the right actions.

4.1.5. Infrastructure Access

Safee protects its product infrastructure against potential security threats by applying a well-designed and strictly controlled access model. Employees are granted access to the services based on their jobs using a role-based access control model. There are more details about applying the RBAC model across Safee company in a following section.

Some of Safee infrastructure access control techniques:

- Access is reduced to the minimum according to the needs of the employee's job.
- JITA model Just-In-Time Access for emergency and administrative access requests.
- All JITA requests are logged and monitored to track abnormal requests.
- Forbid direct network access to the production environment via SSH.
- Authentication is required from employees to access the quality assurance and production environments.
- Unique tokens and two-factor authentications for server-level access requests.

4.2. Application Protection

4.2.1. Web Application Defenses

To protect our customer data, Web Application Firewall WAF aligned exactly to the best security practices documented by the OWASP Open Web Application Security Project has been implemented at Safee.

To ensure business continuity, we have incorporated industry-recommended protection rules against Distributed Denial of Service (DDoS) attacks. Web Application Firewall and DDoS protections combined work together to protect all the services hosted and accessed via the internet browser through https://tracking.safee.xyz and business integrations with Safee API at https://tracking.safee.xyz/api and of course, all customer data stored in our data centers are also automatically protected by well-configured detection and blocking rules against all types and rates of malicious traffic.

4.2.2. Development and Update Management

At Safee, advancing and evolving are basic elements of our work environment. There are always new features to be added to the platform to serve the changing needs of our customers and to solve their future problems. Additionally, the main platform takes the advantage of continuous updating on a regular basis.

Our software development continuous-delivery approach includes the following steps:

1. New features' codes are proposed.
2. Highly specialized teams of developers to perform programming reviews and software quality assurance tasks.
3. Compilation, packaging, and unit testing implemented after the submission of the approved codes to the integration environment.
4. Archives of the current production-level codes are made.
5. The new code is deployed across the application layer.
6. Post-deploying step includes continuous monitoring of the status and performance of the application.
7. In case of any failure, a historical image of the previous production-level codes is ready to be engaged immediately.
8. All the information about the newly added features is documented and provided in the news update posts on the product's website and wiki pages.

The quality assurance environment and production environment are two separated entities and there is no interference at any level. Robust network firewalling blocks any unauthorized and undesirable access between the two environments. At Safee, our customers' data are never used in the QA environment.

4.2.3. Vulnerability Scanning

Our security team implements a comprehensive coverage vulnerability scanning over all the layers of our product infrastructure leveraging the most advanced industry-recommended tools and scanning approaches.

Our main scanning approach includes:

- Vulnerability scanning on a regular basis.
- Over the internal networks, application infrastructure, and corporate infrastructure.
- Early detection of any potential security vulnerabilities via a comprehensive analysis of the coding activities in the development stages.
- Continuous update of the vulnerabilities' signatures lists.

4.2.4. Penetration Testing

In order to identify security flaws that might expose potential risks to our operations and to address any issue quickly, Safee employs the most recognized third parties in the web application security industry to perform 4 penetration tests a year.

To expand the type vectors of the potential security risks that should be assessed, the application layer, network layer, and corporate infrastructure are all targets of our annual penetration tests.

4.2.5. Bug Bounty Program

Besides our own internal vulnerability scanning efforts and independent penetration testing, we run a bug bounty program on a regular basis to give an opportunity for the independent researchers and security experts to provide us with reports about the vulnerabilities they see in our services. So, we can address any emerging issue earlier and be able to provide our customers with the best and most secure experience ever.

4.3. Customer Data Protection

4.3.1. In-Transit and At-Rest Encryption

All our customers' data are protected in transit and at rest. In transit, all the services are introduced and can be accessed via TLS/256 Bit SSL connections, as the same protection level of banking, electronic commerce, and financial services. At rest, we employ RSA 2048 to secure the information and encrypt the submitted data. All accounts' passwords are hashed and login pages are secured with brute force protections.

4.3.2. Login Protections

Safee users can log in to their accounts on the platform via a built-in login page. The uniform password policy enforced by Safee built-in login ensures secure operating by the following rules:

- Requiring a minimum of 8 characters password.
- Combination of lower- and upper-case letters.
- Embedding of special characters, and numbers.
- Users cannot change the default password policy.
- Users are encouraged to activate the two-factor authentication option for their accounts on our platform.

4.3.3. Employee Access

Safee strictly controls its individual staff member access to data in the production environment and at the corporate infrastructure level.

Access permissions to production data are granted to a set of Safee's employees based on their role in the company on an RBAC Role-Based Access Controls basis or on a JITA Just In Time Access basis.

Some of the common access needs:

- Alert response.
- Troubleshooting.
- Product investment decisions data analysis.
- Product support requests.

Sophisticated user authentication and authorization rules govern the network access permissions to the product infrastructure.

Customer support staff members should only request time-limited access to customer portals on a JITA basis, and their requests have to be limited to their work responsibilities associated with supporting and servicing our customers.

All the access requests and related activities are logged and monitored in real-time and are subject to an automated review on a daily basis.

4.4. Privacy

At Safee, our top consideration is the privacy of our customers’ data. According to our Privacy Policy on the website, we never sell your Personal Data to any third parties.

Safee has implemented all the needed protections that are documented in this report and more other protections, just to keep your data safe, private, and unaltered.

All the security practices that our privacy program incorporated meet exactly the regulatory requirements and comply with data protection regulations in the US and EU.

Our data retention policy:

- The data of the customer is stored as long as the customer stays active.
- The platform provides the necessary deleting tools to our active customers when they want to remove their data permanently.
- The data of the customer is removed permanently from our databases after a formal written request from the customer or after a specific period following the ending of the agreements between the customer and Safee.

More detailed information about our Privacy Policy and Customer Data Processing Agreement can be found on our website.

4.5. Business Continuity and Disaster Recovery

Our business continuity and disaster recovery plans have been built depending on the following basic rules:

- Redundancy over the networking layer, production layer, and corporation infrastructure to prevent any potential outages.
- Fast recovery in case of any service unavailability or performance degradation.
- Quick addressing and isolating of the occurred issues.
- Publishing updates about the identified issues and the status of the solving process.

At Safee, we check our business continuity strategies and recovery procedures on a daily basis and that makes us always ready for whatever issue might occur.

Basically, our strategy relies on:

- Infrastructure full redundancy.
- Real-time replication.
- Regular backups.

Additionally, our server infrastructure providers apply a minimum of n+1 redundancy within their facilities which are strategically distributed across multiple zones.

4.6. Safee Corporate Security

4.6.1. Employee Authentication and Authorization

Our corporate password policy meets the best standards in the information security industry.

Some of the enforced rules across the entire company:

- Changing passwords every 3 months.
- Minimum employee’s password length of 12 characters.
- Passwords should include upper- and lower-case characters, special characters, and numbers.
- Password sharing is prohibited.
- Employees’ authentication using SSH keys.
- Multi-factor authentication to access product infrastructure.
- All authentication and authorization procedures are automated.
- Access requests are logged and monitored.
- Regular scan of the entire system to ensure that permissions granted are still valid.

4.6.2. Background Check

All our employees undergo wide and detailed pre-employment background checks that commensurate with the national regulations and industry standards.

The background check basically includes:

- Previous employment.
- Education.
- Criminal record.

Our employees have to comply with non-disclosure agreements before they can start their job and be involved in corporate and production environments.

4.6.3. Physical Security

Some of our offices' protection techniques that are implemented across the whole corporation:

- Video surveillance.
- Special security staff members.
- RFID tokens to control location access.

4.6.4. Vendor Management

Safee maintains a strictly designed vendor management system with the main goal of ensuring that all necessary security controls are taken seriously by our vendors and are implemented appropriately at their services infrastructures.

Complete tracking and reviewing of the security programs of our vendors are achieved on a regular basis.

As part of contract management, unique considerations are coordinated between our security business integration team and the vendors to manage compliance with the future regulations and data protection laws.

4.6.5. Security Awareness and Training

Safee has a well-designed information security training program which covers:

- Data handling requirements.
- Privacy considerations.
- Response policy to violations.

We organize security training programs to ensure all the employees are ready, well-educated and well-equipped for their jobs at our company. Special security awareness and developer-specific training camps are dedicated to our teams of system engineers and software developers.

5. Compliance

Safee is completely compliant with the requirements of the GDPR General Data Protection Regulation of the European Union. The platform also contains all the necessary tools and features that enable our customers to maintain their GDPR and EU-US Privacy Shield compliance requirements. Safee services are hosted with Microsoft Azure Cloud and Google Cloud Services which are both SOC 2 Type II and ISO 27001 certified and GDPR compliant world-class cloud infrastructure service providers.