Frontify

Frontify security controls

security@frontify.com

Table of contents

Introduction

Frontify's security mission is aligned with the company vision: to create a home where all brands are safe. That's why, since day one, IT and information security have been included in every aspect of our system development, internal operations, and data handling. Only by involving all employees, finding the right experts in their fields, and ensuring full transparency for our stakeholders are we able to achieve the highest levels of security.

This whitepaper aims to offer our customers a clear and understandable overview of the security controls that we have implemented and that define our culture of security excellence.

1.1 Who we are and what we do

Frontify is a B2B SaaS company headquartered in St. Gallen (Switzerland), with an additional office in New York City (USA). Founded in 2013, we've gone from zero to more than 4000 customers worldwide and hired over 300 employees, allowing us to become the market leader in the brand management industry. We envision a world where every strong brand will be managed with Frontify.

We aim to create the best and most user-friendly all-in-one brand management platform that provides a home for all brands to thrive. It's our goal to ensure cloud-based efficiency for businesses that collaborate across different teams, borders, and languages to create a wide range of personalized brand content. As a brand management platform for enterprises and an intermediary between companies and external stakeholders, we improve collaboration, increase communication, and simplify client handover. Frontify acts as a single source of truth for brand-related content and the people behind the brands. It's a home where all brands can be their best selves.

1.2 Security excellence at Frontify

This whitepaper outlines the four core pillars that define security excellence at Frontify.

Culture of security: Frontify guarantees ongoing compliance with industry-known security standards, such as ISO 27001, which is facilitated by the close collaboration between our dedicated Information Security Team and all departments in our company.

Cloud infrastructure: Our services and operations rely on the most secure cloud infrastructure. With strict data center security and multiple layers of preventive and detective controls, we're able to offer a secure environment to all our customers.

Identity management: Our customers' Frontify accounts are protected by strong authentication and authorization concepts. Additionally, our platform uses a centralized logging system that facilitates 24/7 monitoring, reporting, and traceability.

Quality assurance: Frontify's quality assurance plan covers strict internal access controls, vulnerability and risk management programs, monitoring and auditing, security-focused development, and change management processes.

The culture of security at Frontify

To earn and maintain our customers' trust, we have implemented the Frontify Information Security Management System (FISMS) in accordance with the internationally recognized data protection best practices outlined by the ISO 27001 standard, for which we have been officially certified since 2021.

Frontify's dedicated Information Security Team works closely with all departments in our company. This collaboration — together with continuous investments in improving and expanding security controls and technical and organizational measures — ensures the highest protection for our customer data. By embedding security in every aspect of our operations, we can provide our customers with a safe and secure environment for their brands.

To ensure that the entire organization respects our high security standards, we regularly conduct mandatory training sessions for all our employees. We instruct all staff members on their roles and responsibilities and raise their awareness throughout their entire time at Frontify. All our employees recognize our security efforts by signing an official statement of acceptance. With these measures, we ensure full compliance from all employees with our security policies and guidelines, as outlined by the ISO 27001 certification process.

2.1 Frontify's certifications

Our efforts to establish security excellence across our entire organization have been officially recognized and certified against industry-known standards.

ISO 27001

ISO 27001 was established by the International Organization for Standardization (ISO). The well-known standard gives companies guiding principles for establishing, implementing, maintaining, and continually improving an information security management system (ISMS).

Frontify has been officially ISO 27001 certified since 2021. The scope of the FISMS covers all essential assets, processes, and services connected to the Frontify application and the company's business operations, irrespective of where the process or service is carried out. We perform annual internal and external audits in line with the ISO 27001 certification.

Cyber Essentials

Cyber Essentials is a globally recognised IT security standard developed by the UK's National Cyber Security Centre, which is used to ensure that IT software and processes are secure and organisations are protected from data breaches and leaks. The Cyber Essentials assessment involves 5 technical controls and is designed to show that an organisation has an extended level of protection in cyber security through annual assessments. Frontify has been assessed for compliance against all controls, and has officially obtained the Cyber Essentials certification in 2022.

HIPAA

Frontify is, as far as applicable, compliant with the HIPAA security, privacy, and breach regulations. To support our customers in aligning their vendor assessments with HIPAA compliance, we have prepared comprehensive self-assessment documentation outlining our security and privacy measures, mapped to the HIPAA security, privacy, and breach notification guidelines.

Contact security@frontify.com to grab a copy of our self-assessment.

SSPA

The Supplier Security and Privacy Assurance (SSPA) Program delivers Microsoft's baseline data processing instructions to suppliers in the form of the Microsoft Supplier Data Protection Requirements (DPR). At the core of Microsoft's SSPA Program are strong privacy and security practices, which are aligned with industry-wide standards such as ISO 27701 (privacy) and ISO 27001 (security).

Frontify is officially compliant with the SSPA and is independently audited against the DPR on a yearly basis, proving our strong commitment towards data privacy and security.

TISAX

Frontify's efforts to address additional, industry-specific data protection and information security requirements resulted in our latest certification (2022) for the TISAX standard: The Trusted Information Security Assessment Exchange is a standard for information security specifically relevant to the automotive industry, and it's operated and managed by the ENX Association (an association of European vehicle manufacturers, suppliers, and organizations). Highly qualified auditors from an audit service provider approved by TISAX perform the audit and conduct the tests based on a specific testing catalog, which follows key aspects of the international standard ISO 27001.

DCSO

The Deutsche Cyber-Sicherheitsorganisation GmbH (DCSO) is a competence center for cybersecurity in Germany. The DCSO Cloud Vendor Assessment Service assesses the security level of cloud service providers.

In 2021, Frontify was evaluated based on the DCSO Cloud Vendor Assessment framework and reached risk-free maturity levels in all subject areas. Members of the DCSO community can obtain more insights into Frontify's results directly from the DCSO.

Cloud infrastructure

3.1 Data center security

Frontify is hosted by one of the biggest data center providers, Amazon Web Services (AWS). Access to these data centers is strictly controlled and monitored by 24/7 on-site security staff, biometric scanning, and video surveillance. AWS maintains multiple certifications for its data centers, including ISO 27001, PCI DSS, Cloud Security Alliance Controls, and SOC reports.

3.2 Hosting and high availability

Frontify is hosted in a multi-tenant environment. All data for enterprise customers is protected in a virtual private cloud (VPC) with a logically separated database and dedicated file storage. All services that make up the Frontify system are highly available: We use a combination of clustering, load balancing, and replication to ensure no single point of failure. Each of our hosting regions uses two or more availability zones, with redundancy across them to guarantee the ongoing operation of our critical components in the unlikely case of a system failure.

3.3 Network security

On the network level, Frontify has implemented multiple layers of preventive and detective controls. At the network perimeter layer, Frontify has a network firewall and a web application firewall. Each production host has an intrusion detection system installed. Access is provisioned on a least-privilege basis, and a management-approved change control is required to affect any network or network security changes. All access to production systems is keystroke logged. Additionally, Frontify uses centralized logging and altering to detect any unusual activity, and AWS automatically blocks distributed denial-of-service (DDoS) attacks.

3.4 Data encryption

All data, at rest and in transit, is protected during its full lifecycle using industry-standard encryption mechanisms.

- **Encryption in transit:** Frontify leverages Transport Layer Security (TLS) 1.2 (or better) for customer data in transit over any network. Frontify supports full encryption in transit: No non-encrypted data leaves our data center. All our monitoring and backend systems either send local traffic over the VPC or use transport-level encryption when communicating with the rest of the internet.

- **Encryption at rest:** Frontify encrypts customer data at rest using the Advanced Encryption Standard (AES) 256-bit (or better).

3.5 Patching policy

Because of our agile software development, we perform multiple updates and patches on the application every day. These processes do not cause any downtime for the customer. Additionally, we continuously monitor our infrastructure for security updates and promptly test and install all new releases as soon as they become available.

3.6 Backups and disaster recovery

We run a nightly backup of files, databases, configuration, and servers. Our detailed business continuity plan covers several scenarios, responsibilities, and action steps, including a disaster recovery process that is tested at least yearly. These measures ensure a timely restoration of all operations in case of system disruption and guarantee adequate resources to face any scenario that might negatively impact our customers' businesses.

Our business continuity plan and disaster recovery process are audited as part of our ISO 27001 certification, assessing compliance with the given standards every year.

Application security and identity management

We have implemented strong authentication and authorization concepts to ensure the highest level of protection for our customers' Frontify accounts. Additionally, our platform uses a centralized logging system that facilitates 24/7 monitoring, reporting, and traceability.

4.1 Authentication

The Frontify access rights are managed at Guideline, Project, and Library levels. Currently, access to Frontify is organized in three ways:

- Single sign-on
- Access request
- Invitation

All access methods (except SSO) require a dedicated email address and password to properly authenticate the user logging in. Multi-factor authentication can also be enabled for an extra layer of security when accessing the platform.

4.2 Password policy

Frontify's default password policy requires a minimum of eight characters, including at least one uppercase and one lowercase letter and one number or special character.

4.3 Granular authorization rules

The granular authorization rules within the Frontify platform allow customers to easily add and manage users, assign them the appropriate privileges, and limit access to selected features.

Frontify supports the following main roles:

- **Viewers** can look at and download the content after being invited to a page.
- **Editors** can create and edit content. They can also invite additional Editors or provide access to Viewers.
- **Owners** can edit and delete the complete Guideline/Project and invite or remove other team members.
- **Account Admins** can manage the account and have complete control of configurations and account details. Only Admins can access User Management, Targets, and Groups settings.

4.4 Single sign-on

Single sign-on (SSO) is a fast and convenient way to access different applications using one set of login credentials. Frontify supports SSO based on the SAML 2.0 or OpenID Connect standards. With SSO, organizations can define user groups with related access permissions to easily manage access for their employees.

4.5 Two-factor authentication

Two-factor authentication (2FA) provides users with an extra layer of protection for their accounts. With Frontify, the second layer of authentication requires an authenticator app. Users can enable 2FA from their user profile settings. Alternatively, Account Admins can enforce 2FA for all of their Frontify users from the Security section in the Account tab.

4.6 Access logging and monitoring

Frontify operates a centralized logging system that facilitates 24/7 monitoring, reporting, and traceability.

The standard logs include the following information:

- **Server:** We provide typical web server access logs, including client IP address, user agent, time, and URL.
- **Application:** We cover the most common user actions, including logging in, logging out, requesting passwords, changing passwords, changing email addresses, removing users, and inviting groups.

Frontify has its own logging function that users with the appropriate permissions can view directly on the platform. In addition, we can also provide log exports on request. All logs are sent to a central log server to counteract manipulation and ensure the highest level of protection. The central server is accessible only by selected employees with the required role and permissions, and the logs are retained for 12 months. In case of unusual behavior on our production systems, our Security Team is alerted immediately through our Security Operations Center.

Quality assurance

Frontify guarantees the highest level of security for the entire infrastructure. Our proactive security approach results from a cross-team collaboration that involves our entire organization. For this reason, we've implemented a quality assurance plan covering strict internal access controls, vulnerability and risk management programs, monitoring and auditing, security-focused development, and change management processes.

5.1 Vulnerability monitoring and reporting

Our proactive vulnerability monitoring approach reflects our commitment to providing our customers with the most secure infrastructure and application. We classify vulnerabilities internally and treat them accordingly.

In line with our proactive approach toward vulnerability monitoring and reporting methodology, we have implemented an official bug bounty program at BugCrowd.

5.2 Incident management process

Frontify has an incident management and reporting process that unifies security monitoring and covers all our internal operations and the services provided to our customers. If a security breach leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to customer data, we'll notify the customers within 48 hours.

We classify incidents according to their severity level and remediate them based on their defined prioritization. To ensure a fast and efficient incident response procedure, Frontify has appointed a dedicated Incident Response Team.

5.3 Risk management and assessment

Frontify has implemented a risk assessment strategy and methodology that is ISO 27001 certified, and we regularly assess risks, threats, and vulnerabilities based on our asset inventory. We perform periodic overall risk assessments and categorize risks according to their likelihood and impact. For each risk, we create a remediation action plan or an acceptance statement in line with the criticality level.

5.4 Audits

Frontify conducts several internal audits throughout the year, ensuring cumulative coverage of the entire information security management system scope. We plan internal audits based on risk assessments and the results of previous audits. Based on our ISO 27001 certification, we conduct external audits at least once a year.

5.5 Secure development lifecycle

Frontify maintains separate testing, development, and production environments to meet the highest code quality. This process includes code reviews and pair programming conducted by experienced developers with a strong focus on security and stability. In addition, we run automated tests and put code builds in place. We use a hosted code platform to reach a high level of traceability and automatically monitor our third-party dependencies for security vulnerabilities. Our developers follow agile and trunk-based development principles and the Open Web Application Security Project (OWASP).

5.6 Change management

Frontify follows a strict procedure for all changes concerning our infrastructure and application. The Product Team reviews the relevant changes and prioritizes them according to their impact. The appointed person responsible for the area must approve each change before development. All changes must undergo manual and automatic testing procedures to meet the highest security requirements.

5.7 Access control

Frontify adheres to the principle of least privilege for provisioning access. We use dedicated roles for different topics and access for database administrators, general administrators, and support staff. All our employees are technically forced to use two-factor authentication and adhere to our password policy for all internal and external tools. We regularly perform access reviews that are defined in our access management policy.

Conclusion

Our goal is to ensure cloud-based efficiency for businesses that collaborate across different teams, borders, and languages to create a wide range of personalized brand content.

We put the protection of data at the core of all our operations. We achieve security excellence by defining a strong culture of security that is fully embraced by all teams and departments within our organization. Additionally, our reliable cloud infrastructure and strong technical controls for our entire operations allow us to offer a service that meets the highest security standards.

Our commitment to gaining and maintaining our customers' trust is reflected in our continuous efforts to improve and expand our security program, which we frequently audit to ensure ongoing compliance with the strictest industry standards. By including IT and information security in every aspect of our system development, internal operations, and data handling, we can offer brands a home where they can thrive.

security@frontify.com