Policies, Procedures & Controls

Information Security at Fabius

FABIUS

February 2022

Security Operations

FABIUS

Our Team

Our team is entirely based in the US and has expertise managing data integrations, analytics infrastructure, and data-driven products for public companies. We were previously responsible for building and maintaining the engineering systems and personnel processes that processed PII for thousands of customers, including hundreds of companies in the Fortune 500.

We know the value of privacy and security by design, and have architected our team, our operations, and our systems with this in mind.

Procedures

At Fabius, we have a rigorous focus on operational effectiveness. Formalized procedures enable us to scale efficiently, but also ensure privacy and security are always considered in our decision making processes and designs.

Monitoring

We monitor our production systems and our critical vendors for availability and address issues in a timely manner. For our policies, procedures and controls - each artifact has a named owner, and we conduct regular reviews to ensure our operations remain aligned with the data we process, the risks we face, and the clients we serve.

Software Development Best Practices

Our best practices include version control, staging environments, formal code reviews, code standards, and robust testing. We release changes to production environments via continuous integration, continuous deployment (CI/CD). We monitor our codebase for dependency vulnerabilities and deploy updates with timeframes based on severity.

We Store the Minimum Amount of Data

We work to minimize the amount of data that we store from Gong and other systems.

We store the following information (all encrypted at rest):

- Call transcripts
- Basic customer information, such as company name, and the names and titles of meeting attendees
- Names and descriptions of product features and use cases
- [Optional] Opportunity metadata such as opportunity size

Controls

We have detailed a number of our security controls on the pages that follow. For additional information, or questions about our other controls, reach out to security@fabius.io.

Security Essentials

FABIUS

Encryption At Rest & In Transit

All transcription data we store and process on behalf our our clients is encrypted at rest and in transit. All call transcript data is stored in AWS S3 leveraging industry-standard AES-256 server-side encryption.

Password Policies

For third party software, we use Google as our SAML provider for Single Sign On when available, and we enforce two-factor authentication whenever possible. We have defined best practices for password creation, and when SSO is not available, we encourage employees to use a password manager to generate and store secure passwords.

Hosting

All of our production systems and databases are running on AWS facilities, hosted in the US. Only customer-facing applications are accessible to the public internet.

Physical & Environmental Security

Fabius relies on AWS and their robust controls to manage the physical and environmental security of our systems. Visit the Amazon Web Services: Risk and Compliance page for more information.

We require Next-Gen antivirus software and Endpoint Detection and Response software to run on each employee laptop, and have policies to handle malware and ransomware. We require laptop hard drives to be encrypted with Apple FileVault.

Access Control - Secrets & Record Level Data

Client secrets are provided directly by users that must be authenticated via our web application using a verified email. Secrets are stored in the industry-standard AWS Secrets Manager. Production systems are restricted so that application servers are authorized with access only when needed.

Access Control - Production Systems

For our production systems, Fabius leverages Auth0 for client authentication to ensure secure access to our application (you can read more about Auth0's security practices here).

Internally, role-based access control is in place to protect our code base and production systems, and is granted on a need to know basis leveraging the principle of least privilege.

Access Control - Onboarding & Offboarding

When granting access to our application, we currently support email/password authentication and we require Multi-Factor Authentication. We remove access when a relationship is terminated according to our documented client and employee offboarding procedures.

Security Measures

FABIUS

Monitoring & Incident Response

We have automated monitoring and alerting for our critical systems and services. To handle and resolve issues that arise, our engineering team maintains an on call rotation 24/7.

Personal Account Information

We aim to minimize the amount of personal data we collect and store about our clients; however, we do collect and store information such as name and email address.

Additionally, we may leverage tools to track usage of our product such as analytics tools and server logs that may receive information such as IP address or potentially email address and / or name.

Security for Fabius Vendors

We regularly monitor, review, and audit vendor service delivery. Vendor security and service delivery performance is reviewed at least annually.

For vendors that handle sensitive information, we require that they implement standard security practices and procedures, such as:

- Secure Development Programs
- Protection against malicious software
- Network protection and management
- Technical vulnerability management
- Logging and monitoring
- Incident response
- Business continuity planning
- Technical access control program
- HR policies such as criminal background checks

Human Resources Policies

During the interview process, we perform competence assessments on relevant technical skills and perform criminal background checks. Once hired, each employee goes through annual security training and is educated on Fabius-specific policies (such as our coding practices).

Risk Assessment & Risk Management

It is important to constantly reevaluate the risks to our business, to evaluate the effectiveness of our operations, and to constantly improve our controls.

As such, we track our IT assets and review access on a regular cadence and we re-evaluate the risks to our business on a continuous basis. When we sign contracts, we review them to make sure our policies, procedures, and controls align with the expectations of our clients.

We strive for a culture of open dialogue within the company about the latest security threats and best practices, and our leadership team is expected to stay up to date on the latest regulation and compliance considerations that are relevant to our business.

security@fabius.io
1410 Franklin Street #104, San Francisco, CA 94109