



Whitepaper

Security Overview

version: 1.4 · Last updated: May, 2023

Pipefy Data Center & Network Security

Physical Security

NAME	DETAILS
Facilities	<p>Pipefy service providers' physical infrastructure is hosted and managed within Amazon's secure data centers and utilizes the Amazon Web Service (AWS) technology. Amazon continually manages risk and undergoes recurring assessments to ensure compliance according to the industry's standards. Amazon's data center operations have been accredited under:</p> <ul style="list-style-type: none">• ISO 27001• ISO 27701• ISO 27018• SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)• PCI Level 1• FISMA Moderate• Sarbanes-Oxley (SOX) <p>If the customer needs to use a multi cloud solution, Pipefy will analyze the case, and provide other cloud providers, with the same quality as AWS.</p>
On-site Security	<p>Pipefy utilizes ISO 27001 and FISMA certified data centers managed by Amazon. AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection.</p> <p>Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to</p>

present identification and are signed in and continually escorted by authorized staff.

Location

Pipefy service providers data centers are located in the United States. If the customer wants to apply for a Single Tenant, multi locations globally are available using different cloud solutions.

Network Security

NAME	DETAILS
Security Response Team	Our Security Response Team is on call to respond to security alerts and events and can be reached at security@pipefy.com
Protection	<p>PAIL firewalls infrastructure and management is provided by our service provider Amazon AWS.</p> <p>Firewalls are utilized to restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are allowed based on business need. Each system is assigned to a firewall security group based on the system's function. Security groups restrict access to the ports and protocols required for a system's specific function in order to mitigate risk. Host-based firewalls also provide the ability to further limit inbound and outbound connections as needed.</p>
Vulnerability Scanning	<p>Our service provider managed firewalls prevent IP, MAC, and ARP spoofing on the network and between virtual hosts to ensure spoofing is not possible. Packet sniffing is prevented by infrastructure including the hypervisor which will not deliver traffic to an interface which it is not addressed to. Our service provider utilizes application isolation, operating system restrictions, and encrypted connections to further ensure risk is mitigated at all levels.</p> <p>Port scanning is prohibited and every reported instance is investigated by our infrastructure provider. When port scans are detected, they are stopped and access is blocked.</p>
Penetration Testing and Vulnerability Assessments	Pipefy has a specialized team responsible for internal pentests, and vulnerabilities assessments. Those tests are performed at least 1 time quarterly.

Third party security testing of our services could be performed by independent and reputable security consulting firms hired by the customer. Possible findings from each assessment would be reviewed with the assessors, risk ranked, and assigned to the responsible team to solve it under a SLA.

Those testings will be done by the customer and all charges involved are customer responsibilities.

Security Incident Event and Response

In the event of a security incident, our engineers are called in to gather extensive logs from critical host systems and analyze them to respond to the incident in the most appropriate way possible.

Gathering and analyzing log information is critical for troubleshooting and investigating issues. Our service provider allows us to analyze three main log types: system, application, and API logs.

Shared responsibilities can exist between Pipefy and our Cloud Providers, and those responsibilities will be the responsibility of the Pipefy Security Team.

DDoS Mitigation

Our service provider's infrastructure provides DDoS mitigation techniques including TCP Syn cookies and connection rate limiting in addition to maintaining multiple backbone connections and internal bandwidth capacity that exceeds the Internet carrier supplied bandwidth. We work closely with our providers to quickly respond to events and enable advanced DDoS mitigation controls when needed.

Logical Access

Access to the Pipefy Production Network is restricted by an explicit need-to-know basis. It utilizes least privilege, is frequently audited, and is closely controlled by our Engineering Team. Employees accessing the Pipefy Production Network are required to use multiple factors of authentication.

Encryption and Authentication Requests

POLICY	DETAILS
Encryption in Transfer	All internal and external communication is done through a secure connection with TLS 1.2 or TLS 1.3.
Encryption in Transfer -- Emails	All emails are sent by Sendgrid through a secure TLS connection.
Encryption at Rest and in Backup	Data at rest is encrypted via AES-256 algorithm. The backup is done through snapshot, also with AES-256 encryption.

Availability & Continuity

POLICY	DETAILS
Uptime	Pipefy availability has been 99.99% for the year of 2022 and is continuously monitored. The availability can be seen on our site at: status.piefy.com .
Redundancy	Piefy service provider clustering and network redundancies eliminate single points of failure.
Disaster Recovery	Our service provider's platform automatically restores customer applications and databases in the case of an outage. The provider's platform is designed to dynamically deploy applications within its cloud, monitor for failures, and recover failed platform components including customer applications and databases.

Application Security

Secure Development (SDLC)

POLICY	DETAILS
Ruby on Rails Framework Security Controls	We utilize Ruby on Rails framework security controls to limit exposure to OWASP Top 10 security flaws. These include inherent controls that reduce our exposure to Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), and SQL Injection (SQLi), among others.
QA	Our QA department reviews and tests our code base. Dedicated application engineers on staff identify, test, and triage security vulnerabilities in code.
Separate Environments	Testing and staging environments are separated from the production environment. No actual customer data is used in the development or test environments.

Application Vulnerabilities

POLICY	DETAILS
Static Code Analysis	Our source code repositories are continuously scanned for security issues via our integrated static analysis tooling.

Product Security Features

Secure Development (SDLC)

FEATURE	DETAILS
Authentication Options	Pipefy supports sign-in, SSO and Google Authentication.
Single sign-on (SSO)	Single sign-on (SSO) allows you to authenticate users in your own systems without requiring them to enter additional login credentials for Pipefy access.
Secure Credential Storage	Pipefy follows secure credential storage best practices by never storing passwords in human readable format.
API Security & Authentication	Pipefy API is SSL-only and you must be a verified user to make API requests. You can authorize against the API using API token.

Additional Product Security Features

POLICY	DETAILS
Access Privileges & Roles	Access to data within your Pipefy account is governed by access rights, and can be configured to define access privileges. Pipefy has various permission levels for organization (member and admin) and pipe users (start form only, member and admin). More details can be seen here .

Transmission Security

All communications with Pipefy service provider servers are encrypted using industry standard HTTPS. This ensures that all traffic between you and Pipefy is secure during transit.

Security Methodologies

Information Security Management System

HIGHLIGHT	DETAILS
Objectives	<p>The strategic objectives of information security (strategic objectives of the ISMS) are those that Pipefy intends to achieve according to a corporate vision for information security and that are aligned with the objectives mentioned in its Corporate Strategic Plan, among which are:</p> <ul style="list-style-type: none">• Promote compliance with laws, rules and regulations related to the business in its aspects related to Information Security;• Continuous improve security controls and maturity on the Pipefy Platform to mitigate risks;• Increase knowledge and internal awareness of the need for Information Security for the business.

Security Awareness

METHODOLOGY	DETAILS
-------------	---------

Policies

Pipefy has developed a comprehensive set of security policies covering a range of topics. These policies are shared with, and made available to all employees and contractors with access to Pipefy information assets.

Audit Reports are not shared externally, only the results and the maturity level of the Pipefy environment.

Training

All new employees attend a Security Awareness Training as well as all employees perform the same training once a year. Furthermore, all employees attend Data Privacy, GDPR and LGPD training. All Engineering team members also participate once a year (apart of the Security Awareness Training) on a Secure Development Training that is based on OWASP TOP 10 and SANS 25. Security Awareness is also part of Pipefy's routine as updates are shared between all the teams via email, blog posts and in presentations during internal events.

Privacy Measures

On Pipefy we are aware about your privacy, and rights, and we work to deliver to you the best practices and measures to keep your data safe.

We are in accord with the requirements from LGPD, and GDPR.

And we are working tirelessly, every day, to maintain a high maturity level on our security measures.

You can see more information about Privacy, on Pipefy at:

Worldwide privacy page: <https://www.pipefy.com/privacy-policy/>

Brazilian privacy page:

<https://www.pipefy.com/pt-br/politica-de-privacidade/>

For any questions and requests, please contact our email:



privacy@pipefy.com.

Our DPO's email: dpo@pipefy.com.

Employee Vetting

METHODOLOGY	DETAILS
Background Checks	Pipefy performs background checks on all new employees in accordance with local laws. The background check includes Criminal, Education, and Employment verification.
Confidentiality Agreements	All new hires are screened through the hiring process and required to sign Non-Disclosure and Confidentiality agreements in accordance with local laws.

Certifications and additional documentation

CERTIFICATION	DETAILS
ISO 27001	<p>ISO 27001 standard is the internationally recognized best practice framework for an Information Security Management System (ISMS).</p> 
ISO 27701	<p>ISO 27701 is the international privacy standard that provides a framework for data privacy management. It is a data privacy extension to ISO 27001.</p> 

ISO 27018

ISO 27018 is the code of practice for protecting personally identifiable information (PII) in cloud computing services.



SOC 1 & 2 type 2

SOC 1 & 2 are regularly refreshed reports that focus on controls related to financial controls, security, availability, and confidentiality of a cloud service. Pipefy can share SOC 1 & 2 reports, through a signed non-disclosure agreement (NDA).



AWS Qualified Software

Our vendor AWS reviews our application infrastructure and security through the Foundational Technical Review (FTR). This process ensures that our implementation and cloud usage have been validated by AWS for their technical proficiency and associated customer references.



Consensus Assessments Initiative Questionnaire (CAIQ)

The CAIQ questionnaire provides an industry-accepted way to document what security controls exist in cloud services. This increases security control transparency for potential and current customers, who can then determine if our services are secure enough for their purposes.

The filled questionnaire can be obtained by a signed non-disclosure agreement (NDA).

