The purpose of Pingflow's security policy is to define the activities associated with the delivery of security services that protect information systems, networks, data, databases, and other assets related to software services. Any terms not defined in this document shall have the meaning given to them in the General Terms of Service for Customers.

1. Software Service Delivery Model

The Software Services are provided on the basis of ongoing maintenance, updates, and bug fixes that are released or deployed continuously.
The automated nature of software and infrastructure delivery, combined with frequent releases, requires security to be embedded throughout Pingflow's development lifecycle. This includes, but is not limited to, the following security, privacy, and quality assurance practices: requirements identification, requirements review, design reviews, development controls (e.g. static analysis, code reviews), automated and manual testing, automated vulnerability scanning, change management, and deployment controls.

2. Data Encryption

Pingflow uses the latest recommended encryption protocols and cipher suites to encrypt data in transit. Customer data is encrypted in transit using Transport Layer Security (TLS) versions 1.2 and 1.3, and encrypted at rest using AES 256-bit encryption, one of the strongest block cipher algorithms in the industry.

Pingflow closely monitors developments in the cryptographic landscape in order to update its software services as new vulnerabilities emerge, implement evolving best practices, and address compatibility requirements.

3. Identity Models and User Authentication

Customers may automatically provision subscribed users using the Pingflow system and Single Sign-On (SSO) to manage user accounts across software service providers.

Customers may also manage user accounts directly within the software service application. Credentials are never stored in a human-readable format. Pingflow uses a secure one-way hashing algorithm with salting.

Access to the Customer's instance is governed by roles and access rights configured by Pingflow administrators designated by the Customer.

4. Firewalls and Access Restrictions

Customers may choose to restrict access to one or more specific IP ranges so that their instance is accessible only from designated physical locations and through their VPN.

Pingflow also supports access restrictions through a unique browser-loaded cookie for web access, password-based access, and SSO authentication for temporary display endpoints.

5. Backups and Disaster Recovery

Customer data is stored redundantly across multiple locations within Pingflow's hosting provider data centers to ensure availability. Customer data is backed up daily and replicated in near real time to a designated secondary Microsoft Azure region. Backups are performed without impacting the availability of Customer data.

Pingflow's operations and IT infrastructure can therefore be easily recovered and restored when necessary. Pingflow regularly tests its disaster recovery measures to ensure appropriate resolution in the event of a major incident.

6. Network Protection and Logging

Pingflow's IT infrastructure uses a variety of controls to ensure the protection and isolation of environments, servers, software containers, and subnets. These controls include logical firewalls, web application firewalls (WAF), application load balancers, and similar mechanisms, ensuring that

only authorized traffic from the Internet or the corporate network is allowed to flow between servers.

Security logs are generated and analyzed for security events through automated monitoring software managed by Pingflow's security team.

Pingflow performs automated vulnerability scans on its production environment and remediates any findings that pose a risk to Pingflow's IT infrastructure.

7. Hosting Infrastructure

Pingflow uses Microsoft Azure to host all Customer instances related to the Pingview, Pingplay, and Pingpaas products.

For more information about Microsoft Azure's compliance and certification programs, please visit the following resources:
Microsoft Azure Compliance: https://learn.microsoft.com/azure/compliance/
Scaleway Compliance: https://www.scaleway.com/en/security-and-resilience/

8. Data Processing

Pingflow complies with European Union data protection laws with respect to international data transfer mechanisms. Accordingly, Pingflow's Data Processing Agreement (DPA) governs the transfer of Customer data in accordance with Regulation (EU) 2016/679 of the European Parliament (GDPR).

9. Data Breach and Incident Management

In the event of a security breach, Pingflow will promptly notify the Customer of any unauthorized access to Customer Data. Pingflow maintains an incident management process to handle the full lifecycle of a security incident.

Accès au doc SLA:
https://docs.google.com/document/d/1pF_7nqUcUUsw2Ic4MAEuVUL66uqC5a206ypJiZwNS2g/edit

Contact

For any questions, requests, or claims, you may contact us by email at the following address:
contact@pingflow.fr

Legal Notice

Pingflow SAS
Registered office: 3 rue des Teinturiers, 59491 Villeneuve-d'Ascq, France
SIRET: 792 600 009 00031
RCS Lille Métropole – France