The purpose of the Pingflow Security Policy is to define the activities associated with the provision of security services that protect information systems, networks, data, databases and other assets in connection with software services. All terms not defined in this document have the meaning given to them in the document General Terms of Service for Customers.

1. Software Services Delivery Model

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

2. Data encryption

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

Pingflow closely follows the evolution of the cryptographic landscape, updating software services to address new weaknesses as they emerge, responding to them as they are discovered, and implementing best practices as they evolve, taking compatibility needs into account.

3. Identity models and authentication users

The customer can also automatically provision subscribed users using Pingflow and Single Sign-On (SSO) to manage user accounts across software service providers.

The customer can also manage user accounts directly within the software services application. Identifying information is never stored in a human-readable format. Pingflow uses a secure one-way hashing algorithm with salt.

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

4. Firewalls and access restrictions

Customers can choose to restrict access to one or more specific IP ranges, so that their instance can only be accessed at designated physical locations and through their VPN.

Pingflow also supports access restrictions via a single cookie loaded into the browser accessing the service, password protection, and SSO login on temporary display points.

5. Backups and disaster recovery

Customer data is stored redundantly in multiple locations in Pingflow's hosting provider data centers to ensure availability. Customer data is backed up daily and replicated in near-real time to the designated Microsoft Azure secondary region. Backups are performed with no impact on customer data availability. Pingflow's operations and IT infrastructure can therefore be easily recovered and restored when necessary. Pingflow regularly tests its disaster recovery measures to ensure adequate resolution of a major disaster.

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, subnets and logical firewalls, web application firewall, logical firewall, web application firewall, application load balancers, etc. to ensure that only authorized traffic from the Internet or corporate network between servers is allowed. Logs are generated and analyzed for security events via automated monitoring software managed by Pingflow's security team.

Pingflow performs automatic vulnerability scans on its production environment and remedies any findings that present a risk to Pingflow's IT infrastructure.

7. Hosting infrastructure

Pingflowuses Microsoft Azure to host all customer instances of Pingview, Pingplay and Pingpaas products. For more information on their certification and compliance program, please visit the following websites:
Link to Microsoft Azure compliance:
https://learn.microsoft.com/fr-fr/azure/compliance/
Link to Scaleway compliance:
https://www.scaleway.com/en/security-and-resilience/

8. Data processing.

Pingflow complies with European Union data protection laws with regard to international data transfer mechanisms. To this extent, Pingflow's Data Processing Agreement (DPA) covers the transfer of customer data. under Regulation (EU) 2016/679 of the European Parliament (RGPD).

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 has an incident management process to manage the entire lifecycle of a security breach.

Access the SLA doc:
https://docs.google.com/document/d/1pF_7nqUcUUsw2Ic4MAEuVUL66uqC5a206ypJiZwNS2g/edit

Contact

If you have any questions, queries or complaints, please contact us by e-mail at: contact@Pingflow.fr

Terms of use
Pingflow SAS
Head office: 3 rue des Teinturiers 59491
Villeneuve d'Ascq
SIRET : 792 600 009 00031 - FRANCE
RCS Lille Métropole - France