

L'objectif de la politique de sécurité de Pingflow est de définir les activités associées à la fourniture de services de sécurité qui protègent les systèmes d'information, les réseaux, les données, les bases de données et les autres actifs en relation avec les services logiciels. Tous les termes qui ne sont pas définis dans le présent document ont la signification qui leur est donnée dans le document Conditions générales de service pour les Clients.

1. Modèle de fourniture des services logiciels

Les Services du Logiciel sont fournis sur la base d'une maintenance, de mises à jour et de corrections de bugs qui sont publiées ou déployées de manière continue. La nature automatisée de la livraison des services logiciels et de l'infrastructure, d'infrastructure, combinée à des versions fréquentes, exige que la sécurité soit intégrée dans le cycle de développement de Pingflow, y compris, mais sans s'y limiter, les pratiques suivantes en matière de sécurité, de confidentialité et d'assurance qualité identification des exigences, revue des exigences, revues de conception, contrôles de développement (ex. statique, revues de code), tests automatisés et manuels, analyses de vulnérabilité automatisées, gestion des changements et contrôles du déploiement.

2. Cryptage des données

Pingflow utilise les derniers protocoles et suites de chiffrement recommandés pour crypter les données en transit. Les données du client sont cryptées en transit à l'aide du protocole TLS (Transport Layer Security) 1.2/1.3 et cryptées au repos à l'aide du protocole AES 256 bits, l'un des algorithmes de chiffrement par blocs les plus puissants de l'industrie.

Pingflow suit de près l'évolution du paysage cryptographique afin de mettre à jour les services logiciels pour répondre aux nouvelles faiblesses dès qu'elles apparaissent pour répondre à celles-ci au fur et à mesure qu'elles sont découvertes et mettre en œuvre les meilleures pratiques au fur et à mesure qu'elles évoluent et en tenant compte des besoins de compatibilité.

3. Modèles d'identité et authentification des utilisateurs

Le client peut aussi automatiquement provisionner les utilisateurs abonnés à l'aide du système Pingflow et du Single Sign-On (SSO) pour gérer les comptes utilisateurs à travers les fournisseurs de services logiciels.

Le client peut également gérer les comptes des utilisateurs directement dans l'application de services logiciels. Les informations d'identification ne sont jamais stockées dans un format lisible par l'homme. Pingflow utilise un algorithme de hachage unidirectionnel sécurisé avec du salage (salt). L'accès à l'instance du Client est régi par les rôles et les droits d'accès configurés par les administrateurs Pingflow désignés par le Client.

4. Pare-feu et restrictions d'accès

Le Client peut choisir de restreindre l'accès à une ou plusieurs plages d'IPs spécifiques afin que son instance ne soit accessible que dans les lieux physiques désignés et à travers leur VPN. Pingflow supporte également les restrictions d'accès par cookie unique chargé dans le navigateur web accédant au service, le mot de passe, ainsi que la connexion par SSO sur les points d'affichages temporaires.

5. Sauvegardes et reprise après sinistre

Les données du client sont stockées de manière redondante à plusieurs endroits dans les centres de données de l'hébergeur de Pingflow afin d'en assurer la disponibilité. Les données du client sont sauvegardées tous les jours et répliquées en temps quasi réel dans la région secondaire désignée de Microsoft Azure. Les sauvegardes sont effectuées sans impact sur la disponibilité des données du client. Les opérations et l'infrastructure informatique de Pingflow peuvent donc être facilement récupérées et restaurées lorsque cela est nécessaire. Pingflow teste régulièrement ses mesures de reprise après sinistre afin de garantir une résolution adéquate d'un sinistre majeur.

6. Protection et journalisation du réseau

L'infrastructure informatique de Pingflow utilise une variété de contrôles pour assurer la protection et l'isolation des environnements, serveurs, conteneurs

logiciels, sous-réseaux tels que le pare-feu logique, le pare-feu d'application web, pare-feu logique, pare-feu d'application web, équilibreurs de charge d'application, etc. afin de garantir que seul le trafic autorisé provenant d'Internet ou du réseau de l'entreprise entre les serveurs est autorisé. Les journaux sont générés et analysés pour les événements de sécurité par le biais d'un logiciel de surveillance automatisé géré par l'équipe sécurité de Pingflow.

Pingflow effectue des scans automatiques de vulnérabilité sur son environnement de production et remédie à toute découverte présentant un risque pour l'infrastructure informatique de Pingflow.

7. Infrastructure d'hébergement

Pingflow utilise Microsoft Azure pour l'hébergement de toutes les instances du Client relative aux produits Pingview, Pingplay et Pingpaas. Pour plus d'informations sur leur programme de certification et de conformité, veuillez visiter les sites suivants :

Lien vers Microsoft Azure compliance :

<https://learn.microsoft.com/fr-fr/azure/compliance/>

Lien vers Scaleway compliance:

<https://www.scaleway.com/en/security-and-resilience/>

8. Traitement des données.

Pingflow se conforme aux lois de l'Union européenne sur la protection des données en ce qui concerne les mécanismes de transfert international de données. Dans cette mesure, l'accord de traitement des données (DPA) de Pingflow couvre le transfert des données du client. en vertu du règlement (UE) 2016/679 du Parlement européen (RGPD).

9. Gestion des violations de données et des incidents.

En cas de violation de la sécurité, Pingflow informera rapidement le Client de tout accès non autorisé aux Données du Client. Pingflow dispose d'un processus de gestion des incidents pour gérer l'ensemble du cycle de vie d'une violation de sécurité.

Accès au doc SLA:

https://docs.google.com/document/d/1pF_7nqUcUUsw2lc4MAEuVUL66uqC5a206ypJiZwNS2g/edit

Contact

Pour toutes questions, requêtes ou plaintes, merci de nous contacter par e-mail à l'adresse: contact@Pingflow.fr

Mentions légales

Pingflow SAS

Siège Social: 3 rue des Teinturiers 59491

Villeneuve d'Ascq

SIRET : 792 600 009 00031 -

RCS Lille Métropole - France
