BORÉALIS

Infokit sur la Sécurité

Boréalis est certifié ISO 27001: 2022

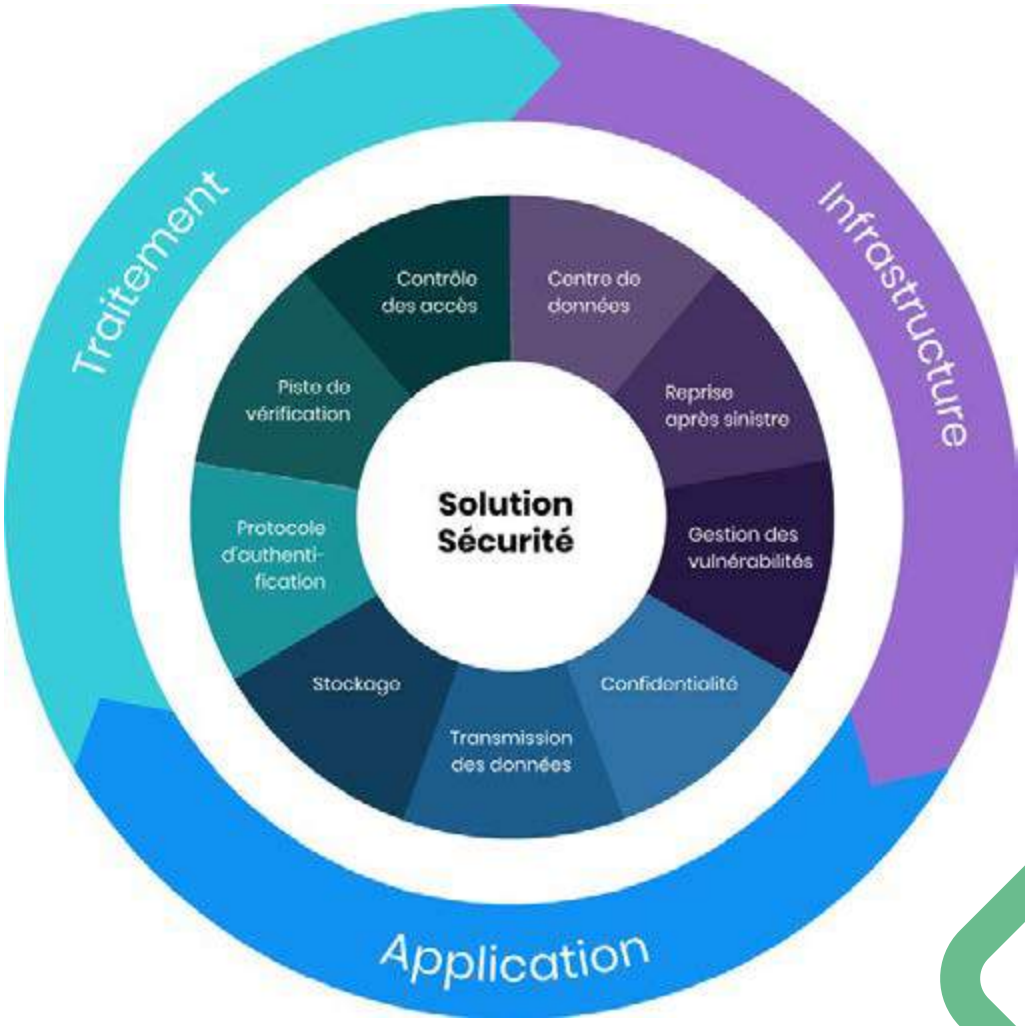
ISO 27001 est une norme internationalement reconnue qui aide les organisations à gérer la sécurité de l'information afin de rendre leurs ressources informatiques plus sûres. Pour obtenir la certification, une organisation doit élaborer et mettre en oeuvre un programme de sécurité strict, évaluer régulièrement les risques, les menaces et les vulnérabilités en matière de sécurité de l'information, et établir que ses programmes de sécurité sont conformes aux meilleures pratiques de l'industrie.

Après un audit réussi réalisé par un tiers indépendant, l'organisation peut être certifiée par un registraire accrédité.

Ce document porte sur un certain nombre de ces mesures, notamment :

- Volet confidentialité intégré à la sécurité des données opérationnelles
- Sécurisation de l'application
- Sécurité organisationnelle et des processus de gestion du changement
- Certification et accréditation des modalités de sécurité
- Modalités de sécurité à la mise en marche du centre de données
- Confidentialité

Téléchargez notre certificat



Aperçu des modalités de sécurité de la plateforme Boréalis

L'application Boréalis est conçue de manière à organiser les aspects fonctionnels et de sécurité en plusieurs couches mutualisées bien définies : présentation, configuration, plateforme et base de données.

Chez **Boréalis**, la confidentialité est assurée par des ententes contractuelles que tous les employés et consultants doivent entériner ainsi que par notre Programme de sensibilisation aux questions de sécurité, mené annuellement.

Afin d'assurer la confidentialité, seul le personnel expressément autorisé a accès à l'information qui nous est confiée.

Confidentialité

Nous traitons toute l'information fournie par les clients avec la plus grande attention et, à défaut de directives claires, nous considérons automatiquement confidentielles l'ensemble des données qui nous sont confiées. Nous encryptons, à l'aide de méthodes à la fine pointe de la technologie, les données afin que seules les personnes dûment autorisées puissent y avoir accès. De plus, grâce à notre méthodologie d'évaluation du risque, nous nous assurons d'avoir toujours en place les modalités nécessaires pour bien protéger les données de nos clients.

Évaluation du risque

Grâce à nos modalités d'évaluation du risque ainsi que de détection et de prévention des vulnérabilités, nous sommes en mesure de faire face aux incidents et aux problèmes pouvant mettre en danger notre infrastructure. Ces mécanismes protègent l'ensemble de notre environnement physique et réseau principal en plus des réseaux internes et l'accès des employés aux environnements clients.

Renforcement et surveillance de la configuration

Le renforcement de nos serveurs fait partie intégrante de nos procédures. Notre surveillance active des changements apportés à l'environnement nous permet de déceler, en temps réel, toute déviation pouvant signaler une modification de la légitimité des activités. Si la vérification confirme une telle modification, les mesures appropriées sont automatiquement appliquées. Nos profils de configuration de sécurité des serveurs-hôtes sont attribués selon les normes et les meilleures pratiques en vigueur.

Sécurité des opérations

Surveillance et correctifs

Notre environnement est soumis à un processus de surveillance, de vérification et de correction constant afin de contrer les menaces, y compris les failles et vulnérabilités communes (Common Vulnerabilities and Exposures [CVE]).

Surveillance des utilisateurs

Nous surveillons et documentons l'accès aux serveurs-hôtes de même que le niveau d'authentification et les délais de connexion afin de nous assurer du respect des modalités d'accès en vigueur.

Gestion de l'intégrité des fichiers

Nous procédons à la détection, au signalement et à la documentation des changements effectués aux dossiers selon les exigences de sécurité et de conformité en vigueur.

Surveillance des journaux (log) et des événements

Nous utilisons un sous-système SIEM (Security Information and Event Management) pour colliger les journaux de nos serveurs et mettre en corrélation les événements. En cas de problème, le système avertira en temps réel notre équipe de sécurité.

Gestion des incidents de sécurité

En cas d'incident, nous procédons rapidement à une enquête approfondie afin de déterminer la nature exacte de l'incident et les clients touchés. Nous travaillons de concert avec les parties en cause afin de régler le problème et nous prenons ensuite note des enseignements à tirer. Par la suite, dans le cadre de notre processus de gestion de la sécurité, nous revoyons nos politiques et notre planification en vigueur afin d'améliorer nos pratiques.

Sécurité des données

Les données sont séparées par instance et chaque instance constitue une entité physique distincte. L'accès aux données est restreint en fonction des droits d'accès configurés et enregistrés dans la plateforme. Cette dernière est construite sur une architecture multi-entités qui permet de multiples scénarios d'accès, qu'il s'agisse d'un projet global incluant les partenaires et les contracteurs de l'entreprise ou du déploiement d'un projet particulier sur un site donné.

Multi-entités

Une seule installation dessert toutes les unités d'affaires, mais ces dernières ne partagent pas toutes la même base de données. De même, l'ensemble des unités d'affaires partagent la même version de l'application Boréalis, mais sont configurées indépendamment les unes des autres.

Multi-instances

Une entité peut avoir plusieurs instances qui sont, par exemple, assignées à des environnements différents. De plus, chaque instance peut être configurée différemment.

Ségrégation des données et sécurité au niveau des enregistrements (row level security)

Pour une même instance, il est possible d'instaurer une ségrégation des données de manière à montrer ou cacher l'information en fonction de degré d'accès accordé à l'utilisateur. Les groupes sont définis et attribués aux différents utilisateurs de manière à contrôler l'accès aux données. L'application Boréalis offre aussi la hiérarchisation des accès afin de permettre une ségrégation complexe des données entre équipes, unités d'affaires, contracteurs et partenaires.

Sécurité au niveau de l'application

L'application Boréalis comporte une série de mécanismes de sécurité permettant d'effectuer une implémentation précise afin de satisfaire à des exigences bien définies. Les modèles d'architecture logicielle sont stratégiquement sélectionnés pour satisfaire aux besoins en matière de confidentialité, d'intégrité et de disponibilité des données : ségrégation des données et sécurité au niveau des lignes, listes de droits d'accès en fonction du rôle, pistes de vérification et gestion des journaux.

Authentication

L'application Boréalis comporte de nombreux fournisseurs de services d'authentification et des politiques complexes de création de mots de passe. La norme SAML (Security Assertion Markup Language) peut aussi être intégrée aux fins d'authentification des entreprises.

Administration

La sécurité et la confidentialité sont présentes au niveau de l'instance. Ainsi, une instance comporte un groupe de données et des utilisateurs. Les utilisateurs de cette instance n'ont jamais accès aux données des autres instances. L'application comporte une console d'administration qui permet aux supers utilisateurs de gérer leurs utilisateurs, c'est-à-dire d'ajouter et d'effacer des utilisateurs, d'assigner des profils d'utilisateur, d'obtenir les statistiques d'accès, de consulter les pistes de vérification, de modifier la langue d'utilisation, etc.

Rôle d'utilisateur et autorisation de groupe

Chaque action peut être configurée selon des paramètres d'autorisation d'accès. Les autorisations sont regroupées sous les profils d'utilisateur et sont définies par rôle et par groupe.

Protection des données en transit

Toutes les données de l'application Boréalis qui doivent transiter sont encryptées suivant le protocole TLS 1.2/1.3, qui est conçu pour sécuriser les communications par Internet. Les clés d'encryptage sont stockées de manière sécuritaire. De plus, les sessions des utilisateurs sont identifiées et vérifiées de nouveau à chaque transaction grâce à un jeton électronique unique qui a été créé au moment de l'ouverture de la session.

Utilisation responsable de l'intelligence artificielle (IA)

Boréalis intègre l'intelligence artificielle (IA) dans certaines fonctionnalités de sa plateforme, principalement pour des tâches de résumé de texte et de traduction. Nos fonctionnalités d'IA utilisent les modèles GPT de Microsoft Azure, garantissant la résidence régionale des données et une communication sécurisée via API.

Protection supplémentaire : Filtre de contenu OpenAI

Afin de mieux protéger les utilisateurs et de garantir une utilisation responsable de l'IA, OpenAI applique un filtre de contenu en amont de l'exécution des requêtes. Ce filtre agit comme une mesure de protection automatique contre les requêtes susceptibles de contenir du contenu inapproprié ou à risque élevé, notamment :

- Langage haineux ou discriminatoire
- Instructions violentes ou nuisibles
- Contenu sexuellement explicite
- Tentatives de manipulation ou d'exploitation du système

Fonctionnement

Chaque requête est analysée par le système de filtrage d'OpenAI avant d'être transmise au modèle de langage.

- Si une requête est classée dans une catégorie bloquée ou à haut risque, la demande est rejetée et une réponse neutre ou un message d'erreur est renvoyé.
- Ce filtrage est effectué côté serveur, avant que le modèle ait accès au contenu de la requête, ce qui ajoute une couche proactive de sécurité.
- Le filtre est continuellement mis à jour par OpenAI pour refléter l'évolution des risques et prendre en compte les retours des utilisateurs.

Objectif

Protéger les utilisateurs finaux, prévenir les usages abusifs et garantir une expérience d'IA sûre et éthique, conforme à nos standards.

Portée des données d'entraînement du modèle

Les modèles GPT-4.1-mini et GPT-4o-mini, utilisés par Boréalis, ont été pré-entraînés par OpenAI à partir de données publiques et sous licence.

- Les deux modèles ont été entraînés avec des données allant jusqu'en octobre 2023, mais GPT-4o a été conçu avec une nouvelle architecture optimisée pour la rapidité et les capacités multimodales.
- Aucun des modèles n'apprend à partir des saisies des utilisateurs et ils ne sont pas mis à jour en temps réel avec les données des clients.

Encryption

Les données au repos stockées sur nos serveurs sont encryptées à l'aide du protocole AES-256 (XTS-AES-128, clé de 256 bits) et les clés sont gérées par notre équipe de sécurité.

Tous les postes de travail Boréalis, y compris les ordinateurs portables et de bureau, ainsi que les serveurs, sont chiffrés afin de garantir la protection des données locales en cas de perte ou de vol d'un appareil. Nous utilisons BitLocker pour les appareils Windows et FileVault pour les appareils macOS afin de maintenir ce niveau de sécurité.

Sécurité organisationnelle et des processus de gestion du changement

Chez Boréalis, le concept de sécurité va bien au-delà de la mise en place des systèmes et des technologies appropriés. Il fait partie intégrante de notre culture d'entreprise et de nos processus d'affaires quotidiens.

La gestion du changement constitue, de même, un des aspects critiques de l'assurance de la sécurité chez Boréalis. Du développement à la mise en opération, nous appliquons les meilleures pratiques de l'industrie pour l'ensemble du cycle de vie de nos produits (détermination des exigences, contrôle de version, vérification continue de l'intégration, emballage, déploiement et assurance qualité). Nous surveillons aussi de manière proactive les vulnérabilités et les incidents.

Accès et soutien global

L'équipe des opérations et du soutien Boréalis surveille l'infrastructure de manière continue et l'accès au système est soumis à des politiques strictes : inscription des utilisateurs, gradation des privilèges d'accès, contrôle, modification et annulation des mots de passe, revue des droits d'accès à l'ensemble du système. Notre équipe de soutien assure l'entretien et le soutien de l'ensemble des applications hébergées. L'accès aux applications et aux données se limite aux usages suivants : surveillance du bon état de marche des applications, entretien des applications ou des systèmes et, à la demande du client, soutien technique. Seuls les employés dûment qualifiés et autorisés ont accès au système grâce à une authentification double facteur, mais les clients sont tenus d'assurer eux-mêmes la sécurité de leurs données de connexion. Une vérification de l'ensemble des accès est effectuée au moins deux fois par année ainsi que chaque fois qu'un employé est engagé/quitte l'entreprise ou change de poste.

Formation à la sensibilisation à la sécurité

Chez Boréalis, nous croyons que la sécurité commence par les individus. Par conséquent, tous les employés sont tenus de suivre une formation obligatoire à la sensibilisation à la sécurité dans les deux premières semaines suivant leur embauche, puis chaque année par la suite.

Cette formation est dispensée sur la plateforme Microsoft Security and Compliance et couvre une variété de sujets essentiels.

Surveillance et gestion des vulnérabilités

Boréalis fait appel à des spécialistes en sécurité tiers et à des solutions de sécurité de niveau entreprise (comme Qualys) pour détecter et corriger les vulnérabilités dans l'infrastructure informatique et les applications web. Des rapports des derniers tests d'intrusion effectués par des tiers, ainsi que des rapports Qualys, sont disponibles sur demande.

Boréalis utilise des systèmes de gestion des vulnérabilités pour sécuriser en continu l'infrastructure informatique contre les menaces les plus récentes d'Internet. Un système d'analyse d'applications Web identifie automatiquement les 10 principaux risques de l'OWASP, notamment l'injection SQL, les scripts intersites (XSS), la falsification de requêtes intersites (CSRF) et la redirection d'URL.

Toutes les applications web, les réseaux et le matériel sont constamment surveillés par Boréalis ainsi que par les fournisseurs d'infrastructure en tant que service (IaaS) gérés.

Chaque ligne de code modifiée dans nos dépôts est vérifiée par un second développeur. Une suite de tests automatisés comprenant plusieurs milliers de tests est ensuite exécutée.

Des vérifications de code sont également effectuées avec Eslint, ainsi qu'un contrôle de vulnérabilités des bibliothèques externes via Yarn audit.

Technologies

L'application Boréalis utilise des technologies récentes et évolue constamment avec elles. Les dernières fonctionnalités offertes par ces technologies sont également disponibles dans l'application, ce qui garantit un niveau élevé de sécurité pour notre backend. Par exemple, les problèmes de sécurité sont rapidement corrigés. De plus, de nouvelles versions sont publiées régulièrement.

Voici quelques-unes des technologies intégrées dans notre application :

- Docker
- Elasticsearch
- Node.js
- NginX
- MongoDB
- OpenSSL
- PostgreSQL
- React

Confidentialité

Boréalis comprend l'importance de garantir la confidentialité de vos informations. Pour en savoir plus, veuillez consulter notre Contrat principal d'abonnement :

https://www.boreal-is.com/data/cdn/media/Borealis-Master-Subscription-Agreement.pdf

Certifications et accréditations de Boréalis en matière de sécurité

Boréalis propose des solutions conçues et utilisées par de nombreuses grandes organisations. Nous respectons les normes les plus strictes de l'industrie en matière de sécurité des entreprises afin de garantir la confidentialité, l'intégrité et la disponibilité des informations de nos clients.

Sécurité chez Boréalis

Afin de répondre aux exigences de sécurité et à la politique de durabilité de Boréalis, notre service est hébergé dans des espaces dédiés au sein d'un centre de données de premier niveau, certifié selon les normes de l'industrie. Un test d'intrusion est réalisé chaque année sur notre plateforme par une entreprise externe.

En complément, nous renforçons la sécurité interne grâce à diverses politiques et procédures visant à protéger l'accès aux données.

Centre de données certifié Tier 3 et conforme à la norme SSAE 16

Les services d'hébergement de Boréalis sont déployés dans un centre de données conçu selon la certification Tier 3. Amazon AWS est certifié ISO 27001:2005 pour la fourniture et l'exploitation d'infrastructures cloud dédiées. Amazon AWS s'appuie sur les normes de gestion de la sécurité et d'évaluation des risques ISO 27002 et ISO 27005, ainsi que sur les processus associés. Amazon AWS a également obtenu les certifications SOC 1 et SOC 2 de type II.

Pour plus de détails sur les certifications d'Amazon AWS :

https://aws.amazon.com/fr/compliance/soc-faqs/
https://aws.amazon.com/fr/compliance/iso-certified/

Mise en œuvre de la sécurité du centre de données

Les services d'hébergement de Boréalis sont construits sur l'infrastructure Amazon AWS, prête pour les entreprises. Une infrastructure informatique distribuée et évolutive est utilisée pour héberger et gérer l'application Boréalis.

Afin de garder le contrôle sur ses capacités, Boréalis choisit l'emplacement d'hébergement des données des clients. Les emplacements actuels d'hébergement sont le Canada, la France ou l'Australie.

Si un client souhaite un centre de données de production spécifique, des frais supplémentaires peuvent s'appliquer.

Sécurité du centre de données

Les serveurs de production de Boréalis sont hébergés dans des centres de données conçus selon la certification Tier 3 (notation de l'Uptime Institute). Les installations sont conformes aux normes ISO 27001:2005, SOC 1 type II (SSAE 16 et ISAE 3402) et SOC 2 type II. Les centres de données sont dotés de mesures de sécurité physique robustes, notamment l'accès par biométrie et carte à puce, ainsi que de mesures de sécurité logique telles que des pare-feux, la détection d'intrusion, la vidéosurveillance, la prévention des intrusions et la protection

contre les attaques par déni de service (DDoS). L'alimentation électrique, le refroidissement et les réseaux sont redondants et diversifiés, construits selon un minimum de redondance N+1. L'auto-évaluation de Boréalis selon la Cloud Security Alliance STAR est disponible ici :

https://cloudsecurityalliance.org/registry/amazon/

Efficacité énergétique des centres de données

Amazon Web Services (AWS) s'engage à fonctionner de la manière la plus respectueuse de l'environnement possible et à atteindre une utilisation de 100 % d'énergie renouvelable pour son infrastructure mondiale.

Une étude menée par 451 Research montre que l'infrastructure d'AWS est 3,6 fois plus écoénergétique que la médiane des centres de données d'entreprise aux États-Unis. Plus des deux tiers de cet avantage proviennent de la combinaison d'une population de serveurs plus écoénergétiques et d'un taux d'utilisation des serveurs nettement plus élevé.

AWS a mis en place plusieurs initiatives pour améliorer l'efficacité de l'utilisation de l'eau et réduire la consommation d'eau potable pour le refroidissement des centres de données. AWS élabore sa stratégie de gestion de l'eau en analysant les conditions climatiques propres à chaque région AWS, la gestion locale des ressources en eau et les possibilités de préserver les sources d'eau potable.

Centres de données Amazon AWS

Pour plus d'informations sur les centres de données, consultez https://aws.amazon.com/fr/

Infrastructure physique

L'infrastructure de Boréalis, incluant les commutateurs réseau, les pare-feux, les serveurs et les dispositifs de stockage partagé, est gérée et configurée par l'équipe Boréalis. Amazon AWS est l'un des principaux fournisseurs de services gérés et a atteint un niveau élevé en matière de certifications de sécurité. Tous les services Boréalis sont configurés pour assurer une haute disponibilité, afin de réduire au minimum les interruptions de service.

Sauvegardes

Des sauvegardes complètes des serveurs virtuels sont effectuées quotidiennement. Les sauvegardes sont conservées selon la politique suivante : les 7 derniers jours, les 8 dernières semaines, et les 12 derniers mois.

Reprise après sinistre

Boréalis utilise plusieurs centres de données pour héberger son application et ses données, offrant ainsi une redondance essentielle. Tous les centres de données appliquent des mesures de sécurité physique, des politiques d'accès strictes, ainsi que des coffres et cages sécurisés. Chaque serveur est répliqué en temps réel dans une seconde zone de disponibilité située dans la même région AWS. Le service Boréalis assure une réplication des données quasi en temps réel entre le centre de données de production et le centre de reprise après sinistre. Des tests de reprise à chaud sont effectués quotidiennement, et un diagnostic complet de reprise après sinistre est réalisé chaque trimestre pour vérifier nos délais de rétablissement prévus ainsi que l'intégrité des données clients.

Sécurité réseau

Le réseau de Boréalis est protégé par un pare-feu de niveau entreprise ainsi qu'un système de prévention et de détection des intrusions (IPS/IDS) permettant de surveiller le trafic réseau et de bloquer un large éventail d'exploits de vulnérabilités connus. Le réseau Amazon AWS est protégé contre les attaques de type DoS/DDoS.

Pour plus de détails : https://aws.amazon.com/fr/shield/ddos-attack-protection/

Transmission

En utilisant le réseau Amazon AWS, plusieurs connexions aux dorsales Internet assurent une redondance du routage et une connectivité haute performance.

Sécurité des ressources humaines

Lors de l'embauche des employés, nous effectuons des vérifications des antécédents criminels. Celles-ci sont répétées tous les 5 ans.

Gestion des actifs

Nous utilisons un outil permettant de réaliser automatiquement l'inventaire de tout notre matériel et de nos logiciels au sein de notre infrastructure informatique.

Gestion des accès logiques

Chaque utilisateur dispose d'un compte nominatif, et des autorisations minimales lui sont attribuées.

Toutes les actions effectuées par les utilisateurs sont enregistrées et surveillées par notre outil SIEM.

Sécurité du développement logiciel

Notre environnement de production est entièrement isolé du réseau de développement, sur un réseau accessible uniquement via un VPN avec authentification à deux facteurs.

Les données de production ne sont jamais utilisées pour les tests ou l'assurance qualité (QA).

Mises à jour des systèmes et des logiciels

Tous les postes de travail (ordinateurs portables et de bureau) de nos utilisateurs sont équipés d'un antivirus, toujours à jour grâce à la fonctionnalité de mise à jour automatique. Les mises à jour du système d'exploitation sont gérées via des GPO (stratégies de groupe) et sont automatiquement appliquées sur leurs ordinateurs.

Confidentialité

Nous accordons une très grande importance à la protection de la vie privée. Chaque jour, les entreprises sont exposées au risque d'une faille de sécurité ou de violation de données, pouvant provenir de n'importe où dans le monde. Beaucoup d'éléments sont en jeu : des données sensibles qui vous fournissent des informations stratégiques, à la confiance que vous avez bâtie avec vos clients — une confiance difficile à regagner. Certaines violations peuvent même conduire des entreprises à la faillite à la suite d'une mauvaise publicité.

Contrairement à d'autres organisations, nous intégrons la confidentialité dès la conception à toutes les étapes de notre cycle de développement logiciel. Pour plus de détails sur notre cycle de développement logiciel :

https://www.boreal-is.com/data/uploads/2023/04/Borealis-software-life-cycle-2022-INDD-FR.pdf

Traiter les questions de confidentialité, de conformité et de sécurité a posteriori entraîne des coûts accrus pour la mise en œuvre de mesures d'atténuation des risques. Chez Boréalis, nous abordons ces aspects dès la phase de conception, et nous révisons constamment nos solutions pour assurer leur conformité aux principes de confidentialité.

Les exigences en matière de confidentialité sont intégrées dans notre solution afin de garantir que les installations d'hébergement des données respectent les exigences en la matière.

Lorsque cela est spécifiquement requis par un client — notamment pour répondre à des exigences réglementaires ou de confidentialité particulières — nous collaborons avec le client, par le biais d'accords contractuels, pour héberger ses données dans un centre de données de son choix, avec l'approbation formelle du client quant au pays d'hébergement des données.

Pour consulter la politique de confidentialité complète :

https://www.boreal-is.com/fr/confidentialite/

Prêt à simplifier vos opérations ?

NOUS SOMMES PRÊTS À VOUS AIDER.

+ 1 819 575-6037
contact-us@boreal-is.com
/borealiscsr/
boreal-is.com
Boreal-is
@BorealisCSR/