BORÉALIS

Infokit sur la Sécurité

Boréalis est certifié ISO 27001: 2017

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 œuvre 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.

Téléchargez notre certificat

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

Infokit Boréalis Sécurité - Copyright © Borealis. Tous droits réservés - Février 2023

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.

Infokit Boréalis Sécurité – Copyright © Borealis. Tous droits réservés – Février 2023

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.

Infokit Boréalis Sécurité – Copyright © Borealis. Tous droits réservés – Février 2023

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.

Communication

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.

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.

Infokit Boréalis Sécurité – Copyright © Borealis. Tous droits réservés – Février 2023

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.

Surveillance et gestion des vulnérabilités

Boréalis fait appel à des entreprises tierces spécialisées en sécurité de même qu'à des systèmes de sécurité d'entreprise, comme Qualys, afin de l'aider à déceler et à régler les problèmes de vulnérabilité de son infrastructure TI et de son application Web. Les clients peuvent, sur demande, obtenir le rapport des tests d'intrusion par un tiers et les rapports Qualys les plus récents.

Boréalis fait appel à des systèmes de gestion des vulnérabilités afin d'assurer la protection constante de son infrastructure TI contre les menaces liées au Web. Une application scrute l'espace Web afin de débusquer automatiquement les 10 menaces les plus courantes (OWASP top 10 risks) dont l'injection SQL, le cross-site scripting (XSS), le cross-site request forgery (CSRF) et la redirection URL.

Les applications, les réseaux et le matériel informatique sont sous constante surveillance par Boréalis et ses fournisseurs infrastructure-service (Infrastructure as-a-Service [IaaS]). Chaque ligne de code modifiée dans nos entrepôts de données est vérifiée par une deuxième personne et passe ensuite par plusieurs milliers de tests automatisés. Le système ESLint procède également à la vérification du code, tandis qu'une vérification des vulnérabilités des bibliothèques externes est effectuée à l'aide du système Yarn.

Infokit Boréalis Sécurité – Copyright © Borealis. Tous droits réservés – Février 2023

Technologies

L'application Boréalis fait appel aux plus récentes technologies ainsi qu'à leurs toutes dernières fonctionnalités afin de garantir un degré de sécurité élevé pour nos serveurs et régler rapidement tout problème de cet ordre. Boréalis veille également à effectuer la mise à jour régulière de ces technologies dont voici une liste non exhaustive :

- Apache2
- Docker
- Elasticsearch
- Node.js
- NginX
- MongoDB
- OpenSSL
- PostgreSQL
- React

Confidentialité

Boréalis comprend l'importance d'assurer la confidentialité de vos données. Pour plus d'information à ce sujet, veuillez consulter notre entente cadre intitulée Master Subscription Agreement (disponible uniquement en anglais) :

https://www.boreal-is.com/terms-of-use/

Certification et accréditation de sécurité Boréalis

Boréalis offre des solutions de sécurité conçues pour et utilisées par de nombreuses grandes entreprises. Boréalis veille également à satisfaire aux normes les plus élevées de l'industrie en matière de sécurité organisationnelle afin d'assurer la confidentialité, l'intégrité et la disponibilité des données de ses clients.

Sécurité Boréalis

Conformément à sa politique de sécurité et de durabilité, le service de sécurité Boréalis est situé dans un centre de données de niveau supérieur certifié selon les normes de l'industrie. Chaque année, un essai d'intrusion est effectué sur notre plateforme par une entreprise retenue à cette fin et notre sécurité interne est assurée par une série de politiques et de processus de protection des données.

Centre de données certifié de niveau 3 conforme à l'énoncé sur les normes pour les engagements d'attestation no 16 (SSAE 16)

Les services d'hébergement Boréalis sont offerts dans un centre de données certifié de niveau 3. La division Amazon Web Services (AWS), certifiée ISO 27001:2005, offre des services spécialisés à partir d'une infrastructure nuagique, le tout conformément aux normes de gestion de la sécurité et de l'évaluation du risque et processus associés ISO 27002 et ISO 27005. Amazon AWS dispose également des certifications pour conformité aux normes SOC 1 et 2 type II.

Pour plus d'information sur les certifications détenues par Amazon AWS, consultez :

https://aws.amazon.com/compliance/soc-faqs/

https://aws.amazon.com/compliance/iso-certified/

Infokit Boréalis Sécurité – Copyright © Boréalis. Tous droits réservés – Février 2023

Modalités de sécurité à la mise en marche du centre de données

Les services d'hébergement Boréalis sont offerts à partir des services pour entreprises de la division Amazon AWS, une infrastructure distribuée et évolutive. Boréalis assure la maîtrise de ses opérations en choisissant où les données du client seront hébergées. Cependant, s'il le désire, le client peut également déterminer lui-même le centre de production ou de réplication de ses données moyennant certains frais.

Sécurité du centre de traitement des données

Les serveurs de production Boréalis sont hébergés dans des centres de traitement des données certifiés de niveau 3 (certification de l'Uptime Institute). Ces établissements détiennent une certification ISO 27001: 2005, SOC 1 type II (SSAE 16 et ISAE 3402) de même que SOC 2 type II. Ils sont également dotés de solides dispositifs de sécurité d'accès physique (données biométriques et accès smart card) et de sécurité logique (pare-feu, détection des intrusions, surveillance vidéo et refus de service en cas d'attaque). L'alimentation, le refroidissement et le traitement par des réseaux diversifiés et redondants sont assurés selon la norme minimale N+1. Enfin, s'ils le désirent, les clients peuvent aussi demander l'auto-évaluation Cloud Security Alliance STAR offerte par Amazon : **https://cloudsecurityalliance.org/registry/amazon/**

Efficacité énergétique des centres de traitement des données

Amazon Web Services (AWS) s'est engagée à fonctionner de la manière la plus écologique possible et à exploiter son infrastructure avec de l'énergie entièrement renouvelable.

Une étude menée par le groupe 451 Research a démontré que l'infrastructure d'AWS est 3,6 fois plus efficace du point de vue énergétique que la moyenne des centres de traitement des données des États Unis. Plus des deux tiers de cette supériorité énergétique est attribuable au fait qu'AWS utilise de manière très intensive son parc de serveurs à haute efficacité énergétique.

AWS a aussi mis en place plusieurs initiatives visant à améliorer l'utilisation des ressources hydriques et à minimiser le recours aux sources d'eau potable pour refroidir les appareils des centres de données. De plus, AWS conçoit ses stratégies d'utilisation des ressources hydriques en fonction des tendances climatiques ainsi que de la disponibilité et de la gestion hydrique des endroits où se trouvent les centres de données, tout en limitant au maximum le recours aux sources d'eau potable.

Centres de données Amazon AWS

Pour plus d'information au sujet des centres de traitement des données, visitez le **https://aws.amazon.com/**

Infokit Boréalis Sécurité – Copyright © Borealis. Tous droits réservés – Février 2023

Infrastructure physique

Boréalis a choisi Amazon AWS à titre de principal fournisseur de services d'infogérence parce que l'entreprise dispose de certificats de sécurité de haut niveau. C'est toutefois l'équipe de Boréalis qui configure et gère elle-même son infrastructure, y compris les commutateurs de réseaux, les pare-feu, les serveurs et les dispositifs de stockage partagés. De plus, tous les services offerts par Boréalis sont configurés de manière à offrir une disponibilité maximale et à minimiser le plus possible les temps d'arrêt.

Sauvegarde des données

Une sauvegarde complète des données des serveurs virtuels est effectuée chaque jour. La politique de sauvegarde Boréalis est la suivante : conservation des données des sept derniers jours, des huit dernières semaines et des 12 derniers mois.

Reprise après sinistre

L'hébergement des données est effectué dans de nombreux centres afin d'offrir la redondance nécessaire au bon fonctionnement de l'application Boréalis. Ces centres sont dotés de dispositifs de sécurité physique, de politiques d'accès strictes de même que de chambres fortes et de cages sécurisées. Chaque serveur est répliqué en temps réel dans un autre centre de données situé dans la même zone géographique. Boréalis peut donc effectuer une réplication des données en temps réel entre le centre de production des données et le centre de reprise après sinistre. Des tests de reprise après sinistre à chaud ont lieu chaque jour, tandis qu'un diagnostic de reprise complète après sinistre est effectué à chaque trimestre afin de vérifier le temps de reprise estimé et l'intégrité des données des clients.

Sécurité des réseaux

Le réseau Boréalis est protégé par un pare-feu pour entreprise et un système de prévention et de détection d'intrusion (IPS/IDS) qui surveillent le trafic du réseau et qui sont en mesure de bloquer un grand nombre de vulnérabilités connues. Le réseau Amazon AWS est pour sa part protégé contre les attaques DoS/DDoS. Pour plus d'information, consultez le site https://aws.amazon.com/shield/ddos-attack-protection/

Transmission

Le réseau Amazon AWS permet l'accès à de nombreuses connexions simultanées qui offrent des fonctions de redondance de routage et de connectivité haute performance.

Sécurité des ressources humaines

Boréalis effectue une vérification des antécédents judiciaires de ses employés au moment de l'embauche et répète le processus tous les cinq ans.

Gestion des actifs

Boréalis procède à un inventaire automatique des appareils et des logiciels de son infrastructure TI grâce un outil spécial.

Gestion d'accès logique

Chaque utilisateur possède un compte assorti de certains droits d'accès et chacune des actions posées est surveillée et enregistrée à l'aide d'un sous-système SIEM (Security Information and Event Management).

Infokit Boréalis Sécurité – Copyright © Borealis. Tous droits réservés – Février 2023

Développement de logiciels

Our production environment is completely isolated from the development network on a network that is only accessible via VPN which has a 2-factor authentication. The production data is never used for testing and QA.

Mise à jour logicielle et de système

Tous nos postes de travail (ordinateurs de bureau et ordinateurs portables) sont dotés d'un antivirus automatiquement mis à jour, ce de manière régulière. Les mises à jour du système d'opération sont effectuées par GPO (Group Policy Objects) et sont automatiquement installées sur les postes de travail.

Confidentialité

La confidentialité est chose sérieuse chez Boréalis puisque les entreprises courent chaque jour le risque d'une intrusion en provenance de n'importe où dans le monde. L'enjeu est donc grand et il va de la préservation de données sensibles pour l'industrie à la confiance de la clientèle, qui comme on le sait est toujours fragile. Une fuite de données clients diffusée par les médias peut même, on l'a déjà vu, entraîner la faillite d'une entreprise.

C'est pourquoi, contrairement à bien d'autres, Boréalis intègre la notion de confidentialité à toutes les étapes du développement logiciel et de son cycle de vie. Pour plus d'information à ce sujet, visitez le **https://media.boreal-is.com/borealis-software-lifecycle-FR.pdf**

Se préoccuper de confidentialité, de conformité et de sécurité des données après les faits peut augmenter sensiblement le coût de mise en place des mesures d'atténuation du risque. C'est pourquoi, chez Boréalis, nous nous tenons compte de ces questions dès l'étape de la conception logicielle et nous veillons à effectuer régulièrement les mises à jour qui s'imposent.

Les exigences en matière de confidentialité font partie intégrante des mesures en place dans nos centres d'hébergement. Si un client le demande, nous pouvons également travailler de concert avec lui, moyennant une entente contractuelle, afin de lui permettre de satisfaire aux exigences qui lui sont propres. Nous pourrons ainsi accueillir les données du client dans le centre de données de son choix, dans le pays de son choix. Pour plus d'information sur la politique de confidentialité Boréalis, visitez le **https://www.borealis.com/privacy-policy/**

Infokit Boréalis Sécurité – Copyright © Borealis. Tous droits réservés – Février 2023

Êtes-vous prêt à simplifier vos opérations ?

NOUS SOMMES PRÊTS

À VOUS AIDER.

+ 1 819 575-6037

contact-us@boreal-is.com

/borealiscsr/

boreal-is.com

Borealis

@BorealisCSR/