

ÉVALUATION DE LA SÉCURITÉ DE CONSIGNO CLOUD



Toute organisation qui opte pour une solution de signature électronique doit s'assurer que cette dernière est basée sur des politiques rigoureuses. Des mesures de sécurité liées à la collecte de données et aux politiques de confidentialité de l'organisation doivent être

prises en place de façon approfondie. Vous trouverez ci-dessous, sous forme de questions-réponses, quelques précisions techniques quant à la sécurité de notre plateforme de signature électronique ConsignO Cloud.

QUESTIONS TECHNIQUES SUR LA SÉCURITÉ

① OÙ LES DONNÉES OU LES SYSTÈMES, Y COMPRIS LES SAUVEGARDES, SERONT-ILS HÉBERGÉS?

Toutes les infrastructures utilisées pour exploiter la plateforme ConsignO Cloud, y compris le stockage des documents, sont situées à Toronto et à Montréal (Canada).

② OÙ LE CENTRE INFORMATIQUE DE SECOURS DE LA SOLUTION HÉBERGÉE EST-IL SITUÉ?

ConsignO Cloud est dotée d'une architecture à haute disponibilité et d'une configuration active-active. Si un site devait tomber en panne, la charge serait automatiquement transférée à l'autre site. Nos deux sites actifs sont situés à Toronto et à Montréal. Notre site de sauvegarde chiffrée hors ligne est également situé à Montréal.

③ DESCRIPTION DE L'INFRASTRUCTURE HÉBERGÉE : TYPES DE SERVEUR, SYSTÈMES DE STOCKAGE, RÉSEAU DE COMMUTATION, ETC.

Les ressources qu'utilise Notarius sont dans des centres de données situés au Canada. Tout le matériel hébergeant l'infrastructure est dans le nuage, à l'exception des modules de sécurité matériels. Les modules de sécurité matériels sont situés dans les locaux de Notarius, au Québec, et comprennent un commutateur double, un pare-feu double et un double fournisseur d'accès à internet (FAI).

④ QUEL TYPE DE BASCULEMENT EST UTILISÉ POUR LA REDONDANCE (À HAUTE DISPONIBILITÉ OU BASCULEMENT MANUEL, DÉLAIS DE RÉTABLISSEMENT PRÉVUS, ETC.)?

Toutes les instances utilisent une haute disponibilité et leur charge est équilibrée dans divers sites au Canada. Chaque site est connecté par l'entremise d'un réseau privé virtuel à équilibrage de charge sur place.

5 QUELLE EST LA STRATÉGIE DE SAUVEGARDE QUOTIDIENNE, ET CETTE SAUVEGARDE SE FAIT-ELLE HORS SITE?

Notarius effectue la sauvegarde des données de ConsignO Cloud aux 6 heures, tous les jours. Les sauvegardes sont stockées dans nos locaux, au Canada. Les sauvegardes hors ligne hebdomadaires sont stockées à Montréal (Canada).

6 LES DONNÉES SUR LES SERVEURS HÉBERGÉS SONT-ELLES CHIFFRÉES, ET SI OUI, DE QUEL TYPE DE CHIFFREMENT S'AGIT-IL?

Toutes les données inactives des utilisateurs sont chiffrées dans la base de données à l'aide du chiffrement AES256-CBC.

7 QUEL TYPE DE CHIFFREMENT EST UTILISÉ POUR LA TRANSMISSION D'INFORMATIONS VERS ET DEPUIS L'ENVIRONNEMENT HÉBERGÉ?

Toutes les communications sont chiffrées. Les sessions utilisateurs sont protégées par le protocole de sécurité TLS du navigateur, et la communication entre les deux sites est chiffrée par l'entremise d'un réseau privé virtuel IPsec.

8 COMMENT LE CONTRÔLE D'ACCÈS EST-IL GÉRÉ? QUELS SONT LES PROCESSUS ET LES PROCÉDURES EN PLACE POUR L'AUTORISATION, LA CRÉATION, L'OCTROI, LE RETRAIT ET LA DÉSACTIVATION DE COMPTES UTILISATEURS ET/OU DE PRIVILÈGES D'ACCÈS?

Notarius est certifiée ISO 27001 et ETSI 319 411 (eIDAS); toute la gestion et tous les processus liés au contrôle d'accès font l'objet de contrôles stricts. Les demandes, les autorisations et les opérations sont effectuées par des employés distincts, suivant un principe rigoureux de séparation des tâches.

9 QUI A ACCÈS AUX DONNÉES ET/OU AUX SYSTÈMES, QUEL EST LEUR NIVEAU D'ACCÈS ET D'OÙ EXPLOITENT-ILS L'INFRASTRUCTURE?

Seuls les administrateurs de système ont accès à l'environnement de production. Tous les administrateurs sont des employés à temps plein de Solutions Notarius, et tous sont situés et travaillent au Canada.

10 LES EMPLOYÉS QUI ONT ACCÈS AUX CLÉS DE CHIFFREMENT ONT-ILS FAIT L'OBJET DE VÉRIFICATIONS DE SÉCURITÉ, TELLES UNE VÉRIFICATION DES RÉFÉRENCES, UNE VÉRIFICATION DES ANTÉCÉDENTS ET UNE VÉRIFICATION DU CASIER JUDICIAIRE, AVANT LEUR EMBAUCHE?

Notarius est certifiée ISO 27001 et ETSI 319 411 (eIDAS); tous les employés de Solutions Notarius sont soumis à des vérifications de sécurité à l'embauche, puis aux deux ans.

11 QUELLES SONT VOS POLITIQUES CONCERNANT LE TÉLÉCHARGEMENT OU LA SAUVEGARDE D'INFORMATION DEPUIS UN SERVEUR STOCKANT DES DONNÉES CLIENTS, Y COMPRIS LE TÉLÉCHARGEMENT DE DONNÉES HORS SITE?

Utilisateurs clients authentifiés : Ces utilisateurs peuvent télécharger les documents signés et les journaux d'audit.

Signataires : Les signataires peuvent télécharger les documents à signer et les documents qu'ils ont déjà signés.

Notarius : Les sauvegardes chiffrées sont entreposées dans un périmètre de sécurité. Les sauvegardes chiffrées hors ligne hebdomadaires sont stockées dans un endroit sécurisé.

12 EST-CE QUE LES DONNÉES DES CLIENTS SONT ACCESSIBLES À L'EXTÉRIEUR DU CANADA, ET SI OUI, LEUR TÉLÉCHARGEMENT EST-IL RESTREINT?

ConsignO Cloud est une solution web accessible de partout, à condition que l'utilisateur ou le signataire puisse ouvrir une session à l'aide d'une authentification à double facteur. Voir la question 11 concernant la politique de téléchargement. Puisque la géolocalisation peut être truquée facilement à l'aide de réseaux privés virtuels et de serveurs mandataires, la restriction est basée sur une authentification à facteurs multiples.

13 COMMENT LES SYSTÈMES SONT-ILS ADMINISTRÉS, LES JOURNAUX D'AUDIT DEMEURENT-ILS ACCESSIBLES, ET SI OUI, PENDANT COMBIEN DE TEMPS? LE DROIT D'ACCÈS MINIMAL EST-IL UTILISÉ POUR LES ADMINISTRATEURS?

Notarius est certifiée ISO 27001 et ETSI 319 411 (eIDAS); tous les journaux d'audit sont rigoureusement examinés par des vérificateurs internes à chaque trimestre et par des vérificateurs externes tous les ans. Notarius suit toujours le principe du droit d'accès minimal, surtout pour les administrateurs de système, lorsque cela est possible.

14 QUELLES SONT LES GARANTIES EN MATIÈRE DE NIVEAU DE SERVICE DISPONIBLE (TEMPS DE DISPONIBILITÉ)?

99,5 %

15 QUELLES SONT VOS PROCÉDURES DE CONTRÔLE DES CHANGEMENTS?

Notarius est certifiée ISO 27001 et ETSI 319 411 (eIDAS); tous les changements font l'objet de contrôles stricts. Les demandes, les autorisations et les opérations sont effectuées par des employés distincts, suivant un principe rigoureux de séparation des tâches. Des procédures strictes doivent être suivies.

16 AVEZ-VOUS UN PLAN D'INTERVENTION EN CAS D'INCIDENT ET QUELLE EST VOTRE CLASSIFICATION DES INCIDENTS?

Notarius est certifiée ISO 27001 et ETSI 319 411 (eIDAS); tous les incidents font l'objet d'un suivi et sont classifiés en fonction de leur impact sur la disponibilité, l'intégrité et la confidentialité. Le plan d'intervention est alors ajusté ou un nouveau plan est créé afin de réduire les risques.

17 QUELLE PROTECTION UTILISEZ-VOUS CONTRE LES LOGICIELS MALVEILLANTS?

Notarius utilise la plus récente version du logiciel de protection pour entreprises Symantec sur chaque serveur et ordinateur utilisateur, et des balayages externes sont effectués toutes les semaines à l'aide de la plateforme Warden de Delve Labs.

18 QUELS TYPE ET NIVEAU DE PROTECTION PARE-FEU UTILISEZ-VOUS?

Un pare-feu privé virtuel est utilisé et peut atteindre la 5e couche du modèle OSI. La liste des droits d'accès du pare-feu est basée sur l'adresse IP, le port, la session, les applications et les utilisateurs.

19 COMMENT LES DONNÉES SONT-ELLES SUPPRIMÉES? QUEL EST LE DÉLAI?

Tous les documents téléversés dans ConsignO Cloud sont supprimés à l'expiration du projet ou à la demande de l'utilisateur depuis l'interface web ou l'API. Des sauvegardes sur place et externes sont conservées jusqu'à un an.

20 RÉPONDEZ-VOUS AUX NORMES DE SÉCURITÉ SUR LES DONNÉES DE L'INDUSTRIE DES CARTES DE PAIEMENT (PCI), LE CAS ÉCHÉANT?

Toutes les informations relatives aux cartes de crédit sont entrées sur la page de notre commerçant; les numéros de carte de crédit ne transitent pas par nos systèmes. Notre commerçant de paiement est certifié PCI.

21 VOICI, EN GUISE DE RÉFÉRENCES, QUELQUES ORGANISATIONS QUI UTILISENT CES SERVICES :

Barreau du Québec

Université de Montréal

Office des professions du Québec

Réseaux Agriconseils

Tribunal administratif des marchés financiers

Association des municipalités de l'Ontario (AMO)

Ville de Vaudreuil-Dorion

Ville de Drummondville

Qui est Notarius

Expert en signature numérique et électronique ainsi qu'en fiabilité à long terme des documents électroniques depuis 1998, Notarius est la seule entreprise canadienne à émettre des signatures de confiance reconnues par Adobe (Adobe Approved Trust List – AATL) et eIDAS (electronic IDentification Authentication and trust Services). Notarius est également une entreprise écoresponsable certifiée carboneutre, ISO 27001 et ISO 9001. Les signatures numériques de Notarius permettent de créer des documents qui constituent des preuves, et non de simples commencements de preuve, au sens des lois en vigueur au Canada.

Expertise

Notarius a contribué à la transformation numérique de certaines d'organisations en aidant les professionnels à adopter des pratiques 100 % numériques et conformes aux exigences de leur ordre ou de leur association. Nos produits permettent à des milliers de professionnels, de cadres, d'employés, de clients et de partenaires de signer annuellement des millions de documents reconnus au plan juridique. Notarius possède une solide feuille de route dans le développement de solutions respectant les plus hautes exigences de sécurité et de confidentialité.

Environnement

En plus de réduire les coûts de gestion et d'améliorer la productivité, les signatures numériques et électroniques permettent d'adopter une approche « sans papier » et de réduire l'empreinte environnementale de façon significative.



Pour plus d'information

notarius.com | 1 888 588-0011 | info@notarius.com



Transformation numérique.
Documents juridiquement fiables.