Politique de sécurité

Signatures électroniques eZsign

ezsign

Introduction

La sécurité a toujours été une préoccupation dans le monde des affaires. À l'heure du numérique, la sécurité des renseignements occupe une place centrale dans toutes les entreprises, y compris la nôtre.

Nous savons à quel point les processus opérationnels qui donnent lieu à des signatures électroniques sont sensibles. Les documents qui exigent des signatures électroniques contiennent souvent des renseignements névralgiques ou confidentiels, comme des renseignements personnels, des secrets professionnels, des renseignements commerciaux ou financiers, des renseignements médicaux, et plus encore. Lorsqu'il s'agit de traiter des documents qui exigent des signatures électroniques, la sécurité, la conformité et la confidentialité sont essentielles. Prendre des risques n'est pas envisageable.

En tant que spécialiste en solutions informatiques et fournisseur de solutions logicielles de confiance depuis 2005, nous sommes conscients qu'il peut être difficile pour les entreprises de garantir la sécurité de leur infrastructure et des données. Il est essentiel de faire équipe avec un partenaire de solutions de signature électronique sur lequel on peut compter. La sécurité est dans l'ADN d'eZsign. Elle fait partie intégrante de nos activités commerciales, c'est pourquoi nous avons créé la présente politique de sécurité. Lorsque vous travaillez avec eZsign, vous avez l'assurance que vos données sont entre les mains d'un partenaire qui prend la sécurité au sérieux. Nous suivons les meilleures façons de faire en matière de sécurité et de conformité, comparables à celles adoptées par les plus grandes entreprises et les institutions financières les plus fiables. Notre réputation et notre parcours parlent d'eux-mêmes.

Dans les sections suivantes, vous lirez au sujet de l'importance que nous accordons à la sécurité dans nos opérations, des règlements et des normes auxquels nous adhérons, de l'importance de la confidentialité et de notre plan d'action dans l'éventualité improbable d'un incident :

Sécurité

Nous sommes fermement déterminés à protéger vos documents et vos données. Dès le départ, nous avons conçu et créé notre solution eZsign en accordant la priorité à la sécurité. Nous favorisons l'instauration d'une culture de la sécurité dans tout ce que nous faisons, de la conception de nos logiciels à nos opérations quotidiennes et notre service à la clientèle. Cette culture transparaît dans quatre domaines clés qui se recoupent : notre équipe de gestion, nos employés, nos processus et notre infrastructure.

Notre équipe de gestion

Notre équipe de gestion a rédigé la présente politique de sécurité pour intégrer la sécurité dans la structure même de notre entreprise. Pour voir à son respect, la direction a également préparé une série d'audits et contrôles pour vérifier si nous respectons les règlements et les procédures. Notre équipe de direction est l'ultime responsable de la sécurité de nos renseignements et de l'application de cette politique. En plus de la sécurité, la direction est guidée par sa recherche de la qualité et est déterminée à surpasser les attentes de la clientèle. Ces pratiques ne sont pas seulement bonnes pour nos clients, elles sont également bonnes pour les affaires.

Nous avons formulé et adopté la présente politique avec les objectifs suivants :

1. Créer un système de règles pour encadrer notre sécurité des TI.
2. Voir à ce que nos employés et l'entreprise dans son ensemble se comportent selon nos attentes et dans le respect de toutes les lois et règles applicables.
3. Veiller à ce que nos systèmes, notre matériel informatique et nos ressources soient utilisés correctement afin de mener nos activités de façon conforme à notre mission et qui protège, met en valeur et promeut notre image et notre réputation de manière continue.
4. Offrir, favoriser et maintenir un milieu de travail sécuritaire et confortable où les droits collectifs et individuels sont respectés.
5. Encourager les gens qui relèvent de la présente politique à contribuer de façon positive à notre façon de voir, de planifier et d'exécuter nos activités.
6. Mettre à la disposition des personnes qui relèvent de la présente politique des ressources et des outils qui les aident à exécuter leurs rôles, faire leur travail et assumer leurs obligations.

Nos employés

Même si notre équipe de direction est l'ultime responsable de la sécurité d'eZsign, tout le monde chez eZsign joue un rôle clé. Chaque employé d'eZsign voit en tout temps à la sécurité de nos données et celles de nos clients. À cette fin, nous procédons à une vérification rigoureuse des antécédents avant chaque embauche, et tous les employés d'eZsign adhèrent à un code de conduite strict sur la sécurité et signent une entente de confidentialité avant de se joindre à l'entreprise. Nous utilisons des codes d'accès pour restreindre et surveiller l'accès du personnel afin de protéger notre infrastructure matérielle et les données qu'elle contient.

Tous les programmeurs d'eZsign et toute l'équipe informatique participent régulièrement à des formations sur la sécurité afin de veiller à ce que leurs connaissances des dernières tendances en matière de technologie de la sécurité soient à jour ainsi que leurs compétences. Nous abordons également la sécurité à chaque réunion de l'équipe eZsign.

Chaque employé est tenu d'informer sans tarder son supérieur immédiat s'il constate que des renseignements de nature délicate transmis lors de l'utilisation d'eZsign ont été compromis ou s'il est témoin d'un incident ou d'une situation qui pourrait constituer un risque d'atteinte à la sécurité ou compromettre la confidentialité de renseignements confidentiels qui sont sous notre responsabilité.

Nos processus

Nous sommes résolus à prendre des mesures et à mettre en place les mesures de sécurité nécessaires pour protéger la confidentialité, l'intégrité et l'accessibilité des actifs numériques de notre clientèle. Pour y arriver, nous faisons appel aux meilleures techniques de cryptage de l'industrie pour tous les documents et les données qui sont transmis ou stockés à l'aide d'eZsign. Nous avons mis au point des mécanismes de contrôle d'accès et d'authentification des utilisateurs ainsi que des mécanismes pour garantir la continuité des affaires dans l'éventualité d'un incident. Ces mesures sont proportionnelles à la nature délicate des données, à leur utilisation, à leur quantité et à leur format.

Nos processus doivent aider à prévenir les incidents et les failles de sécurité, les erreurs, les actes malveillants et la divulgation non autorisée ou la destruction de renseignements. Tous nos processus d'affaires prévoient des éléments à cet égard.

Nous avons intégré la sécurité à chaque étape du cycle de vie du développement logiciel (CVDL) et l'évaluons régulièrement pour assurer la sécurité de notre produit. Nous effectuons des tests de sécurité dans les environnements suivants :

- Développement (Dév)
- Assurance qualité (AQ)
- Préproduction (Préprod)
- Production (Prod)

Par ailleurs, nous employons les pratiques DevOps comme l'intégration continue/déploiement continue (CI/CD) et l'infrastructure en tant que code (IaC) qui nous permettent de surveiller la sécurité à chaque étape du processus. Nous avons une équipe consacrée à la sécurité qui mène régulièrement des vérifications de la sécurité des données, de la sécurité matérielle et du risque fournisseur dans le cadre des processus de développement et indépendamment de ceux-ci. Ces vérifications sont réalisées au moins deux fois par année.

Nous produisons et stockons des rapports d'activité sur la sécurité et des journaux des événements de sécurité pour tous les systèmes et données névralgiques. Nous suivons également toutes les activités liées à eZsign, sans égard à la provenance de l'activité, et nous produisons et stockons les journaux d'activités importants :

- Activité Web
- Activité liée aux courriels
- Activité liée au serveur de fichiers
- Gestion des clés
- Activité liée au réseau privé virtuel (RPV)
- Connexion à l'application eZsign

Notre infrastructure

Mesures de protection de la sécurité de l'infrastructure matérielle

Les locaux où sont stockées les données d'eZsign sont protégés 24 h sur 24, 7 jours sur 7. Les données sont hébergées dans des centres de données possédant les certifications SOC 1, SOC 2, SOC 3 et ISO 27001. Les accès aux installations sont surveillés et l'accès est restreint aux personnes autorisées.

Nous utilisons les applications et l'équipement les plus récents pour que l'accès à notre environnement de développement et de production soit restreint aux employés qui sont autorisés et dûment formés, pour prévenir ainsi l'accès aux personnes non autorisées et malveillantes.

Transmission et stockage des données

Nous savons que vos données sont précieuses, c'est pourquoi nous prenons toutes les précautions possibles pour les protéger. Nous utilisons les normes de cryptage qui rivalisent avec celles des banques et institutions financières les plus respectées au monde pour empêcher qu'une autre personne que vous accède à vos renseignements confidentiels. L'application eZsign utilise le cryptage de bout en bout, ce qui signifie que nous prenons en charge la chaîne entière de cryptage de votre appareil à nos serveurs.

Mécanismes de sécurité en place :

1. HTTPS: TLS 1.2, RSA-AES128-GCM-SHA256, clés de 128 bits
2. Stockage de fichiers et serveurs de données (données entreposées) : norme de cryptage AES256
3. Horodatage certifié émis par un service d'horodatage certifié en conformité avec le protocole d'horodatage RFC 3161
4. Serveur OCSP intégré selon les normes RFC 2560 et RFC 6960
5. Module de sécurité matérielle conforme à la norme FIPS 140-2

Infrastructure infonuagique

eZsign utilise Amazon Web Services (AWS), un modèle d'excellence en matière d'infrastructure infonuagique sûre, complète et fiable. En ayant AWS comme plateforme informatique en nuage, vous avez accès à vos documents, même s'il y a une interruption d'activité régionale ou une panne du centre de données.

- Architecture hautement disponible et redondante qui permet au système complet de tolérer une panne complète du site et de continuer de fonctionner
- Multiples zones de disponibilité
- Conteneurs Docker
- Reproduction des données en temps réel (Real-Time data replication)
- Zones DNS reproduites dans près de 60 régions dans le monde (global DNS)
- Réseau mondial de diffusion du contenu (CDN)
- Pare-feu et système de détection des intrusions pour prévenir et repérer les attaques

Grâce à toutes les mesures que nous avons instaurées, notre accord sur les niveaux de service (ANS) font état d'une durabilité annuelle des données de 99,999999999 % et d'une disponibilité des applications de 99,99 %.

Conformité

Compte tenu de la popularité des signatures électroniques aujourd'hui et de leur importance dans les transactions et les processus d'affaires partout dans le monde, il existe une mosaïque de règles et normes cruciales qui visent à assurer la conformité des signatures électroniques à l'échelle de la planète. Chez eZsign, nous faisons bien plus que de simplement respecter les normes de l'industrie et les règles relatives à la signature électronique et à la cybersécurité : nous allons au-delà de notre devoir pour toujours avoir une longueur d'avance dans notre façon de gérer notre réseau et de protéger vos données. Nous sommes constamment à l'affût des connaissances du marché pour garantir que nos processus, nos systèmes et notre approche respectent les normes internationales les plus strictes, surtout que ces normes changent et évoluent pour tenir compte des nouvelles réalités technologiques et commerciales.

En plus de la vérification régulière des risques virtuels et physiques, notre équipe de la sécurité procède également à la vérification de la conformité avec les lois et les normes internationales sur la cybersécurité. Cette détermination à respecter les lois, les règles et les normes internationales nous permet de garantir que les signatures eZsign apposées sur les documents de nos clients sont exécutoires et non répudiables, peu importe qui les a signés.

Ci-après, nous présentons les caractéristiques uniques des signatures eZsign qui garantissent leur conformité avec toutes les lois en vigueur dans le monde entier.

Propriétés des signatures

- eZsign prend en charge les formats de signature électronique les plus récents, notamment le format PDF 2.0, conformément aux normes ISO 32000-2 et PAdES requises par le règlement eIDAS de l'Union Européenne
- eZsign applique les signatures PDF qui peuvent être validées au moyen d'Adobe Reader, Adobe Acrobat, ou tout autre programme de validation qui prend en charge les signatures PDF
- L'information de validation est stockée directement dans la signature en conformité avec la norme ISO 32000-1 ou dans un système de stockage des documents sécurisé (DSS) précisé dans la norme ISO 32000-2 et à la partie 4 de PAdES
- Les signatures sont sauvegardées de manière incrémentale pour préserver les signatures et la structure du document

eZsign prend en charge toutes les versions et normes PDF pertinentes

- eZsign prend en charge toutes les versions PDF jusqu'à PDF 1.7 (ISO 32000-1), y compris les extensions niveau 8 et PDF 2.0 (ISO 32000-2)

- eZsign est au fait des normes d'archivage PDF/A-1/2/3 (ISO 19005) : si le document d'entrée est conforme à PDF/A, le document de sortie le sera également. eZsign prend totalement en charge les schémas d'extension XMP requis par PDF/A. La capacité d'insérer des métadonnées XMP conformes à PDF/A dans des documents PDF est un avantage important d'eZsign

Caractéristiques de signature

- Validation à long terme des signatures électroniques (LTV) selon la norme PDF 2.0 (ISO 32000-2)
- PAdES (ETSI TS 102 778 parties 2, 3, et 4, ETSI EN 319 142) et CAdES (ETSI TS 101 733) pour les signatures qualifiées au sens du règlement eIDAS
- Signatures assurant la validité à long terme (LTV) et l'intégrité du document (B-LTA) pour veiller à la conformité avec eIDAS
- eZsign récupère un horodatage émis par un service d'horodatage certifié (TSA) en conformité avec la norme RFC 3161, RFC 5816 et ETSI EN 319 422 et l'intègre dans la signature qu'elle génère
- eZsign crée des signatures assorties d'un horodatage qui respectent les normes ISO 32000-2 et PAdES partie 4

Détails sur la signature cryptographique

- Algorithme de signature RSA
- Authentification forte et fonctions de hachage
- Chaîne de certificats totalement intégrée dans les signatures générées, ce qui signifie que les signatures assorties de certificats provenant d'une autorité de certification (CA) qui figure à la liste Adobe Approved Trust List (AATL) peuvent être validées dans Adobe Acrobat et Adobe Reader sans configuration de la part du client
- Réponses du protocole de vérification de certificat en ligne intégrées (OCSP conformément aux RFC 2560 et 6960) et listes de révocation des certificats (CRL conformément à RFC 3280) comme information de révocation pour la validation à long terme (LTV)

Notre solution répond aux exigences suivantes en matière de sécurité et de conformité :

Electronic Signatures in Global and National Commerce Act (E-Sign Act)

La *Electronic Signatures in Global and National Commerce Act (E-Sign Act)* est une loi fédérale adoptée aux États-Unis en 2000 qui autorise l'utilisation de documents et de signatures électroniques dans les transactions commerciales. Elle permet aux organismes d'adopter un processus uniforme de signature électronique dans les 50 états avec la certitude que ces documents ne seront pas refusés par un tribunal au motif qu'ils ont été signés de façon électronique.

ISO 32000-2

La norme ISO 32000-2:2017 précise une forme numérique pour représenter les documents électroniques afin de permettre aux utilisateurs d'échanger et de visualiser des documents électroniques, peu importe l'environnement dans lequel ils ont été créés ou l'environnement dans lequel ils sont affichés ou imprimés.

ETSI TS 102 778-1

La spécification technique ETSI TS 102 778-1 précise l'utilisation des signatures PDF, décrites dans ISO 32000-1 et basées sur la syntaxe de message cryptographique [i.3], dans tous les domaines d'application où le PDF est le format approprié pour l'échange de documents numériques.

Uniform Electronic Transactions Act (UETA)

Comme la *E-Sign Act, la Uniform Electronic Transactions Act* (UETA) est une loi américaine adoptée pour assurer la validité des contrats électroniques et la légitimité des signatures électroniques. L'UETA donne aux états un cadre pour déterminer la légalité d'une signature électronique dans les transactions commerciales et gouvernementales.

Conformité avec les lois internationales, fédérales et provinciales

Alors qu'il existe des normes comme SOC ou ISO pour certifier les processus des institutions et pour établir leur conformité, il n'existe aucune certification officielle à proprement dit pour les entreprises ou les clients leur permettant de prouver leur conformité avec les lois internationales, fédérales ou provinciales. Il appartient aux clients de vérifier si leur utilisation des données est conforme à ces lois, et nos clients peuvent être certains que lorsqu'ils utilisent eZsign, ils respectent toutes les obligations légales qui leur incombent en vertu des lois suivantes :

Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)

Une loi fédérale canadienne qui vise à favoriser et encourager le commerce électronique en protégeant les renseignements personnels recueillis, utilisés ou communiqués dans certaines circonstances en prévoyant l'utilisation de moyens électroniques pour communiquer ou enregistrer des renseignements ou des transactions et en modifiant la Loi sur la preuve du Canada, la Loi sur les textes réglementaires et la Loi sur la révision des lois.

Freedom of Information and Protection of Privacy Act (FOIPPA)

Une loi de la Colombie-Britannique sur le droit à l'information qui octroie à une personne le droit légal d'accéder aux dossiers d'organismes publics provinciaux, sous réserve d'exceptions précises et limitées. Cette loi exige également que les organismes publics protègent la confidentialité des renseignements personnels d'une personne contenus dans les dossiers tenus par des organismes publics.

Loi sur la protection des renseignements personnels sur la santé (LPRPS)

Une loi de la province de l'Ontario qui fixe les règles concernant la collecte, l'utilisation et la

communication de renseignements personnels sur la santé. Ces règles s'appliquent à tous les dépositaires de renseignements sur la santé dans la province et aux personnes et aux organismes qui reçoivent des renseignements personnels de la part de dépositaires de renseignements sur la santé.

Health Insurance Portability and Accountability Act de 1996 (HIPAA)
Une loi fédérale américaine qui énonce les exigences en matière de gestion, stockage et transmission des renseignements protégés sur la santé en format matériel et numérique.

Centres de données

Les données d'eZsign sont hébergées dans plusieurs centres de données d'Amazon Web Services, ce qui signifie pour nos clients un accès supérieur et une meilleure disponibilité. Nous travaillons avec AWS, un chef de file des solutions d'infrastructures infonuagiques, en raison de son excellent dossier sur le plan de la conformité et de ses contrôles rigoureux. Selon vos besoins, nous vous garantissons que vos données seront hébergées en sol canadien, américain ou européen.

Voir les homologations d'AWS

Confidentialité

Le respect de la vie privée est primordial chez eZsign, c'est pourquoi notre priorité absolue est de préserver la confidentialité de vos données. Nous savons que lorsque nos clients utilisent eZsign, ils communiquent souvent des renseignements très sensibles et confidentiels, y compris des renseignements personnels recueillis et stockés dans le cadre de leurs activités d'affaires courantes. Sachant cela, il est de notre devoir de veiller à la protection de vos renseignements personnels.

Nous savons qu'en vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé*, les utilisateurs ou propriétaires de données conservent les droits exclusifs sur leurs renseignements confidentiels et peuvent par conséquent demander en tout temps de consulter des documents qui contiennent leurs renseignements personnels. Nous savons que nos utilisateurs subiraient des préjudices importants si leurs renseignements personnels étaient divulgués sans autorisation.

Par conséquent, nous nous engageons à prendre toutes les mesures nécessaires pour préserver la confidentialité de tous les renseignements personnels :

1. Nous employons les pratiques exemplaires de l'industrie pour préserver la confidentialité des codes utilisateurs, des mots de passe et des clés de cryptage.

2. Toute personne qui dans l'exercice de ses fonctions est appelée à traiter des renseignements de nature confidentielle est tenue de signer une entente de confidentialité. Nous demandons également à ces personnes de signer une entente qui les oblige à respecter toutes les mesures de sécurité nécessaires pour faire en sorte qu'elles soient les seules à avoir accès aux renseignements confidentiels et pour limiter le transfert ou la divulgation de ces renseignements. Tous les candidats doivent signer ces ententes avant de se joindre à l'entreprise.

3. Nous utilisons les renseignements confidentiels uniquement aux fins auxquelles ils ont été fournis.

4. Nous travaillons avec les utilisateurs, et, le cas échéant, avec leurs clients finaux, pour permettre aux personnes visées d'exercer leur droit à consulter, corriger ou modifier leurs renseignements personnels.

5. Nous travaillons avec les utilisateurs pour détruire les renseignements personnels et les profils d'utilisateurs en conformité avec les calendriers de rétention applicables.

6. Nous coopérons aux enquêtes et aux vérifications pour préserver la confidentialité des renseignements personnels ou confidentiels.

Plan d'action en cas d'incident

Échouer dans la planification, c'est planifier son échec. Nous nous efforçons de préserver la sécurité de notre infrastructure de TI et des données de nos clients tout en étant conscients que nous ne sommes pas à l'abri d'un incident. Pour cette raison, nous avons préparé un plan d'action détaillé en cas d'incident dans l'éventualité improbable d'une atteinte à la sécurité. Advenant un incident, nous informerons les utilisateurs dans les 24 heures de tout accès ou tentative d'accès à leurs renseignements personnels sans autorisation, ou d'une fuite de données ou de tout autre incident qui pourrait avoir des répercussions sur la sécurité ou la confidentialité des données.

Nous sommes résolus à agir pour atténuer le risque de fuites continuelles de données dans les plus brefs délais, de faire enquête pour cerner les vulnérabilités et d'adopter les mesures correctrices nécessaires afin de prévenir tout nouvel incident. Les membres de l'équipe d'intervention se concerteront pour évaluer et gérer la situation afin de réduire le risque et identifier les intervenants appropriés selon le niveau de risque.

Même si jusqu'ici, nous n'avons jamais vécu d'atteinte à la protection des données chez eZsign, nous reconnaissons que chaque incident est unique. Le but ultime d'un plan d'action en cas d'incident est de protéger les données de nos clients et de respecter toutes les exigences légales et réglementaires. Vous trouverez ci-après un aperçu de notre plan d'action en cas d'incident, qui compte trois étapes : détection et analyse, colmatage et restauration, et amélioration.

Détection et analyse

- Identifier l'incident ou l'infraction et vérifier si c'est en cours. Avant d'intervenir, voir à ce que toute brèche ait été colmatée.
- Lorsqu'un incident est signalé, un membre compétent de l'équipe d'intervention sur appel examine les faits.
- Déterminer quelles parties du système sont touchées et les isoler.
- Analyser tous les journaux de vérification pour déterminer si des données sont compromises, et si c'est le cas, déterminer lesquelles.
- Au besoin, le membre de l'équipe amorce l'étape de colmatage et de restauration.

Colmatage et restauration

- Concentrer les efforts pour trouver la cause de l'incident.
- Utiliser les journaux de vérification pour déterminer la portée de l'incident.
- Prendre les mesures nécessaires pour réparer le point d'entrée, éliminer la cause de l'incident et restaurer les systèmes.
- Limiter les répercussions de l'incident.

Amélioration

- Analyser l'incident pour récolter des éléments nouveaux afin d'améliorer les outils et les processus.
- Instaurer les mesures de correction nécessaires.
- Documenter toutes les modifications et améliorations.

1-844-EZSIGN2 (1-844-397-4642)

info@ezsign.ca