ILLUXI

POLITIQUE DE SÉCURITÉ

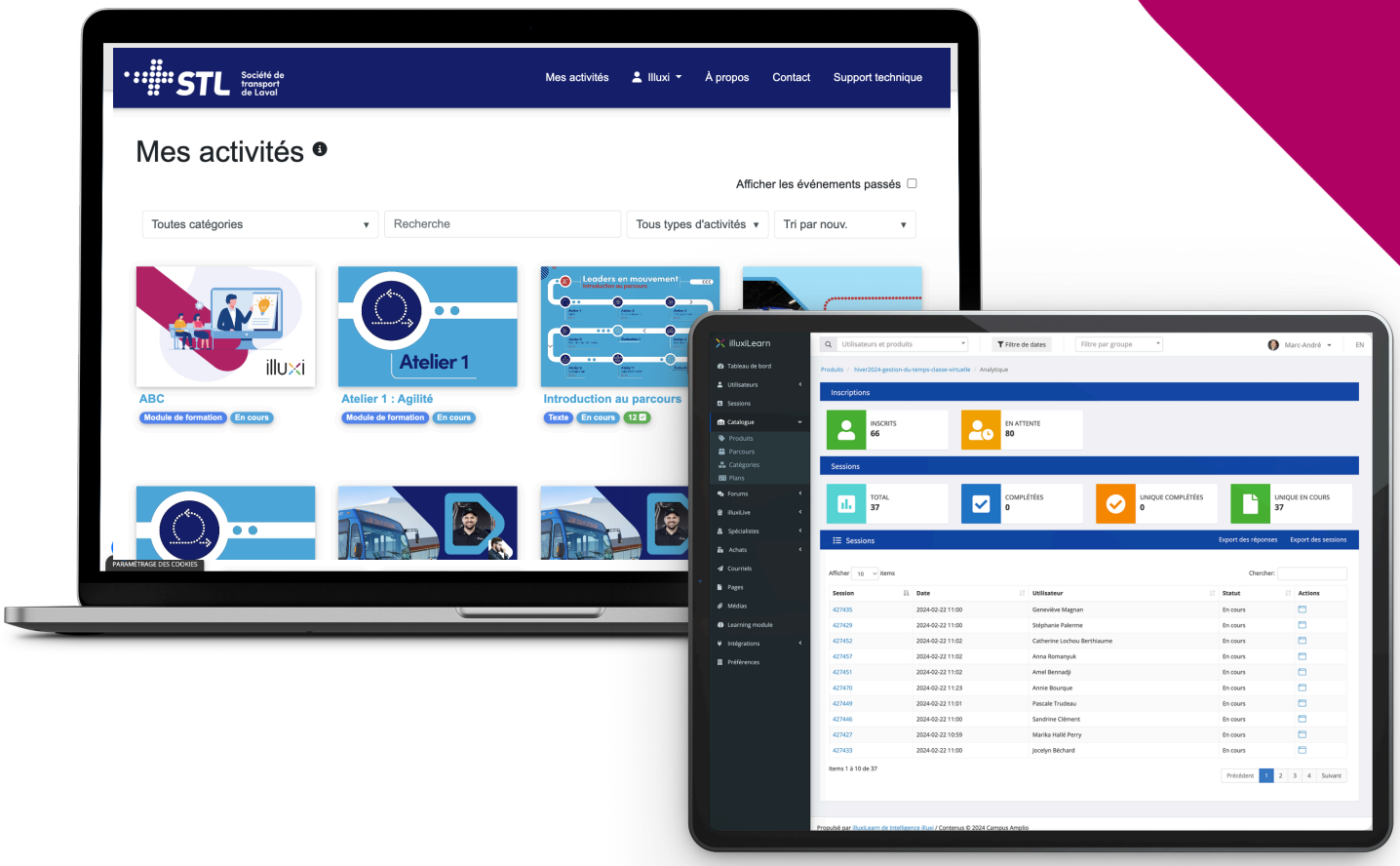


Table des matières

Annexe 1 - Liste des différentes politiques de sécurité d’illuxi

Chez illuxi, nous avons développé un cadre robuste de sécurité informatique basé sur des politiques rigoureuses et des pratiques éprouvées. Chaque membre de notre équipe suit une formation annuelle obligatoire pour s'assurer qu'ils maîtrisent parfaitement ces politiques, garantissant ainsi une adhésion totale à nos protocoles de sécurité. La dernière session de formation a été complétée en mai 2024, et chaque nouvel employé doit compléter cette formation durant sa première semaine. Certaines de ces politiques ont été annexées à ce document (annexe 2 à 6), et nous sommes fiers de pouvoir fournir les autres politiques sur demande, illustrant notre engagement à protéger vos données de manière proactive et efficace.

- Politique de protection des données (Data Protection Policy)
- Politique d'utilisation acceptable (Acceptable Use Policy)
- Politique de gestion des actifs (Asset Management Policy)
- Politique de sauvegarde (Backup Policy)
- Plan de continuité des activités (Business Continuity Plan) - (voir **Annexe 3)**
- Code de conduite (Code of Conduct)
- Politique de classification des données (Data Classification Policy)
- Politique de conservation des données (Data Retention Policy)
- Plan de reprise après sinistre (Disaster Recovery Plan) - (voir **Annexe 4)**
- Politique de cryptage (Encryption Policy)
- Plan de réponse aux incidents (Incident Response Plan)
- Politique de sécurité de l'information (Information Security Policy) - (voir **Annexe 2)**
- Politique de mot de passe (Password Policy)
- Politique de sécurité physique (Physical Security Policy)
- Politique de divulgation responsable (Responsible Disclosure Policy)
- Politique d'évaluation des risques (Risk Assessment Policy)
- Politique de cycle de vie du développement logiciel (Software Development Life Cycle Policy)
- Politique de contrôle d'accès système (System Access Control Policy)
- Politique de gestion des fournisseurs (Vendor Management Policy)
- Politique de gestion des vulnérabilités (Vulnerability Management Policy)

Annexe 2 - Politique de sécurité de l'information d'illuxi

Objectif

Cette politique définit bon nombre des procédures et des contrôles techniques visant à soutenir la protection des données.

Portée

Les systèmes de production qui créent, reçoivent, stockent ou transmettent les données des clients d'Intelligence illuxi inc. (ci-après dénommés "systèmes de production") doivent suivre les exigences et les directives décrites dans cette politique.

Rôles et responsabilités

Le Chef de la technologie est responsable de :

- la mise à jour, la révision et le maintien de cette politique
- la mise en œuvre des mesures de protection des données
- la gestion des journaux
- l'application des exigences de cette politique

Politique

La politique d'Intelligence illuxi inc. exige que :

- Les données doivent être manipulées et protégées selon leurs exigences de classification et conformément aux normes de chiffrement approuvées, le cas échéant.
- Dans la mesure du possible, stocker les données de même classification dans un référentiel de données donné et éviter de mélanger des données sensibles et non sensibles dans le même référentiel. Les contrôles de sécurité, y compris l'authentification, l'autorisation, le chiffrement des données et l'audit, doivent être appliqués selon la classification la plus élevée des données dans un référentiel donné.
- Les employés ne doivent pas avoir un accès administratif direct aux données de production pendant les opérations commerciales normales. Les exceptions incluent les opérations d'urgence telles que l'analyse médico-légale et la récupération manuelle après sinistre.
- Tous les systèmes de production doivent désactiver les services qui ne sont pas nécessaires pour atteindre l'objectif ou la fonction commerciale du système.
- Tous les accès aux systèmes de production doivent être journalisés.
- Tous les systèmes de production doivent avoir la surveillance de la sécurité activée, y compris la surveillance de l'activité et de l'intégrité des fichiers, le balayage des vulnérabilités et/ou la détection de logiciels malveillants, le cas échéant.

Protection des données client

Intelligence illuxi inc. héberge des données sur AWS dans la région CA-Central et sur Google Workspace.

Tous les employés d'Intelligence illuxi inc. adhèrent aux processus suivants pour réduire le risque de compromission des données de production :

- Mettre en œuvre et/ou réviser des contrôles conçus pour protéger les données de production contre une altération ou une destruction impropre.
- Veiller à ce que les données confidentielles soient stockées de manière à soutenir les journaux d'accès utilisateur et la surveillance automatisée des incidents de sécurité potentiels.
- Veiller à ce que les données de production d'Intelligence illuxi inc. soient segmentées et accessibles uniquement aux clients autorisés à y accéder.
- Toutes les données en cours de stockage doivent être stockées sur des volumes chiffrés à l'aide de clés de chiffrement gérées par Intelligence illuxi inc..

- Les clés de chiffrement de volume et les machines qui génèrent les clés de chiffrement de volume sont protégées contre tout accès non autorisé. Le matériel de clé de chiffrement est protégé par des contrôles d'accès de telle sorte que le matériel de clé n'est accessible que par des comptes privilégiés.

Accès

L'accès des employés d'Intelligence illuxi inc. à la production est contrôlé par un processus d'approbation et est désactivé par défaut. Lorsque l'accès est approuvé, un accès temporaire est accordé permettant l'accès à la production. L'accès à la production est examiné par l'équipe de sécurité au cas par cas.

Séparation

Les données client sont logiquement séparées au niveau de la base de données/du magasin de données en utilisant un identifiant unique pour le client. La séparation est imposée au niveau de l'API où le client doit s'authentifier avec un compte choisi, puis l'identifiant unique du client est inclus dans le jeton d'accès et utilisé par l'API pour restreindre l'accès aux données du compte. Toutes les requêtes de base de données/magasin de données incluent ensuite l'identifiant du compte.

Surveillance

Intelligence illuxi inc. utilise AWS CloudWatch/CloudTrail pour surveiller l'ensemble de l'exploitation des services cloud (les capacités de surveillance et de rapports internes sont utilisées pour rendre compte des opérations cryptographiques, du chiffrement et des politiques, processus, procédures et contrôles de gestion des clés). En cas de défaillance du système et si une alarme est déclenchée, le personnel clé est notifié par message texte, chat et/ou e-mail afin de prendre les mesures correctives appropriées.

Accord de confidentialité/non-divulgation (NDA)

Intelligence illuxi inc. utilise des accords de confidentialité ou de non-divulgation pour protéger les informations confidentielles à l'aide de termes juridiquement contraignants. Les NDA s'appliquent aussi bien aux parties internes qu'externes. Les NDA auront les éléments suivants :

- Définition des informations à protéger
- Durée de l'accord
- Actions requises à la résiliation de l'accord
- Responsabilités et actions pour éviter la divulgation non autorisée
- Propriété des informations, secrets commerciaux et propriété intellectuelle
- Utilisation autorisée des informations confidentielles et droits d'utilisation des informations
- Audit et surveillance des activités impliquant des informations confidentielles
- Processus de notification et de signalement de la divulgation non autorisée ou de la fuite d'informations
- Termes de restitution ou de destruction des informations lorsque l'accord est résilié
- Actions en cas de violation de l'accord
- Révision périodique

Données au repos

Chiffrement

Toutes les bases de données, les magasins de données et les systèmes de fichiers sont chiffrés conformément à la Politique de Chiffrement de Intelligence illuxi inc.

Conservation

Les données stockées doivent être correctement catégorisées et un calendrier de conservation doit être appliqué en conjonction avec la Politique de Gestion des Actifs de Intelligence illuxi inc., la Politique de Classification des Données et la Politique de Conservation des Données. Les considérations pour la durée de conservation comprennent :

- Les exigences légales, réglementaires ou contractuelles
- Le type de données (par exemple, les enregistrements comptables, les enregistrements de bases de données, les journaux d'audit)
- Le type de support de stockage (par exemple, papier, disque dur, serveur)

Stockage et Élimination

Les données stockées doivent être correctement stockées et manipulées pendant leur repos. Les considérations pour le stockage et l'élimination des données au repos en conjonction avec la Politique de Gestion des Actifs, la Politique de Classification des Données et la Politique de Conservation des Données de Intelligence illuxi inc. comprennent :

- Autorisation d'accès ou de gestion des données stockées
- Identification correcte des enregistrements et de leur période de conservation
- Changement technologique et capacité d'accès aux données pendant toute la période de conservation
- Délai et format acceptables pour récupérer les données
- Méthodes appropriées d'élimination

Suppression des données

Les données sensibles stockées qui ne sont plus nécessaires seront correctement supprimées conformément aux objectifs commerciaux de Intelligence illuxi inc., aux lois et réglementations applicables, ainsi qu'aux accords de tiers pertinents. Un enregistrement de cette suppression sera conservé.

Les méthodes suivantes seront utilisées pour supprimer les données : Google Workspace Accès et contrôle des données

Données en transit

Nécessité

Les données ne seront transférées que si cela est strictement nécessaire pour les processus commerciaux efficaces.

Échange d'informations

Les informations seront échangées entre le système de Intelligence illuxi inc. et d'autres systèmes d'information uniquement selon les autorisations accordées par <TYPE D'ACCORD(S)>, qui comprennent :

- Caractéristiques de l'interface ;
- Exigences en matière de sécurité et de confidentialité, contrôles et responsabilités pour chaque système ; et,
- Niveau d'impact des informations communiquées.

Le(s) accord(s) seront examiné(s) et mis à jour mensuellement, ou au besoin.

Canaux de messagerie pour les utilisateurs finaux

- Les données restreintes et sensibles ne sont pas autorisées à être envoyées via des canaux de messagerie électronique pour les utilisateurs finaux tels que l'e-mail ou le chat, sauf si le chiffrement de bout en bout est activé.

Annexe 3 - Politique de continuité des activités

Objet
Cette politique établit des procédures pour la récupération de Intelligence illuxi inc. suite à une perturbation, en conjonction avec le Plan de Reprise Après Sinistre.

Politique
La politique de Intelligence illuxi inc. exige que :

- Un plan et un processus pour la continuité des activités, y compris la sauvegarde et la récupération des systèmes et des données, soient définis et documentés.
- Le Plan de Continuité des Activités soit simulé et testé au moins une fois par an. Des indicateurs de performance doivent être mesurés et les améliorations identifiées pour la récupération doivent être enregistrées afin d'améliorer le processus.
- Les contrôles de sécurité et les exigences doivent être maintenus sur les sites principaux et secondaires lors de toutes les activités liées au Plan de Continuité des Activités, ainsi que lors des perturbations.

Rôles et responsabilités
Cette politique est maintenue par le Responsable de la Sécurité et le Responsable de la Confidentialité de Intelligence illuxi inc. Toute l'équipe de direction doit être informée de tout événement de contingence.

Ligne de succession
L'ordre de succession suivant garantit que l'autorité décisionnelle pour le Plan de Continuité des Activités de Intelligence illuxi inc. est maintenue sans interruption. Le PDG est responsable de la sécurité du personnel et de l'exécution des procédures documentées dans ce Plan. Le Responsable de l'Ingénierie est responsable de la récupération des environnements techniques de Intelligence illuxi inc. Si le PDG ou le Responsable de l'Ingénierie est incapable de remplir ses fonctions ou choisit de déléguer cette responsabilité, le Responsable des Opérations fonctionnera comme autorité ou désignera un autre délégué.

Équipes de réponse et responsabilités
Les équipes suivantes ont été formées pour répondre à un événement de contingence affectant l'infrastructure et les systèmes de Intelligence illuxi inc. :

- **RH et installations** : responsable de la sécurité physique de tous les employés de Intelligence illuxi inc. et de la sécurité environnementale sur chaque site physique de Intelligence illuxi inc. Le responsable d'équipe est le Responsable RH, qui rend compte au PDG.
- **DevOps** : responsable de garantir le bon fonctionnement des applications, des services web, des plateformes et de l'infrastructure Cloud. DevOps teste également les redéploiements et évalue les dommages causés à l'environnement. Le responsable est le Responsable de l'Ingénierie.
- **Sécurité** : évalue et réagit à tous les incidents liés à la cybersécurité conformément à la politique de Réponse aux Incidents de Intelligence illuxi inc. L'équipe sécurité aide les autres équipes en cas d'événements non liés à la cybersécurité. Le responsable est le Responsable de la Sécurité.

Les membres des équipes susmentionnées doivent conserver une copie locale des informations de contact de l'équipe de succession du Plan de Continuité des Activités. Les responsables d'équipe doivent également maintenir une copie locale de cette politique en cas d'indisponibilité d'Internet lors d'un scénario de sinistre.

Politique

Stratégie de Résilience Opérationnelle

Les stratégies de Intelligence illuxi inc. pour la résilience opérationnelle adoptent une approche globale de l'entreprise et de ses processus métier, et sont développées en tenant compte des limites acceptables en termes d'appétit et de tolérance au risque de l'entreprise. Ces stratégies sont développées à travers :

- **Évaluation des risques** : pour identifier les menaces internes et externes à la capacité de l'entreprise à mener ses activités, notamment dans les domaines de la technologie, des ressources humaines, des installations et des tiers ;
- **Analyse des vulnérabilités** : pour identifier les faiblesses pouvant accroître le risque de perturbation opérationnelle ;
- **Analyse d'impact sur les activités** (BIA) : (a) pour définir les processus métier critiques, ainsi que les technologies, les personnes et les installations qui les soutiennent ; et, (b) pour évaluer les effets potentiels sur l'entreprise si ces processus ne peuvent pas être exécutés.

Analyse d'Impact sur les Activités (BIA)

La BIA déterminera la criticité des activités pour assurer la résilience opérationnelle et la continuité des activités durant et après une perturbation. La BIA aidera à identifier et prioriser les composants système en les reliant aux processus métier qu'ils soutiennent. Elle se déroule en trois étapes :

1. **Détermination des processus et criticité de la récupération** : identifier les processus métier pris en charge par le système et évaluer l'impact d'une perturbation du système sur ces processus.
2. **Identification des besoins en ressources** : identifier les ressources nécessaires pour reprendre les processus métier. Exemples de ressources : installations, personnel, équipements, logiciels, fichiers de données, composants système, et documents essentiels.
3. **Priorisation des ressources du système pour la récupération** : lier plus clairement les ressources du système aux processus métier critiques et établir des priorités pour la récupération.

Récupération des sites de travail

Si une installation de Intelligence illuxi inc. est indisponible en raison d'un sinistre, les employés travailleront de chez eux ou d'un site secondaire avec accès Internet jusqu'à ce que la récupération du site soit terminée. L'organisation peut travailler depuis n'importe quel endroit disposant d'un accès Internet.

Récupération des services applicatifs

Intelligence illuxi inc. maintient une page de statut pour informer les clients en temps réel de l'état des services. La page est mise à jour avec les détails d'un événement pouvant causer une interruption ou un arrêt du service.

Annexe A : Analyse d'Impact sur les Activités

I. Description du Système

Intelligence illuxi inc. fonctionne entièrement sur des services cloud :

- Google Workspace : gestion des emails, calendriers, fichiers.
- Amazon Web Services (AWS) : gestion des serveurs, bases de données, stockage, surveillance.
- WP Engine : pour tous les sites WordPress.
- Atlassian : gestion de projet, documentation, dépôts de code.

II. Collecte de Données

Les données ont été recueillies auprès des administrateurs des locataires, des utilisateurs et des feuilles Excel fournies par les administrateurs.

Étapes suivantes :
Déterminer la criticité des processus métier, évaluer les besoins en ressources, et définir les priorités de récupération des systèmes.

Annexe 4 - Plan de reprise après sinistre

Objectif
Cette politique établit les procédures de reprise d'Intelligence illuxi inc. suite à une perturbation résultant d'une catastrophe. Cette politique de reprise après sinistre est maintenue par le responsable de la sécurité et le responsable de la confidentialité d'Intelligence illuxi inc.

Contexte
Les objectifs suivants ont été établis pour ce plan :

- Maximiser l'efficacité des opérations de contingence à travers un plan établi qui comprend les phases suivantes :
    - Phase de notification/activation pour détecter et évaluer les dommages et activer le plan.
    - Phase de récupération pour rétablir des opérations temporaires et récupérer les dommages subis par le système original.
    - Phase de reconstitution pour restaurer les capacités de traitement du système à des opérations normales.
- Identifier les activités, ressources et procédures nécessaires pour répondre aux exigences de traitement d'Intelligence illuxi inc. pendant des interruptions prolongées des opérations normales.
- Identifier et définir l'impact des interruptions sur les systèmes d'Intelligence illuxi inc.
- Attribuer des responsabilités au personnel désigné et fournir des conseils pour la reprise des systèmes d'Intelligence illuxi inc. pendant de longues périodes d'interruption des opérations normales.
- Assurer la coordination avec d'autres membres du personnel d'Intelligence illuxi inc. participant aux stratégies de planification de la reprise après sinistre.
- Assurer la coordination avec les points de contact externes et les fournisseurs participant aux stratégies de planification de la reprise après sinistre.

Politique
Exemples de types de catastrophes qui déclencheraient ce plan : catastrophes naturelles, troubles politiques, catastrophes d'origine humaine, menaces humaines externes et activités malveillantes internes.

Intelligence illuxi inc. définit deux catégories de systèmes du point de vue de la reprise après sinistre :

- Systèmes critiques. Ces systèmes hébergent des serveurs d'application et des serveurs de base de données ou sont nécessaires au fonctionnement des systèmes hébergeant des serveurs d'application et de base de données. Si ces systèmes sont indisponibles, ils affectent l'intégrité des données et doivent être restaurés, ou un processus de restauration doit être initié immédiatement.
- Systèmes non-critiques. Ce sont tous les systèmes non considérés comme critiques. Bien qu'ils puissent affecter les performances et la sécurité globale des systèmes critiques, ils ne les empêchent pas de fonctionner et d'être accessibles correctement. Ces systèmes sont restaurés avec une priorité inférieure à celle des systèmes critiques.

Évaluation et gestion des menaces et des risques
Il existe de nombreuses menaces perturbatrices potentielles qui peuvent survenir à tout moment et affecter le processus métier normal. Nous avons envisagé une large gamme de menaces potentielles et les résultats de nos délibérations sont inclus dans cette section. Chaque catastrophe environnementale potentielle ou situation d'urgence a été examinée. L'accent est mis sur le niveau de perturbation des activités pouvant découler de chaque type de catastrophe.

L'évaluation des risques informatiques d'Intelligence illuxi inc. documente une évaluation détaillée des menaces.

Tests et maintenance
Le responsable de la sécurité établira des critères de validation/test d'un plan de reprise après sinistre, un calendrier de test annuel, et s'assurera de la mise en œuvre du test. Ce processus servira également de formation pour le personnel impliqué dans l'exécution du plan. À tout le moins, le plan de reprise après sinistre doit être testé annuellement. Les types d'exercices de validation/test incluent les tests sur table et les tests techniques.

Test sur table
L'objectif principal du test sur table est de s'assurer que le personnel désigné est compétent et capable d'effectuer les exigences et procédures de notification/activation comme indiqué dans le plan de reprise après sinistre, en temps opportun. Les exercices incluent, mais ne sont pas limités à :

- Tester la capacité à répondre à une crise de manière coordonnée, opportune et efficace, en simulant l'occurrence d'une crise spécifique.

Test technique
L'objectif principal du test technique est de s'assurer que les processus de communication et de stockage et de récupération des données peuvent fonctionner sur un site alternatif pour exécuter les fonctions et capacités du système selon les exigences désignées. Le test technique inclut, mais n'est pas limité à :

- Processus à partir du système de sauvegarde sur le site alternatif
- Restauration du système à l'aide des sauvegardes
- Commutation des ressources de calcul et de stockage vers des sites de traitement alternatifs.

Procédures de reprise après sinistre
Phase de notification et d'activation
Cette phase traite des actions initiales prises pour détecter et évaluer les dommages causés par une perturbation à Intelligence illuxi inc. Selon l'évaluation de l'événement, et parfois conformément à la politique de réponse aux incidents d'Intelligence illuxi inc., le plan de reprise après sinistre peut être activé par le responsable de la sécurité et/ou le directeur technique (CTO).

Séquence de notification

- Le premier intervenant doit notifier le CTO. Toutes les informations connues doivent être transmises au CTO.
- Le CTO doit contacter le reste de l'équipe et les informer de l'événement. Le CTO doit commencer les procédures d'évaluation.
- Le CTO doit notifier les membres de l'équipe et les diriger pour qu'ils effectuent les procédures d'évaluation décrites ci-dessous afin de déterminer l'étendue des dommages et le temps de récupération estimé.

Évaluation des dommages

- Le CTO doit évaluer logiquement les dommages, déterminer si l'infrastructure est récupérable, et commencer à formuler un plan de récupération.

Annexe 5 - Processus d’audit

La sécurité des systèmes et la confidentialité des données de nos clients sont des priorités absolues. Notre engagement envers l'excellence en matière de sécurité se traduit par la réalisation régulière d'audits annuels, visant à évaluer et renforcer notre environnement informatique. Notre processus d'audit annuel est conçu pour assurer la conformité aux normes industrielles les plus strictes et répondre aux besoins spécifiques de la Ville de Sherbrooke. Voici les étapes clés de ce processus:

illuxi s’est associé à Drata pour assurer en continu le respect des normes de sécurité SOC 2. Drata est une plateforme automatisée de sécurité et conformité qui surveille et collecte en continu les preuves des contrôles de sécurité d’une entreprise, tout en facilitant le processus d’audit de conformité aux différentes normes de sécurité.

De plus, illuxi a retenu les services de la firme A-LIGN, un partenaire technologique de sécurité et de conformité, à qui plus de 4 000 organisations font confiance pour atténuer les risques liés à la cybersécurité.

Chaque année, A-LIGN procède à un audit de certification SOC2 Type 2 et émet un rapport qui inclut une évaluation minutieuse des contrôles de sécurité, attestant ainsi de la robustesse de notre environnement.

Notre approche en matière d'audit ne se limite pas à une simple conformité, mais s'étend à une collaboration continue avec la Ville de Sherbrooke. Nous sommes flexibles et disposés à répondre à tout besoin spécifique en matière d'audit et d'évaluation. La transparence, la communication ouverte et la recherche constante de l'amélioration guident notre processus d'audit annuel, garantissant à nos clients un niveau de sécurité et de conformité exceptionnel.

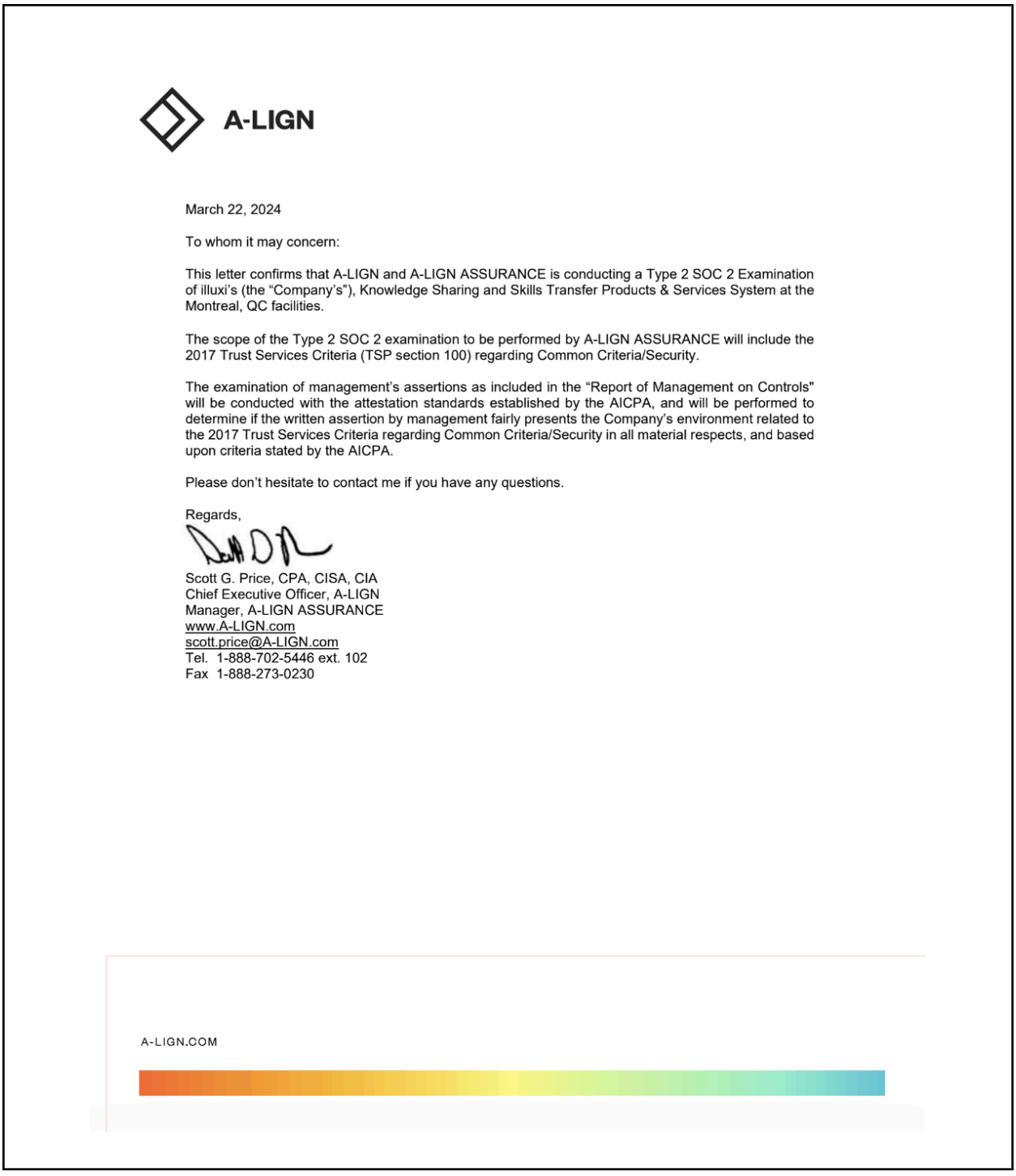
Annexe 6 - Normes de chiffrement et de contrôle

Chez illuxi, la sécurité des données est notre priorité absolue. Nous mettons en œuvre des normes de chiffrement rigoureuses et des contrôles de sécurité robustes pour assurer la confidentialité, l'intégrité et la disponibilité des informations sensibles.

Voici un aperçu de nos normes de chiffrement et des contrôles associés :

- illuxi adopte les normes de chiffrement les plus avancées pour sécuriser les données. Actuellement, notre infrastructure intègre les algorithmes de chiffrement suivants :
    - AES (Advanced Encryption Standard) : utilisé pour le chiffrement des données au repos et en transit.
    - TLS (Transport Layer Security) : employé pour sécuriser les communications entre les utilisateurs et nos serveurs.
- Nous avons mis en place des contrôles de sécurité stricts pour renforcer l'efficacité de nos normes de chiffrement. Ces contrôles garantissent une protection complète des données tout au long de leur cycle de vie, de la création à la transmission et au stockage :
- Une gestion robuste des clés est mise en œuvre pour assurer la sécurité des clés de chiffrement. Les clés sont générées, stockées et régulièrement mises à jour conformément aux meilleures pratiques de sécurité.
- Des outils de surveillance en temps réel sont déployés pour détecter toute activité suspecte ou violation potentielle. Les incidents sont traités immédiatement avec des protocoles d'intervention prédéfinis.
- L'accès aux données sensibles est strictement contrôlé avec des politiques d'accès basées sur des rôles. Les connexions aux systèmes d'illuxi sont sécurisées et authentifiées.
- Le chiffrement est appliqué à plusieurs niveaux, couvrant les bases de données, les canaux de communication et les sauvegardes.

Annexe 7 - Confirmation d’engagement SOC 2 Type 2 de notre auditeur A-LIGN



A-LIGN

March 22, 2024

To whom it may concern:

This letter confirms that A-LIGN and A-LIGN ASSURANCE is conducting a Type 2 SOC 2 Examination of illuxi’s (the “Company’s”), Knowledge Sharing and Skills Transfer Products & Services System at the Montreal, QC facilities.

The scope of the Type 2 SOC 2 examination to be performed by A-LIGN ASSURANCE will include the 2017 Trust Services Criteria (TSP section 100) regarding Common Criteria/Security.

The examination of management’s assertions as included in the “Report of Management on Controls" will be conducted with the attestation standards established by the AICPA, and will be performed to determine if the written assertion by management fairly presents the Company’s environment related to the 2017 Trust Services Criteria regarding Common Criteria/Security in all material respects, and based upon criteria stated by the AICPA.

Please don’t hesitate to contact me if you have any questions.

Regards,

Scott G. Price, CPA, CISA, CIA
Chief Executive Officer, A-LIGN
Manager, A-LIGN ASSURANCE
www.A-LIGN.com
scott.price@A-LIGN.com
Tel. 1-888-702-5446 ext. 102
Fax 1-888-273-0230

A-LIGN.COM

Annexe 8 - Lettre de confirmation - certification SOC 2 Type 2

DRATA

4660 La Jolla Villa Drive, Suite 100
San Diego, CA 92122

January 26, 2024
Illuxi
Re: Letter of Assertion

To Whom it May Concern:

Drata Inc. understands Illuxi is actively working towards an upcoming examination of its system based on the criteria set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report. Effective, January 26, 2024, Illuxi has procured the services of Drata's software to prepare for this upcoming SOC 2 examination, as well as continuously monitor its compliance posture post-audit.

Drata is a security and compliance automation platform that continuously monitors and collects evidence of a company's security controls, while streamlining end-to-end workflows to help ensure audit-readiness.

If you have any further questions you may email verify@drata.com.

Sincerely,

Ashley Hyman
VP of Customer Experience
Drata Inc.

Annexe 9 - Preuve de certification aux normes d'accessibilité

Accessibility Statement

Issued by accessiBe

sherbrooke.illuxi.com August 29, 2024

Compliance status

We firmly believe that the internet should be available and accessible to anyone and are committed to providing a website that is accessible to the broadest possible audience, regardless of ability.

To fulfill this, we aim to adhere as strictly as possible to the World Wide Web Consortium's (W3C) Web Content Accessibility Guidelines 2.1 (WCAG 2.1) at the AA level. These guidelines explain how to make web content accessible to people with a wide array of disabilities. Complying with those guidelines helps us ensure that the website is accessible to blind people, people with motor impairments, visual impairment, cognitive disabilities, and more.

This website utilizes various technologies that are meant to make it as accessible as possible at all times. We utilize an accessibility interface that allows persons with specific disabilities to adjust the website's UI (user interface) and design it to their personal needs.

Additionally, the website utilizes an AI-based application that runs in the background and optimizes its accessibility level constantly. This application remediates the website's HTML, adapts its functionality and behavior for screen-readers used by blind users, and for keyboard functions used by individuals with motor impairments.

If you wish to contact the website's owner please use the following email prod@illuxi.com

Screen-reader and keyboard navigation

Our website implements the ARIA attributes (Accessible Rich Internet Applications) technique, alongside various behavioral changes, to ensure blind users visiting with screen-readers can read, comprehend, and enjoy the website's functions. As soon as a user with a screen-reader enters your site, they immediately receive a prompt to enter the Screen-Reader Profile so they can browse and operate your site effectively. Here's how our website covers some of the most important screen-reader requirements:

1. **Screen-reader optimization:**
   we run a process that learns the website's components from top to bottom, to ensure ongoing compliance even when updating the website. In this process, we provide screen-readers with meaningful data using the ARIA set of attributes. For example, we provide accurate form labels; descriptions for actionable icons (social media icons, search icons, cart icons, etc.); validation guidance for form inputs; element roles such as buttons, menus, modal dialogues (popups), and others.

   Additionally, the background process scans all of the website's images. It provides an accurate and meaningful image-object-recognition-based description as an ALT (alternate text) tag for images that are not described. It will also extract texts embedded within the image using an OCR (optical character recognition) technology. To turn on screen-reader adjustments at any time, users need only to press the Alt+1 keyboard combination. Screen-reader users also get automatic announcements to turn the Screen-reader mode on as soon as they enter the website.

   These adjustments are compatible with popular screen readers such as JAWS, NVDA, VoiceOver, and TalkBack.

2. **Keyboard navigation optimization:**
   The background process also adjusts the website's HTML and adds various behaviors using JavaScript code to make the website operable by the keyboard. This includes the ability to navigate the website using the Tab and Shift+Tab keys, operate dropdowns with the arrow keys, close them with Esc, trigger buttons and links using the Enter key, navigate between radio and checkbox elements using the arrow keys, and fill them in with the Spacebar or Enter key.

   Additionally, keyboard users will find content-skip menus available at any time by clicking Alt+2, or as the first element of the site while navigating with the keyboard. The background process also handles triggered popups by moving the keyboard focus towards them as soon as they appear, not allowing the focus to drift outside.

   Users can also use shortcuts such as "M" (menus), "H" (headings), "F" (forms), "B" (buttons), and "G" (graphics) to jump to specific elements.

Disability profiles supported on our website

- Epilepsy Safe Profile: this profile enables people with epilepsy to safely use the website by eliminating the risk of seizures resulting from flashing or blinking animations and risky

color combinations.

- Vision Impaired Profile: this profile adjusts the website so that it is accessible to the majority of visual impairments such as Degrading Eyesight, Tunnel Vision, Cataract, Glaucoma, and others.

- Cognitive Disability Profile: this profile provides various assistive features to help users with cognitive disabilities such as Autism, Dyslexia, CVA, and others, to focus on the essential elements more easily.

- ADHD Friendly Profile: this profile significantly reduces distractions and noise to help people with ADHD, and Neurodevelopmental disorders browse, read, and focus on the essential elements more easily.

- Blind Users Profile (Screen-readers): this profile adjusts the website to be compatible with screen-readers such as JAWS, NVDA, VoiceOver, and TalkBack. A screen-reader is installed on the blind user's computer, and this site is compatible with it.

- Keyboard Navigation Profile (Motor-Impaired): this profile enables motor-impaired persons to operate the website using the keyboard Tab, Shift+Tab, and the Enter keys. Users can also use shortcuts such as "M" (menus), "H" (headings), "F" (forms), "B" (buttons), and "G" (graphics) to jump to specific elements.

Additional UI, design, and readability adjustments

1. **Font adjustments**
   users can increase and decrease its size, change its family (type), adjust the spacing, alignment, line height, and more.

2. **Color adjustments**
   users can select various color contrast profiles such as light, dark, inverted, and monochrome. Additionally, users can swap color schemes of titles, texts, and backgrounds with over seven different coloring options.

3. **Animations**
   epileptic users can stop all running animations with the click of a button. Animations controlled by the interface include videos, GIFs, and CSS flashing transitions.

4. **Content highlighting**
   users can choose to emphasize essential elements such as links and titles. They can also

choose to highlight focused or hovered elements only.

5. **Audio muting**
   users with hearing devices may experience headaches or other issues due to automatic audio playing. This option lets users mute the entire website instantly.

6. **Cognitive disorders**
   we utilize a search engine linked to Wikipedia and Wiktionary, allowing people with cognitive disorders to decipher meanings of phrases, initials, slang, and others.

7. **Additional functions**
   we allow users to change cursor color and size, use a printing mode, enable a virtual keyboard, and many other functions.

Assistive technology and browser compatibility

We aim to support as many browsers and assistive technologies as possible, so our users can choose the best fitting tools for them, with as few limitations as possible. Therefore, we have worked very hard to be able to support all major systems that comprise over 95% of the user market share, including Google Chrome, Mozilla Firefox, Apple Safari, Opera and Microsoft Edge, JAWS, and NVDA (screen readers), both for Windows and MAC users.

Notes, comments, and feedback

Despite our very best efforts to allow anybody to adjust the website to their needs, there may still be pages or sections that are not fully accessible, are in the process of becoming accessible, or are lacking an adequate technological solution to make them accessible. Still, we are continually improving our accessibility, adding, updating, improving its options and features, and developing and adopting new technologies. All this is meant to reach the optimal level of accessibility following technological advancements. If you wish to contact the website's owner, please use the following email prod@illuxi.com

accessiBe

Annexe 10 - Certification iso27001 de notre centre d'hébergement Amazon

*Vous pouvez télécharger le rapport de 179 pages d'une firme indépendante ici : https://illuxi-team.atlassian.net/wiki/spaces/IT/pages/2319450116/Rapport+de+certification+SOC+2+AWS

DocuSign Envelope ID: DE1A0974-DC50-4840-8DAC-11D6C06DACEF

MGMT. SYS. RvA C 466

Certificat

Numéro de certificat : 2013-009

Certifié par EY CertifyPoint depuis le : 18 Novembre 2010

Basé sur une vérification de la certification conforme aux exigences définies par les normes ISO/IEC 17021-1:2015 et ISO/IEC 27006:2015/A1:2020, le système de management de la sécurité de l'information tel que défini et mis en œuvre par :

Amazon Web Services, Inc.*

Et ses filiales (collectivement appelés Amazon Web Services (AWS)) sont conformes aux exigences énoncées dans la norme :

ISO/IEC 27001:2013

Date de délivrance du certificat : 18 Novembre 2022
Date de réémission du certificat : 25 Novembre 2022
Date d'expiration du certificat : 31 Octobre 2025
Date d'expiration du dernier cycle de certification : 30 Novembre 2022

Selon l'accord de certification du 1er Avril 2022, EY CertifyPoint effectuera des audits de surveillance et reconnaitra la validité du certificat jusqu'à la date d'expiration indiquée ci-dessus.

**En ce qui concerne les exigences spécifiques en matière de sécurité de l'information telles qu'énoncées dans la déclaration d'applicabilité version 2022.01 du 14 Septembre 2022, la certification est applicable aux actifs, services et localisations/sites décrits dans la section sur la portée au dos de ce certificat. Et (b) à toutes les filiales qui sont responsables de, ou qui contribuent à, la fourniture de tels services et leurs actifs et localisations associés.*

DocuSigned by:
Satin Sehgal
6E3A0F2A5EBF4C7...

J. Sehgal | Directeur, EY CertifyPoint

Le certificat officiel délivré par EY CertifyPoint est en version anglaise avec le même numéro de certificat. Cette copie en français n'est qu'une traduction et ne peut être utilisée qu'à titre informatif ou complètement avec le certificat original en anglais. Ce certificat n'est pas transférable et reste la propriété d'Ernst & Young CertifyPoint B.V., situé à Antonio Vivaldistraat 150, 1083 HP, Amsterdam, Pays-Bas. Tout litige relative à ce certificat sera soumise au droit néerlandais et à la compétence exclusive du tribunal de Rotterdam. Le contenu ne doit pas être modifié et toute promotion en utilisant ce certificat ou cette marque doit respecter la portée et la nature de la certification et les conditions du contrat. Compte tenu de la nature et des limites intérentes des évaluations de certification basées sur des échantillons, ce certificat n'a pas pour objectif d'exprimer une quelconque forme d'assurance quant à la performance de l'organisation certifiée selon la norme ISO mentionnée. Le certificat n'accorde aucune immunité à toute obligation légale / réglementaire. Tous droits réservés. © Copyright

Page 1 sur 6

Version digitale

Amazon Web Services, Inc.

Domaine d'application de la certification 2013-009

Le domaine d'application de cette certification ISO/IEC 27001:2013 est limitée par les services spécifiés d'Amazon Web Services, Inc. et des sites spécifiées. Le système de management de la sécurité de l'information (SMSI) est géré de manière centralisée à partir du siège social d'Amazon Web Services, Inc. à Seattle, Washington, États-Unis d'Amérique.

Les applications, systèmes, personnes et processus dans le domaine d'application sont globalement mis en œuvre et exploités par des équipes à partir d'un ensemble explicite de sites qui constituent Amazon Web Services, Inc. et qui sont spécifiquement définis dans le champ d'application et les limites de la certification.

Le domaine d'application du SMSI de Amazon Web Services, Inc. inclut les services mentionnés sur https://aws.amazon.com/compliance/iso-certified/, les sites et les ressources des services et de support AWS sont indiqués dans la section suivante de ce certificat.

Le système de management de la sécurité de l'information mentionné dans le domaine d'application ci-dessus est limité tel que défini dans le "IIMS Manual" version 2022.05.01, du 10 Novembre 2022.

Ce domaine d'application est uniquement valable pour le certificat 2013-009. Le certificat officiel délivré par EY CertifyPoint est en version anglaise avec le même numéro de certificat. Cette copie en français n'est qu'une traduction et ne peut être utilisée qu'à titre informatif ou conjointement avec le certificat original en anglais.

Amazon Web Services, Inc.

Domaine d'application de la certification 2013-009

Sites concernés :

Les services AWS sont proposés et disponibles dans plusieurs régions géographiques du monde. La portée de l'infrastructure AWS comprend le siège social, les installations du centre de données, le matériel de réseau et de serveur et les ressources qui prennent en charge les opérations du centre de données.

Les centres de données AWS hébergent du matériel qui prend en charge les services AWS répertoriés ci-dessus. Les centres de données AWS sont situés à : USA Est (Virginie du Nord), USA Est (Ohio), USA Ouest (Oregon), USA Ouest (Californie du Nord), AWS GovCloud (US-Est), AWS GovCloud (US-Ouest), Canada (Central), UE (Irlande), UE (Francfort), UE (Londres), UE (Paris), UE (Stockholm), UE (Milan), UE (Espagne), UE (Zurich), Asie-Pacifique (Hong Kong), Asie-Pacifique (Singapour), Asie-Pacifique (Mumbai), Asie-Pacifique (Hyderabad), Asie-Pacifique (Osaka), Asie-Pacifique (Séoul), Asie-Pacifique (Sydney), Asie-Pacifique (Tokyo), Asie-Pacifique (Jakarta), Amérique du Sud (São Paulo), Moyen-Orient (Bahreïn), Moyen-Orient (EAU), Afrique (Le Cap), ainsi que les localisations/sites suivants :

Sites périphériques AWS à :

- Alexandrie, Australie
- Amsterdam, Pays-Bas
- Anyang-si, République de Corée
- Ashburn, États-Unis
- Athènes, Grèce
- Atlanta, États-Unis
- Auckland, Nouvelle-Zélande
- Ballerup, Danemark
- Bangalore, Inde
- Bangkok, Thaïlande
- Bannmai, Thaïlande
- District de Banqiao, Nouveau Taipei, Taïwan
- Barcelone, Espagne
- Bekasi, Indonésie
- Berlin, Allemagne
- Bhubaneswar, Inde
- Billerica, États-Unis
- Birmingham, Royaume-Uni
- Bogota - Colombie
- Boston, États-Unis
- Brentford, Royaume-Uni
- Bruxelles, Belgique
- Bucarest, Roumanie
- Budapest, Hongrie
- Buenos Aires, Argentine
- Caba, Argentine
- Canberra, Australie
- Le Cap, Afrique du Sud
- Changodar, Inde
- Chennaï, Inde
- Chicago, États-Unis
- Christchurch, Nouvelle-Zélande
- Clonshaugh, Irlande
- Colomb, États-Unis
- Copenhague, Danemark
- Dallas, États-Unis Texas
- Denver, États-Unis
- Dubaï, Émirats Arabes Unis
- Dublin, Irlande
- Düsseldorf, Allemagne
- Eden Prairie, États-Unis
- El Segundo, États-Unis

Ce domaine d'application est uniquement valable pour le certificat 2013-009. Le certificat officiel délivré par EY CertifyPoint est en version anglaise avec le même numéro de certificat. Cette copie en français n'est qu'une traduction et ne peut être utilisée qu'à titre informatif ou conjointement avec le certificat original en anglais.

Amazon Web Services, Inc.

Domaine d'application de la certification 2013-009

- Elk Grove Village, États-Unis
- Estación Terrena, Pérou
- Francfort, Allemagne
- Fujairah, Émirats Arabes Unis
- Guirlande, États-Unis
- Général Pacheco, Argentine
- Greenwood Village, États-Unis
- Haifa, Israël
- Hambourg, Allemagne
- Hanoi, Vietnam
- Helsinki, Finlande
- Hillsboro, États-Unis
- Ho Chi Minh, Vietnam
- Hong Kong, Chine
- Houston, États-Unis
- Huechuraba, Chili
- Hull, Royaume-Uni
- Hyderâbâd, Inde
- Irving, États-Unis
- Itasca, États-Unis
- Jaipur, Inde
- Jacksonville, États-Unis
- Jakarta, Indonésie
- Jersey City, États-Unis
- Johannesbourg, Afrique du Sud
- Kansas City, Missouri, États-Unis
- Khlong Nueng, Thaïlande
- Calcutta, Inde
- Ville de Koto, Japon
- Korpia, Grèce
- Kuala Lumpur, Malaisie
- Las Vegas, États-Unis
- Lisbonne, Portugal
- Londres, Royaume-Uni
- Los Angeles, États-Unis
- Madrid, Espagne
- Manama, Bahreïn
- Manchester, Royaume-Uni
- Manille, Philippines
- Marseille, France
- Melbourne, Australie
- Memphis, États-Unis
- Miami, États-Unis
- Milan, Italie
- Milpita, États-Unis
- Milton Keynes, Royaume-Uni
- Minneapolis, États-Unis
- Montréal Canada
- Mumbai, Inde
- Munich, Allemagne
- Nairobi, Kenya
- Nashville, États-Unis
- District de Neihu, Taïwan
- New Delhi, Inde
- New York, États-Unis
- Newark, États-Unis
- Noord Holland, Pays-Bas
- Norfolk, États-Unis
- Nord de Las Vegas, États-Unis
- Osaka, Japon
- Oslo, Norvège
- Pakkret, Thaïlande
- Palerme, Italie
- Palo Alto, États-Unis
- Paris, France
- Parkwest, Irlande
- Patna, Inde
- Perth, Australie
- Philadelphie, États-Unis
- Phoenix, États-Unis
- Piscataway, États-Unis
- Pittsburg, États-Unis
- Portland, États-Unis
- Prague, République Tchèque
- Pueblo Nuevo, Panamá
- Rancho Cordoue, États-Unis
- Reston, États-Unis
- Richardson, États-Unis
- Rio de Janeiro, Brésil
- Rome, Italie
- Rosedale, Nouvelle-Zélande
- San-Diego, États-Unis

Ce domaine d'application est uniquement valable pour le certificat 2013-009. Le certificat officiel délivré par EY CertifyPoint est en version anglaise avec le même numéro de certificat. Cette copie en français n'est qu'une traduction et ne peut être utilisée qu'à titre informatif ou conjointement avec le certificat original en anglais.

Page 4 sur 6 Version digitale

Amazon Web Services, Inc.

Domaine d'application de la certification 2013-009

- San José, États-Unis
- Santiago de Querétaro, Mexique
- Santiago, Chili
- São Paulo, Brésil
- Schiphol-Rijk, Pays-Bas
- Seattle, États-Unis
- Secaucus, États-Unis
- Séoul, République de Corée
- Shinagawa, Japon
- Singapour, Singapour
- Slough, Royaume-Uni
- Sofia, Bulgarie
- Southfield, États-Unis
- Stockholm, Suède
- Streford, Royaume-Uni
- Surrey, Royaume-Uni
- Sydney, Australie
- Taipei, Taiwan
- Tallinn, Estonie
- Tambon Klong Tamru, Thaïlande
- Tel-Aviv, Israël
- Tempé, États-Unis
- Thung Song Hong, Thaïlande
- Tokyo, Japon
- Toronto, Canada
- Tukwila, États-Unis
- Ultime, Australie
- Vancouver, Canada
- Varsovie, Pologne
- Vienne, Autriche
- Vienne, États-Unis
- West Valley City, États-Unis
- Wiltshire, Royaume-Uni
- Zagreb, Croatie
- Zurich, Suisse

Les sites wavelength à :

- Alpharetta, États-Unis
- Annapolis Junction, États-Unis
- Atlanta, États-Unis
- Aurore, États-Unis
- Azusa, États-Unis
- Berlin, Allemagne
- Boston, États-Unis
- Charlotte, États-Unis
- Daejon, Corée du Sud
- Denver, États-Unis
- Dortmund, Allemagne
- Euless, États-Unis
- Houston, États-Unis
- Las Vegas, États-Unis
- Londres, Royaume Uni
- Los Angeles, États-Unis
- Minneapolis, États-Unis
- Munich, Allemagne
- Nouveau Berlin, États-Unis
- Osaka, Japon
- Pembroke Pines, États-Unis
- Redmond, États-Unis
- Rocklin, États-Unis
- Southfield, États-Unis
- Tama, Japon
- Tempé, États-Unis
- Tokyo, Japon
- Toronto, Canada
- Canton de Wall, États-Unis
- Westborough, États-Unis

Ce domaine d'application est uniquement valable pour le certificat 2013-009. Le certificat officiel délivré par EY CertifyPoint est en version anglaise avec le même numéro de certificat. Cette copie en français n'est qu'une traduction et ne peut être utilisée qu'à titre informatif ou conjointement avec le certificat original en anglais.

Amazon Web Services, Inc.

Domaine d'application de la certification 2013-009

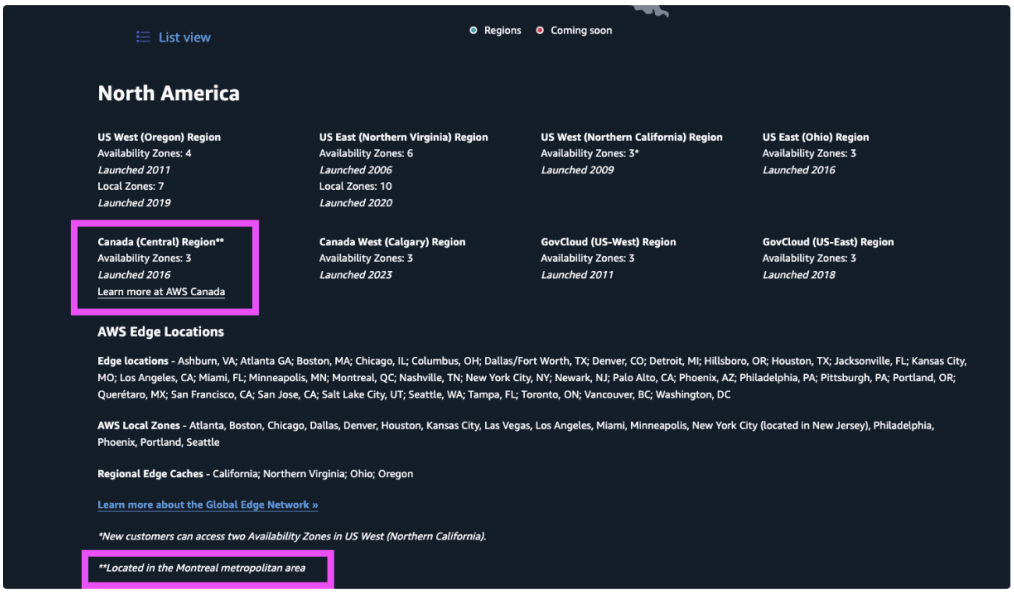
Les sites de zones locales à :

- Atlanta, États-Unis
- Boston, États-Unis
- Chicago, États-Unis
- New Delhi, Inde
- Denver, États-Unis
- Le deuxième, États-Unis
- Greenwood Village, États-Unis
- Hillsboro, États-Unis
- Houston, États-Unis
- Irvin, États-Unis
- Kansas City, Missouri, États-Unis
- Calcutta, Inde
- Las Vegas, États-Unis
- Sommet Lee, États-Unis
- Los Angeles États-Unis
- Miami, États-Unis
- Minneapolis, États-Unis
- Philadelphie, États-Unis
- Phoenix, États-Unis
- Piscataway, États-Unis
- Richardson, États-Unis
- Seattle, États-Unis

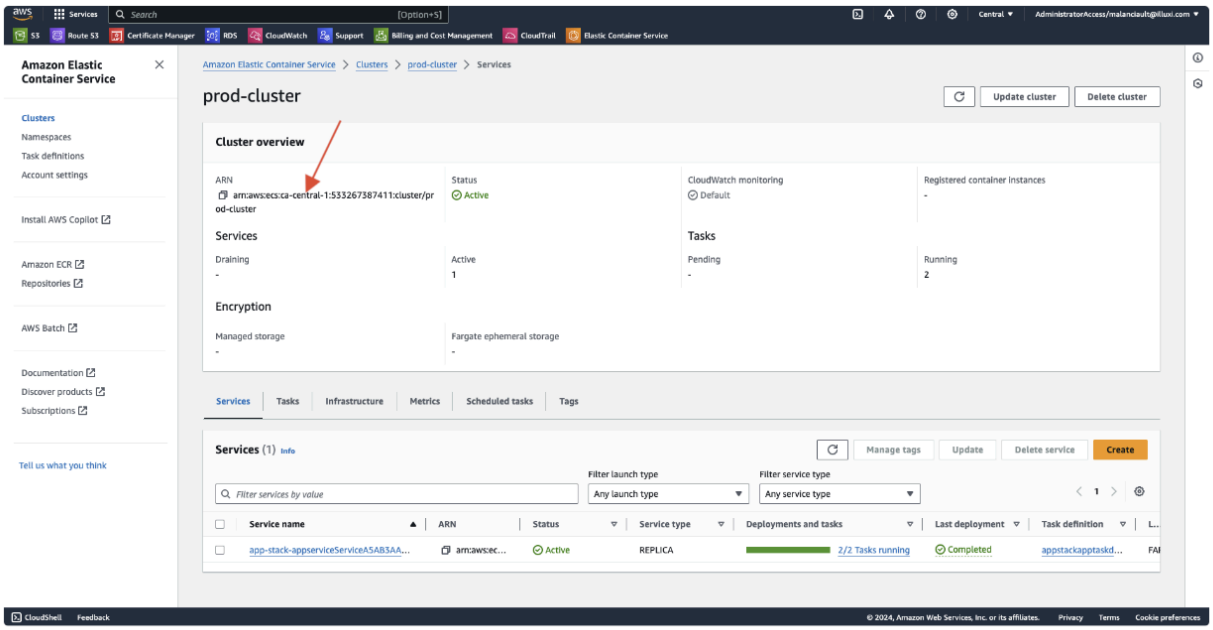
Ce domaine d'application est uniquement valable pour le certificat 2013-009. Le certificat officiel délivré par EY CertifyPoint est en version anglaise avec le même numéro de certificat. Cette copie en français n'est qu'une traduction et ne peut être utilisée qu'à titre informatif ou conjointement avec le certificat original en anglais.

Annexe 11 - Preuve de localisation de l’infrastructure technologique

L’ensemble de notre infrastructure réside dans la zone géographique Canada Central (ca-central-1) dont les centres de données se trouvent à Montréal:



Voici une copie de notre cluster de serveurs, démontrant sa localisation dans la zone ca-central-1:



Voici une copie de notre cluster de base de données, démontrant sa localisation dans la zone ca-central-1: