Réponse d'AWS au sous-comité sur l'information, les communications et la technologie de l'Association canadienne des chefs de police (ACCP)

Pratiques exemplaires en matière de stockage et de traitement de données hors site

Mai 2017

Avis

Ce document est fourni à titre informatif uniquement. Il présente l'offre de produits et les pratiques actuelles d'AWS à la date de publication de ce document, des informations qui sont susceptibles d'être modifiées sans préavis. Il incombe aux clients de procéder à leur propre évaluation indépendante des informations contenues dans ce document et chaque client est responsable de son utilisation des produits ou services AWS, chacun étant fourni « en l'état », sans garantie d'aucune sorte, qu'elle soit explicite ou implicite. Ce document n'offre pas de garantie, représentation, engagement contractuel, condition ou assurance de la part d'AWS, de ses sociétés apparentées, fournisseurs ou concédants de licence. Les responsabilités et obligations d'AWS vis-à-vis de ses clients sont régies par les contrats AWS. Le présent document ne fait partie d'aucun contrat et ne modifie aucun contrat entre AWS et ses clients.

Table des matières

Introduction 4

Exigences de l'ACCP 5

- Exigences du fournisseur 6
- Exigences en matière de sécurité pour les renseignements 18
- Exigences en matière de sécurité pour les centres de données 27
- Exigences en matière de sécurité visant le personnel 32
- Exigences relatives au contrôle des accès 34

Versions du document 38

Introduction

Les renseignements présentés dans ce document aident les organismes d'application de la loi du Canada à évaluer si les services AWS respectent leurs exigences et à savoir comment intégrer AWS à l'infrastructure de contrôle existante sur laquelle repose leur environnement informatique. Pour en savoir plus sur la conformité dans AWS, consultez AWS Risk and Compliance Overview (https://do.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Overview.pdf).

Les tableaux figurant dans la section Exigences de l'ACCP ci-dessous traitent des exigences mentionnées dans les *pratiques exemplaires en matière de stockage et de traitement de données hors site du sous-comité sur l'information, les communications et la technologie de l'Association canadienne des chefs de police (ACCP)*. Il est possible de demander des renseignements complémentaires sur le respect des pratiques exemplaires du sous-comité de l'ACCP par AWS à condition de respecter une entente de non-divulgation avec AWS. Veuillez communiquer avec votre représentant AWS.

Exigences de l'ACCP

Les tableaux ci-dessous décrivent comment AWS s'y prend pour respecter les exigences de stockage des renseignements de l'ACCP.

> ***Protégé A*** *et* ***Protégé B*** *font référence à des niveaux de sécurité établis par le gouvernement du Canada pour les renseignements et les actifs de nature délicate du gouvernement. Un accès non autorisé à des renseignements désignés* ***Protégé A*** *pourrait mener à un « préjudice à une personne, à une organisation ou à un gouvernement ». Un accès non autorisé à des renseignements désignés* ***Protégé B*** *pourrait mener à un « préjudice grave à une personne, à une organisation ou à un gouvernement ».*

Les valeurs des désignations **Protégé A** et **Protégé B** sont réglées aux options d'état suivantes :

- **O** – Obligatoire
- **H** – Hautement souhaitable
- **S** – Souhaitable

Exigences du fournisseur

Exigence	Protégé A	Protégé B	Référence	Responsabilité d'AWS
Soutien de niveau 1 et de niveau 2 géré en tout temps.	O	O	CJIS	AWS offre différentes options pour un soutien de niveau 1 et de niveau 2 en tout temps au niveau de soutien opérationnel ou supérieur. Pour en savoir plus, veuillez consulter https://aws.amazon.com/premiumsupport/compare-plans/.
Garantie de disponibilité d'un minimum de 99,9 %.	H	H	ACCP-ICT	Chaque service AWS donne des renseignements sur les ententes de niveaux de service par rapport à la disponibilité. Par exemple, Amazon EC2 a une entente de niveau de service par rapport à la disponibilité de 99,95 % (https://aws.amazon.com/ec2/sla) et Amazon S3 a une entente de niveau de service par rapport à la disponibilité de 99,99 % (https://aws.amazon.com/s3/sla).

Processus de gestion de la configuration documentés et éprouvés.	O	O	MITS	AWS maintient un processus de gestion de la configuration documenté et éprouvé qui est utilisé lors des étapes de conception, de développement, de mise en œuvre et d'exploitation du système d'information.
Des processus de contrôle des changements documentés et éprouvés qui respectent les processus de gestion des services ITIL.	O	O	MITS/ACCP-ICT	AWS maintient des processus de contrôle des changements qui soutiennent l'échelle et la complexité de l'organisation et qui ont été évalués de façon indépendante.
Processus d'intervention en cas d'incident documentés et éprouvés, notamment : • **Identification de l'incident** • **Intervention en cas d'incident** • **Rapport sur l'incident** • **Rétablissement à la suite d'un incident** • **Analyse après l'incident**	O	O	MITS	Le programme d'intervention en cas d'incident d'AWS (détection, enquête et intervention relativement à un incident) a été conçu en conformité avec les normes ISO 27001.

Fournir un rapport de conformité de niveau 2 SOC à jour (si les données financières sont utilisées ou stockées).	O	O	ACCP-ICT	AWS offre l'accès à son SOC 1 de type 2 et à son SOC 2 de type 2 : Rapports de sécurité et de disponibilité, assujettis à une entente de non-divulgation, tandis que le SOC 3 : Rapport de sécurité et de disponibilité est accessible au public. Pour en savoir plus, veuillez consulter https://aws.amazon.com/compliance/soc-faqs/.
Maintenir la conformité PCI (si des données PCI sont utilisées ou stockées).	O	O	ACCP-ICT	AWS maintient la conformité à PCI-DSS v3.2 en tant que fournisseur de services de niveau 1. Pour en savoir plus, veuillez consulter https://aws.amazon.com/compliance/pci-dss-level-1-faqs/.
Maintenir le rapport de conformité Cloud Controls Matrix (CCM) existant et le fournir à l'organisme sur demande.	H	H	ACCP-ICT	AWS est mentionné sur la page « Star registrant » de la CSA, se trouvant à https://cloudsecurityalliance.org/star-registrant/amazon-aws/.

Le sous-traitant doit avoir des processus adéquats de continuité des affaires et de reprise après sinistre pour se remettre d'une catastrophe naturelle ou attribuée à une activité humaine. Le sous-traitant doit fournir son plan de continuité des affaires et de reprise après sinistre au client sur demande. Les plans doivent inclure, mais sans s'y limiter : • **Le temps requis pour la reprise.** • **Le temps requis pour déménager à un site auxiliaire.** • **Le niveau de service et de fonctionnalité fourni par le site auxiliaire; et le délai requis pour que le fournisseur récupère les données principales et pour que le service reprenne.** • **Un rapport sur comment et à quelle fréquence les données du client sont sauvegardées.**	O	O	GRC	La résilience du client dans le nuage est transformée par l'utilisation du nuage. Les entreprises utilisent AWS pour avoir une reprise plus rapide des systèmes informatiques essentiels après une catastrophe et nous fournissons un livre blanc (https://aws.amazon.com/blogs/aws/new-whitepaper-use-aws-for-disaster-recovery/) sur l'utilisation d'AWS pour la reprise après un sinistre. La résilience du client ne dépend donc pas des répercussions possibles sur l'infrastructure sous-jacente. AWS maintient des processus de continuité des opérations internes, y compris la redondance physique N+2 allant des générateurs aux tiers fournisseurs de service à chaque centre de données, et ce, à l'échelle mondiale.
Capacité de déterminer où se trouvent tous les renseignements de l'organisme en tout temps, y compris les données en ligne et les sauvegardes.	S	O	ACCP-ICT	Lorsqu'ils utilisent AWS, les clients ont le contrôle complet du mouvement de leurs données; en outre, ils ont la capacité de choisir la région dans laquelle leurs données sont conservées.

Assurez-vous que toute connexion à Internet, à d'autres réseaux externes ou à des systèmes d'information est effectuée au moyen d'interfaces contrôlées (p. ex. les serveurs mandataires, les passerelles, les routeurs, les coupe-feu, les tunnels chiffrés).	H	O	CJIS	AWS dispose d'un nombre limité de points d'accès au système d'information en vue de permettre une surveillance plus complète des communications entrantes et sortantes et du trafic réseau. Ces points d'accès du client sont appelés des points de terminaison API, qui permettent aux clients d'établir une séance de communication sécurisée avec leur espace de stockage ou leurs instances informatiques dans AWS. Les clients ont la capacité de déployer différents outils et mécanismes pour surveiller le trafic et les activités, par exemple, les configurations VPC, les groupes de sécurité EC2, le pare-feu d'applications Web d'AWS et les connexions sécurisées par chiffrement. Pour en savoir plus, veuillez consulter https://aws.amazon.com/security/.
Employer des outils et des techniques pour surveiller les événements sur le réseau, détecter les attaques et repérer une utilisation non autorisée en tout temps.	S	O	CJIS	Les clients d'AWS profitent des services et des technologies d'AWS, conçus de A à Z pour leur permettre d'être résilients lorsqu'ils sont confrontés à des attaques DDoS et d'avoir des services qui comprennent une réponse automatique aux attaques DDoS, ce qui contribue à minimiser le temps requis pour atténuer et réduire les répercussions. Le client dispose d'une grande marge de manœuvre lui permettant de mettre en œuvre des capacités similaires dans son environnement client afin de surveiller les événements système, de détecter les attaques et de repérer les utilisations non autorisées en tout temps, en vue d'inclure les vulnérabilités et les tests d'intrusion. Pour en savoir plus, veuillez consulter https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf.

S'assurer que l'arrêt du fonctionnement des mécanismes de protection des limites n'entraîne pas la divulgation non autorisée de renseignements à l'extérieur des limites du système d'information (c.-à-d. que la panne de l'appareil doit entraîner une « fermeture », et non une « ouverture »).	S	O	CJIS	Les utilisateurs d'AWS ont la possibilité d'adapter la configuration de leurs services de plusieurs façons pour respecter les exigences de sécurité en cas de panne.
Répartir les composantes du système d'information qui sont accessibles par le public (p. ex., les serveurs Web publics) sur des sous-réseaux indépendants qui ont des interfaces réseau distinctes.	S	H	ACCP-ICT	AWS n'exploite pas de composantes de système d'information accessibles au public (p. ex., les serveurs Web publics) à partir de l'infrastructure du nuage. Toutes les interactions de l'extérieur avec l'infrastructure utilisent un ensemble de points de terminaison API bien connus et structurés. Les serveurs Internet du compte client relèvent entièrement de son contrôle opérationnel. Pour en savoir plus, veuillez consulter https://aws.amazon.com/whitepapers/aws-security-best-practices/.
Les données en transit sont chiffrées.	H	O	MITS	AWS fournit plusieurs moyens pour chiffrer les données en transit. On peut créer des tunnels chiffrés IPSec entre le point de terminaison d'un client et son VPC. Pour en savoir plus, veuillez consulter https://aws.amazon.com/vpc.

Les données inactives (locales ou sauvegardées) sont chiffrées.	H	O	MITS	AWS fournit plusieurs moyens pour chiffrer les données inactives. Par exemple, en utilisant Amazon S3, les clients peuvent télécharger des données en amont ou en aval en toute sécurité par l'intermédiaire des points de terminaison chiffrés SSL, à l'aide d'un protocole HTTPS. Amazon S3 peut chiffrer automatiquement les données de client inactives et offre plusieurs options de gestion des clés. Sinon, les clients peuvent utiliser une bibliothèque de chiffrement cliente telle que Amazon S3 Encryption Client pour chiffrer leurs données avant de les téléverser dans Amazon S3. Au besoin, Amazon S3 peut chiffrer les données inactives du client en utilisant le chiffrement côté serveur (SSE); Amazon S3 chiffrera automatiquement les données du client à mesure qu'elles sont écrites et il les déchiffrera au moment de les récupérer. Lorsqu'Amazon S3 SSE chiffre les données inactives, il utilise les clés symétriques 256 bits Advanced Encryption Standard (AES). Il existe trois façons de gérer les clés de chiffrement d'un chiffrement côté serveur dans Amazon S3 : • Chiffrement côté serveur (SSE) avec gestion des clés Amazon S3 (SSE-S3) : Amazon S3 chiffre les données inactives et gérera les clés de chiffrement. • SEE utilisant les clés de chiffrement fournies par le client (SSE-C) : Amazon S3 chiffrera les données inactives à l'aide des clés de chiffrement fournies par le client. • Chiffrement côté serveur (SSE) utilisant AWS KMS (SSE-KMS) : Amazon S3 chiffrera les données inactives en utilisant les clés qui sont gérées uniquement par le client dans AWS Key Management Service (KMS). Pour en savoir plus, veuillez consulter : • https://aws.amazon.com/s3/details/#security • https://aws.amazon.com/kms/

Lorsqu'on utilise le chiffrement, les clés de chiffrement satisfont la norme AES 256 ou sont supérieures à celle-ci.	H	O	ACCP-ICT	AWS prend en charge AES 256.
Lorsqu'on utilise le chiffrement, le module de chiffrement utilisé sera certifié conforme aux normes FIPS 140-2.	S	H	MITS	AWS GovCloud (US) assure la conformité des points de terminaison aux exigences des normes FIPS 140-2. Les clients ont la capacité d'installer des modules conformes aux normes FIPS dans leur compte, si leur application est capable de prendre en charge les modules de chiffrement FIPS 140-2.
Les clés de chiffrement sont très sécuritaires et protégées, et elles sont offertes à l'organisme sur demande.	O	O	MITS	Utiliser AWS CloudHSM ou AWS KMS permet aux clients de créer et de gérer leurs propres clés de chiffrement. Pour en savoir plus, veuillez consulter : • https://aws.amazon.com/kms/ • https://aws.amazon.com/cloudhsm/

Les clés de chiffrement sont contrôlées et stockées par l'organisme.	S	H	ACCP-ICT	Utiliser AWS CloudHSM ou AWS KMS permet aux clients de créer et de gérer leurs propres clés de chiffrement. Pour en savoir plus, veuillez consulter : • https://aws.amazon.com/kms/ • https://aws.amazon.com/cloudhsm/
L'accès externe aux fonctions d'administration ou de gestion doit se faire par RPV uniquement. Ceci comprend les modems, les clients FTP ou les protocoles/ports dont le soutien est assuré par le fabricant du matériel. Cet accès doit se limiter aux utilisateurs dotés de l'authentification à deux facteurs.	S	H	NPISAB	Les clients peuvent se connecter à la console de gestion pour gérer leur environnement sur le RPV et exiger l'utilisation d'une authentification à deux facteurs, conformément aux exigences internes de l'organisme. Pour en savoir plus, veuillez consulter https://aws.amazon.com/iam/details/mfa/. Les connexions administratives à l'infrastructure d'AWS sont établies à l'aide de mécanismes sécurisés.
Les données de l'organisme ne seront pas utilisées par un fournisseur de services, et ce, pour quelque raison que ce soit. Il est interdit pour le fournisseur de services de balayer les fichiers de données dans le but d'explorer les données ou à des fins publicitaires.	O	O	ACCP-ICT	AWS n'accède pas au contenu du client et ne l'utilise pas, sauf en vertu d'une exigence légale, à quelque fin que ce soit autre que la gestion des services AWS et leur prestation aux clients et à leurs utilisateurs finaux. AWS n'utilise jamais le contenu des clients ni aucune information récupérée à des fins de marketing ou publicitaires. Pour en savoir plus, veuillez consulter https://aws.amazon.com/compliance/data-privacy-faq/. La politique de confidentialité d'AWS décrit comment AWS recueille et utilise les renseignements fournis par les clients pour la création ou la gestion des comptes AWS, et c'est pour cette raison qu'on les appelle des « renseignements sur le compte ». Par exemple, les renseignements sur le compte comprennent les noms, noms d'utilisateur, numéros de téléphone, adresses électroniques et renseignements de facturation associés au compte AWS d'un client.

				La politique de confidentialité d'AWS s'applique aux renseignements sur le compte des clients et ne s'applique pas au contenu stocké par les clients dans AWS, y compris tout renseignement de nature personnelle sur les utilisateurs finaux du client. AWS ne divulgue pas, ne déplace pas, n'accède pas et n'utilise pas le contenu du client, sauf si cela s'avère nécessaire en vertu de l'entente du client avec AWS. L'entente du client avec AWS (https://aws.amazon.com/agreement/) et la FAQ sur la protection des données d'AWS contiennent plus de renseignements sur la manière dont nous gérons les contenus que vous stockez dans nos systèmes.
Tous les pare-feu respectent la norme minimale Evaluation Assurance Level (EAL) 4.	H	O	NPISAB	AWS fournit plusieurs caractéristiques et plusieurs services pour aider les clients à protéger leurs données, y compris le pare-feu d'applications Web d'AWS. De plus, plusieurs fournisseurs dans AWS Marketplace offrent des produits de gestion de la sécurité semblables. Pour en savoir plus, veuillez consulter : • https://aws.amazon.com/waf/ • https://aws.amazon.com/marketplace
S'assurer d'effectuer régulièrement des balayages contre les virus et les logiciels malveillants et d'effectuer des tests d'intrusion dans l'environnement.	O	O	NPISAB	AWS s'assure d'effectuer régulièrement des balayages contre les virus et les logiciels malveillants et d'effectuer des tests d'intrusion dans l'environnement de l'infrastructure. Les clients peuvent aussi effectuer leurs propres tests d'intrusion dans leur compte. Pour en savoir plus, veuillez consulter https://aws.amazon.com/security/penetration-testing/.

Bien documenter leurs résultats de balayage contre les virus et les logiciels malveillants et de tests d'intrusion et, sur demande de l'organisme, le fournisseur fournira un rapport à jour.	H	O	ACCP-ICT	Tous les programmes, processus et procédures AWS de gestion des logiciels antivirus et de détection de programmes malveillants sont conformes à la norme ISO 27001 et sont mentionnés dans les rapports AWS SOC. AWS Security retient souvent les services d'entreprises de sécurité indépendantes pour mener des évaluations extérieures des vulnérabilités et il a été validé et certifié par un vérificateur indépendant pour confirmer le respect de la norme de certification ISO 27001.
Bien documenter toute la gestion de correctifs et, sur demande de l'organisme, le fournisseur fournira un rapport à jour.	H	O	ACCP-ICT	Les clients gardent le contrôle de leurs propres systèmes d'exploitation invités, ainsi que de leurs logiciels et applications, et il leur incombe d'exécuter des analyses de vulnérabilité et d'appliquer des correctifs sur leurs propres systèmes. Un client peut demander la permission de mener à bien des analyses sur l'infrastructure du nuage tant que celles-ci se limitent à ses propres instances et n'enfreignent pas la politique d'utilisation acceptable d'AWS. AWS analyse régulièrement toutes les adresses IP de tous les points de terminaison des services ayant accès à Internet à la recherche de vulnérabilités. Elle informe ensuite les parties concernées du résultat de ses analyses afin que celles-ci puissent corriger les vulnérabilités identifiées. Les opérations de maintenance et d'application des correctifs d'AWS n'ont généralement pas de répercussions sur les clients. Pour en savoir plus, consultez le livre blanc sur la sécurité d'AWS (accessible à https://aws.amazon.com/security/) et la norme ISO 27001, annexe A, domaine 12. La solution AWS a été validée et certifiée par un vérificateur indépendant afin de confirmer son respect de la norme de certification ISO 27001.

Surveillance et enregistrement sur une base continue pour les événements suivants : • **Attaques par DDOS** • **Changements non autorisés appliqués au matériel, aux micrologiciels et aux logiciels** • **Anomalies du rendement du système** • **Signatures connues d'attaques**	S	O	MITS	AWS utilise différents outils et différentes techniques pour surveiller les événements sur le réseau et repérer une utilisation non autorisée en tout temps. Les clients d'AWS profitent des services et des technologies d'AWS, conçus de A à Z pour leur permettre d'être résilients lorsqu'ils sont confrontés à des attaques DDoS et d'avoir accès à des services qui comprennent une réponse automatique aux attaques DDoS, ce qui contribue à minimiser le temps requis pour atténuer et réduire les répercussions. Le client dispose d'une grande marge de manœuvre lui permettant de mettre en œuvre des capacités similaires dans son environnement client afin de surveiller les événements système, de détecter les attaques et de repérer les utilisations non autorisées en tout temps. Pour en savoir plus, veuillez consulter : • https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf • https://aws.amazon.com/security
Capacité à appliquer les politiques de conservation des données définies par le client.	S	H	ACCP-ICT	Bien que AWS donne aux clients la capacité de supprimer leurs données, les clients AWS conservent le contrôle et la propriété de leurs données et il leur incombe donc de gérer la conservation des données selon leurs propres exigences. AWS maintient les politiques de conservation des données conformément à plusieurs normes internationales et plusieurs règlements internationaux bien connus, notamment SOC et PCI-DSS, qui font l'objet d'une évaluation et d'une attestation indépendantes.

Exigences en matière de sécurité pour les renseignements

Exigence	Protégé A	Protégé B	Référence	Responsabilité d'AWS
Capacité de déterminer où se trouvent tous les renseignements de l'organisme en tout temps, y compris les données en ligne et les sauvegardes.	S	O	ACCP-ICT	Les clients ont le contrôle complet du mouvement de leurs données lorsqu'ils utilisent AWS; en outre, ils ont la capacité de choisir la région dans laquelle leurs données sont conservées.
Assurez-vous que toute connexion à Internet, à d'autres réseaux externes ou à des systèmes d'information est effectuée au moyen d'interfaces contrôlées (p. ex. les serveurs mandataires, les passerelles, les routeurs, les coupe-feu, les tunnels chiffrés).	H	O	CJIS	AWS dispose d'un nombre limité de points d'accès au système d'information en vue de permettre une surveillance plus complète des communications entrantes et sortantes et du trafic réseau. Ces points d'accès du client sont appelés des points de terminaison API, qui permettent aux clients d'établir une séance de communication sécurisée avec leur espace de stockage ou leurs instances informatiques dans AWS. Les clients ont la capacité de déployer différents outils et mécanismes pour surveiller le trafic et les activités, par exemple, les configurations VPC, les groupes de sécurité EC2, le pare-feu d'applications Web d'AWS et les connexions sécurisées par chiffrement. Pour en savoir plus, veuillez consulter https://aws.amazon.com/security/.

Employer des outils et des techniques pour surveiller les événements sur le réseau, détecter les attaques et repérer une utilisation non autorisée en tout temps.	S	O	CJIS	Les clients d'AWS profitent des services et des technologies d'AWS, conçus de A à Z pour leur permettre d'être résilients lorsqu'ils sont confrontés à des attaques DDoS et d'avoir des services qui comprennent une réponse automatique aux attaques DDoS, ce qui contribue à minimiser le temps requis pour atténuer et réduire les répercussions. Le client dispose d'une grande marge de manœuvre lui permettant de mettre en œuvre des capacités similaires dans son environnement client afin de surveiller les événements système, de détecter les attaques et de repérer les utilisations non autorisées en tout temps, en vue d'inclure les vulnérabilités et les tests d'intrusion. Pour en savoir plus, veuillez consulter : • https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf • https://aws.amazon.com/security • https://aws.amazon.com/security/penetration-testing/
S'assurer que l'arrêt du fonctionnement des mécanismes de protection des limites n'entraîne pas la divulgation non autorisée de renseignements à l'extérieur des limites du système d'information (c.-à-d. que la panne de l'appareil doit entraîner une « fermeture », et non une « ouverture »).	S	O	CJIS	Les utilisateurs d'AWS ont la possibilité d'adapter la configuration de leurs services de plusieurs façons pour respecter les exigences de sécurité en cas de panne.

Répartir les composantes du système d'information qui sont accessibles par le public (p. ex., les serveurs Web publics) sur des sous-réseaux indépendants qui ont des interfaces réseau distinctes.	S	H	ACCP-ICT	AWS n'exploite pas de composantes de système d'information accessibles au public (p. ex., les serveurs Web publics) à partir de l'infrastructure du nuage. Toutes les interactions de l'extérieur avec l'infrastructure utilisent un ensemble de points de terminaison API bien connus et structurés. Les serveurs Internet du compte client relèvent entièrement de son contrôle opérationnel. Pour en savoir plus, veuillez consulter : https://aws.amazon.com/whitepapers/aws-security-best-practices/.
Les données en transit sont chiffrées.	H	O	MITS	AWS offre plusieurs options de prise en charge du chiffrement des données en transit. On peut créer des tunnels chiffrés IPSec entre le point de terminaison d'un client et son VPC. Pour en savoir plus, veuillez consulter https://aws.amazon.com/vpc.
Les données inactives (locales ou sauvegardées) sont chiffrées.	H	O	MITS	AWS fournit plusieurs moyens pour chiffrer les données inactives. Par exemple, en utilisant Amazon S3, les clients peuvent télécharger des données en amont ou en aval en toute sécurité par l'intermédiaire des points de terminaison chiffrés SSL, à l'aide d'un protocole HTTPS. Amazon S3 peut chiffrer automatiquement les données de client inactives et offre plusieurs options de gestion des clés. Sinon, les clients peuvent utiliser une bibliothèque de chiffrement cliente telle que Amazon S3 Encryption Client pour chiffrer leurs données avant de les téléverser dans Amazon S3. Au besoin, Amazon S3 peut chiffrer les données inactives du client en utilisant le chiffrement côté serveur (SSE); Amazon S3 chiffrera automatiquement les données du client à mesure qu'elles sont écrites et il les déchiffrera au moment de les récupérer.

				Lorsqu'Amazon S3 SSE chiffre les données inactives, il utilise les clés symétriques 256 bits Advanced Encryption Standard (AES). Il existe trois façons de gérer les clés de chiffrement d'un chiffrement côté serveur dans Amazon S3 : • Chiffrement côté serveur (SSE) avec gestion des clés Amazon S3 (SSE-S3) : Amazon S3 chiffre les données inactives et gère les clés de chiffrement; • SEE utilisant les clés de chiffrement fournies par le client (SSE-C) : Amazon S3 chiffre les données inactives à l'aide des clés de chiffrement fournies par le client; ou • Chiffrement côté serveur (SSE) utilisant AWS KMS (SSE-KMS) : Amazon S3 chiffrera les données inactives en utilisant les clés qui sont gérées uniquement par le client dans AWS Key Management Service (KMS). Pour en savoir plus, veuillez consulter : • https://aws.amazon.com/s3/details/#security • https://aws.amazon.com/kms
Lorsqu'on utilise le chiffrement, les clés de chiffrement satisfont la norme AES 256 ou sont supérieures à celle-ci.	H	O	ACCP-ICT	AWS prend en charge AES 256.

Lorsqu'on utilise le chiffrement, le module de chiffrement utilisé sera certifié conforme aux normes FIPS 140-2.	S	H	MITS	AWS GovCloud (US) assure la conformité des points de terminaison aux exigences des normes FIPS 140-2. Les clients ont la capacité d'installer des modules conformes aux normes FIPS dans leur compte, si leur application est capable de prendre en charge les modules de chiffrement FIPS 140-2. Pour en savoir plus, veuillez consulter https://aws.amazon.com/federal/.
Les clés de chiffrement sont très sécuritaires et protégées, et elles sont offertes à l'organisme sur demande.	O	O	MITS	Utiliser AWS CloudHSM ou AWS KMS permet aux clients de créer et de gérer leurs propres clés de chiffrement. Pour en savoir plus, veuillez consulter : • https://aws.amazon.com/kms/ • https://aws.amazon.com/cloudhsm/
Les clés de chiffrement sont contrôlées et stockées par l'organisme.	S	H	ACCP-ICT	Utiliser AWS CloudHSM ou AWS KMS permet aux clients de créer et de gérer leurs propres clés de chiffrement. Pour en savoir plus, veuillez consulter : • https://aws.amazon.com/kms/ • https://aws.amazon.com/cloudhsm/

L'accès externe aux fonctions d'administration ou de gestion doit se faire par RPV uniquement. Ceci comprend les modems, les clients FTP ou les protocoles/ports dont le soutien est assuré par le fabricant du matériel. Cet accès doit se limiter aux utilisateurs dotés de l'authentification à deux facteurs.	S	H	NPISAB	Les clients peuvent se connecter à la console de gestion pour gérer leur environnement sur le RPV et exiger l'utilisation d'une authentification à deux facteurs, conformément aux exigences internes de l'organisme. Pour en savoir plus, veuillez consulter https://aws.amazon.com/iam/details/mfa/. Les connexions administratives à l'infrastructure d'AWS sont établies à l'aide de mécanismes sécurisés.
Les données de l'organisme ne seront pas utilisées par un fournisseur de services, et ce, pour quelque raison que ce soit. Il est interdit pour le fournisseur de services de balayer les fichiers de données dans le but d'explorer les données ou à des fins publicitaires.	O	O	ACCP-ICT	AWS n'accède pas au contenu du client et ne l'utilise pas, sauf en vertu d'une exigence légale, à quelque fin que ce soit autre que la gestion des services AWS et leur prestation aux clients et à leurs utilisateurs finaux. AWS n'utilise jamais le contenu des clients ni aucune information récupérée à des fins de marketing ou publicitaires. Pour en savoir plus, veuillez consulter https://aws.amazon.com/compliance/data-privacy-faq/. La politique de confidentialité d'AWS décrit comment AWS recueille et utilise les renseignements fournis par les clients pour la création ou la gestion des comptes AWS, et c'est pour cette raison qu'on les appelle des « renseignements sur le compte ». Par exemple, les renseignements sur le compte comprennent les noms, noms d'utilisateur, numéros de téléphone, adresses électroniques et renseignements de facturation associés au compte AWS d'un client. La politique de confidentialité d'AWS s'applique aux renseignements sur le compte des clients et ne s'applique pas au contenu stocké par les clients dans AWS, y compris tout renseignement de nature personnelle sur les utilisateurs finaux du client. AWS ne divulgue pas, ne déplace pas, n'accède pas et n'utilise pas le contenu du client, sauf si cela s'avère nécessaire en vertu de l'entente du client avec AWS. L'entente du client avec AWS (https://aws.amazon.com/agreement/) et la FAQ sur la protection des données d'AWS contiennent plus de renseignements sur la manière dont nous gérons les contenus que vous stockez dans nos systèmes.

Tous les pare-feu respectent la norme minimale Evaluation Assurance Level (EAL) 4.	H	O	NPISAB	AWS fournit plusieurs caractéristiques et plusieurs services pour aider les clients à protéger leurs données, y compris le pare-feu d'applications Web d'AWS. De plus, plusieurs fournisseurs dans AWS Marketplace offrent des produits de gestion de la sécurité semblables. Pour en savoir plus, veuillez consulter : • https://aws.amazon.com/waf/ • https://aws.amazon.com/marketplace
S'assurer d'effectuer régulièrement des balayages contre les virus et les logiciels malveillants et d'effectuer des tests d'intrusion dans l'environnement.	O	O	NPISAB	AWS s'assure d'effectuer régulièrement des balayages contre les virus et les logiciels malveillants et d'effectuer des tests d'intrusion dans l'environnement de l'infrastructure. Les clients peuvent aussi effectuer leurs propres tests d'intrusion dans leur compte. Pour en savoir plus, veuillez consulter https://aws.amazon.com/security/penetration-testing/.
Bien documenter leurs résultats de balayage contre les virus et les logiciels malveillants et de tests d'intrusion et, sur demande de l'organisme, le fournisseur fournira un rapport à jour.	H	O	ACCP-ICT	Les clients gardent le contrôle de leurs propres systèmes d'exploitation invités, ainsi que de leurs logiciels et applications, et il leur incombe d'exécuter des analyses de vulnérabilité et d'appliquer des correctifs sur leurs propres systèmes. Un client peut demander la permission de mener à bien des analyses sur l'infrastructure du nuage tant que celles-ci se limitent à ses propres instances et n'enfreignent pas la politique d'utilisation acceptable d'AWS. AWS analyse régulièrement toutes les adresses IP de tous les points de terminaison des services ayant accès à Internet à la recherche de vulnérabilités. Elle informe ensuite les parties concernées du résultat de ses analyses afin que celles-ci puissent corriger les vulnérabilités identifiées. Les opérations de maintenance et d'application des correctifs d'AWS n'ont généralement pas de répercussions sur les clients.

				Pour en savoir plus, consultez le livre blanc sur la sécurité d'AWS (accessible à https://aws.amazon.com/security/) et la norme ISO 27001, annexe A, domaine 12. La solution AWS a été validée et certifiée par un vérificateur indépendant afin de confirmer son respect de la norme de certification ISO 27001.
Bien documenter toute la gestion de correctifs et, sur demande de l'organisme, le fournisseur fournira un rapport à jour.	H	O	ACCP-ICT	Les clients gardent le contrôle de leurs propres systèmes d'exploitation invités, ainsi que de leurs logiciels et applications, et il leur incombe d'exécuter des analyses de vulnérabilité et d'appliquer des correctifs sur leurs propres systèmes. Un client peut demander la permission de mener à bien des analyses sur l'infrastructure du nuage tant que celles-ci se limitent à ses propres instances et n'enfreignent pas la politique d'utilisation acceptable d'AWS. AWS analyse régulièrement toutes les adresses IP de tous les points de terminaison des services ayant accès à Internet à la recherche de vulnérabilités. Elle informe ensuite les parties concernées du résultat de ses analyses afin que celles-ci puissent corriger les vulnérabilités identifiées. Les opérations de maintenance et d'application des correctifs d'AWS n'ont généralement pas de répercussions sur les clients. Pour en savoir plus, consultez le livre blanc sur la sécurité d'AWS (accessible à https://aws.amazon.com/security/) et la norme ISO 27001, annexe A, domaine 12. La solution AWS a été validée et certifiée par un vérificateur indépendant afin de confirmer son respect de la norme de certification ISO 27001.

Surveillance et enregistrement sur une base continue pour les événements suivants : • **Attaques par DDOS** • **Changements non autorisés appliqués au matériel, aux micrologiciels et aux logiciels** • **Anomalies du rendement du système** • **Signatures connues d'attaques**	S	O	MITS	AWS utilise différents outils et différentes techniques pour surveiller les événements sur le réseau et repérer une utilisation non autorisée en tout temps. Les clients d'AWS profitent des services et des technologies d'AWS, conçus de A à Z pour leur permettre d'être résilients lorsqu'ils sont confrontés à des attaques DDoS et d'avoir accès à des services qui comprennent une réponse automatique aux attaques DDoS, ce qui contribue à minimiser le temps requis pour atténuer et réduire les répercussions. Le client dispose d'une grande marge de manœuvre lui permettant de mettre en œuvre des capacités similaires dans son environnement client afin de surveiller les événements système, de détecter les attaques et de repérer les utilisations non autorisées en tout temps. Pour en savoir plus, veuillez consulter : • https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf • https://aws.amazon.com/security
Capacité à appliquer les politiques de conservation des données définies par le client.	S	H	ACCP-ICT	Bien que AWS donne aux clients la capacité de supprimer leurs données, les clients AWS conservent le contrôle et la propriété de leurs données et il leur incombe donc de gérer la conservation des données selon leurs propres exigences. AWS maintient les politiques de conservation des données conformément à plusieurs normes internationales et plusieurs règlements internationaux bien connus, notamment SOC et PCI-DSS, qui font l'objet d'une évaluation et d'une attestation indépendantes.

Exigences en matière de sécurité pour les centres de données

Exigence	Protégé A	Protégé B	Référence	Responsabilité d'AWS
Le centre de données doit disposer de moyens physiques pour empêcher l'entrée de personnel non autorisé.	H	O	MITS	AWS contrôle de façon stricte l'accès aux centres de données, même pour les employés internes. L'accès physique à tous les centres de données d'AWS qui hébergent des composants d'infrastructure de TI est restreint aux employés du centre de données, aux fournisseurs et aux sous-traitants autorisés qui ont besoin d'un accès dans le cadre de leurs fonctions. Les centres de données d'AWS sont surveillés par des agents de sécurité formés en tout temps. Puisque nos centres de données desservent de multiples clients, AWS ne permet pas aux clients de visiter les centres de données, car cela exposerait de nombreux clients à l'accès physique d'un tiers. Afin de satisfaire à cette exigence de client, un vérificateur indépendant compétent valide la présence et l'application des contrôles dans le cadre de notre rapport SOC 1 de type 2. Cette forme de validation par un tiers largement acceptée offre aux clients une perspective indépendante sur l'efficacité des contrôles mis en place.
Portes verrouillées, avec systèmes de contrôle d'accès qui restreignent l'entrée aux parties autorisées uniquement. Toutes les activités doivent être consignées.	H	O	GRC	L'accès physique aux centres de données d'AWS est géré par un système de contrôle d'accès et toutes les activités sont consignées.

Les journaux des privilèges d'accès du personnel doivent être conservés un minimum d'un an et fournis à l'organisme sur demande.	S	O	ACCP-ICT	Journaux d'accès physique conservés pendant un minimum d'un an. Les journaux d'accès sont fournis aux vérificateurs indépendants dans le cadre des audits officiels sur la conformité.
Les journaux des modifications aux accès du personnel doivent être conservés un minimum d'un an et fournis à l'organisme sur demande.	S	O	CJIS	Journaux d'accès physique conservés pendant un minimum d'un an.
L'édifice doit être fait de murs difficiles à percer.	S	O	GRC	Édifices construits conformément au code du bâtiment local (généralement en béton).

Authentification à deux facteurs requise pour entrer dans l'édifice qui abrite le centre de données.	S	H	MITS	L'accès aux centres de données d'AWS s'appuie sur une variété de mécanismes d'authentification à deux facteurs.
Vidéos en CCTV diffusées et enregistrées de toutes les entrées et sorties et de l'extérieur de l'édifice.	S	O	ACCP-ICT	Des systèmes de CCTV avec fonction d'enregistrement sont utilisés dans chaque centre de données d'AWS.
Agents de sécurité présents en tout temps à toutes les entrées principales de l'édifice. Les sacs et colis sont examinés au moment d'entrer.	S	O	CJIS	AWS emploie des agents de sécurité qui sont présents en tout temps à toutes les entrées principales de l'édifice et examinent systématiquement le contenu des sacs.

Authentification des visiteurs avant d'autoriser l'accès escorté au centre de données.	H	O	CJIS	L'accès physique à tous les centres de données d'AWS qui hébergent des composants d'infrastructure de TI est restreint aux employés du centre de données, aux fournisseurs et aux sous-traitants autorisés qui ont besoin d'un accès dans le cadre de leurs fonctions. Les visiteurs sont également escortés, au besoin.
Les données du client doivent être séparées logiquement (ou physiquement) des données des autres clients. Cette séparation doit être testée par un tiers impartial ou démontrée par la direction du centre de données.	S	H	CJIS	Toutes les données du client sont séparées logiquement par défaut en faisant appel au service Amazon VPC (Amazon Virtual Private Cloud), un service évalué par de multiples contrôleurs tiers. Pour en savoir plus, veuillez consulter https://aws.amazon.com/vpc/.
Possibilité d'indiquer dans quels centres de données les données d'organisme seront stockées et de les limiter.	S	O	ACCP-ICT	L'emplacement des données du client est déterminé par le client au niveau régional. AWS n'accède pas au contenu du client, ne l'utilise pas et ne le déplace pas, sauf en vertu d'une exigence légale, à quelque fin que ce soit autre que la gestion des services AWS et leur prestation aux clients et à leurs utilisateurs finaux.

Données d'organismes conservées dans une salle de serveurs protégée qui comprend : • **Des dispositifs de détection des vibrations sur les murs** • **Un système de détection des intrusions dans la salle de serveurs protégée** • **Une méthode d'authentification à deux personnes pour entrer dans la salle de serveurs protégée**	S	H	GRC	AWS emploie plusieurs couches de sécurité pour protéger les salles de serveurs au sein du centre de données (les « zones rouges »). AWS a aussi recours à plusieurs mécanismes de sécurité physiques, y compris des systèmes de détection des intrusions et l'authentification à deux personnes.
L'élimination des disques durs contenant des renseignements d'organismes comprend les étapes suivantes conformément à la norme canadienne ITSG-06 : 1. **Chiffrement ou écrasement des données** 2. **Destruction en au moins trois morceaux (broyage)**	S	O	GRC	AWS applique plusieurs étapes lors de son processus de mise hors service des supports de données comme les disques durs magnétiques (HDD) et électroniques (SSD). Sur place, les disques HDD sont démagnétisés, puis pliés, et les disques SSD passent par un écrasement logique des données avant d'être perforés. Ces deux types de supports sont par la suite déchiquetés en vue d'en recycler les matériaux. Les clients ont la possibilité d'appliquer eux-mêmes diverses méthodes de nettoyage, dont la suppression des données à l'aide d'outils sur mesure ou le chiffrement des données et la destruction de la clé de chiffrement afin de rendre les données inutilisables de façon permanente.

Exigences en matière de sécurité visant le personnel

Exigence	Protégé A	Protégé B	Référence	Responsabilité d'AWS
Tous les administrateurs de système et les employés ayant accès aux installations doivent se soumettre à une enquête de sécurité approfondie effectuée par un organisme d'application de la loi important. Un niveau d'habilitation fédéral canadien de « Secret » ou plus peut remplacer cette enquête et y équivaloir. Un niveau d'habilitation fédéral américain de « Secret » ou plus peut remplacer cette enquête et y équivaloir.	H	O	GRC	Tous les employés d'AWS doivent se soumettre à une vérification des antécédents complète avant leur embauche. De nombreux postes particuliers font aussi l'objet d'une vérification distincte relative aux emplois de confiance. En outre, de nombreux employés possèdent un niveau d'habilitation national américain (TS/SCI) (réévalué tous les cinq ans) ou sont soumis à un prélèvement d'empreintes et à une vérification des antécédents auprès des CJIS (Criminal Justice Information Services).
Tout le personnel passe par une vérification des antécédents avant l'embauche dans un centre de données. Les niveaux d'habilitation doivent être maintenus avant leur échéance. Tous les administrateurs de système et les employés ayant accès aux installations doivent se soumettre à une nouvelle vérification des antécédents tous les cinq ans.	H	O	GRC	Tous les employés d'AWS doivent se soumettre à une vérification des antécédents complète avant leur embauche. De nombreux postes particuliers font aussi l'objet d'une vérification distincte relative aux emplois de confiance. En outre, de nombreux employés possèdent un niveau d'habilitation national américain (TS/SCI) (réévalué tous les cinq ans) ou sont soumis à un prélèvement d'empreintes et à une vérification des antécédents auprès des CJIS (Criminal Justice Information Services). Les employés ayant un accès physique n'obtiennent pas d'accès logique.

L'accès aux installations est révoqué immédiatement au moment de la cessation d'emploi.	O	O	GRC	Au moment de sa cessation d'emploi, l'accès d'un employé aux systèmes et aux installations est immédiatement révoqué.
Une liste du personnel ayant obtenu une autorisation d'accès physique ou logique au centre de données et à ses systèmes doit être tenue à jour et fournie à l'organisme sur demande.	H	O	CJIS	AWS maintient une liste des employés ayant un accès physique accordé en vertu d'un processus particulier. Les listes d'accès logique sont conservées au sein de la structure de groupe de permission LDAP et ne constituent pas une liste amalgamée aux fins de distribution. L'ensemble de la gestion des accès physiques et logiques est vérifié de façon indépendante par de multiples vérificateurs tiers pour divers programmes de conformité officiels.
Le contractant doit appliquer une séparation des tâches, exiger la signature d'accords de non-divulgation commercialement raisonnables et limiter les connaissances du personnel concernant les données du client à ce qui est absolument nécessaire à leur travail.	H	O	GRC	AWS applique rigoureusement les principes de droit d'accès minimal, de séparation des rôles et des responsabilités et de divulgation des informations en fonction du besoin de les connaître.

Exigences relatives au contrôle des accès

Exigence	Protégé A	Protégé B	Référence	Responsabilité d'AWS
La longueur minimale des mots de passe doit être de huit caractères et ils doivent satisfaire à trois de ces quatre exigences de complexité : • **Majuscule** • **Minuscule** • **Caractères spéciaux** • **Chiffres**	H	O	CJIS	L'accès à l'infrastructure d'AWS nécessite une authentification multifactorielle qui comprend les exigences de complexité des mots de passe. Les clients peuvent mettre en œuvre cette exigence au sein de leur compte, lequel n'est pas géré par AWS en leur nom.
Les règles de mots de passe suivantes sont appliquées : • **Une restriction sur la réutilisation des mots de passe est appliquée** • **Une procédure de durée de vie des mots de passe est mise en œuvre et cette durée peut être configurée par l'organisme (normalement 90 jours)** • **Ne peut pas être un mot du dictionnaire ou un nom propre** • **Doit être différent de l'identifiant de l'utilisateur** • **Doit être différent des six derniers mots de passe**	H	O	CJIS/NPISAB	L'accès à l'infrastructure d'AWS nécessite une authentification multifactorielle qui comprend les exigences de complexité et de protection des mots de passe. Les clients peuvent mettre en œuvre cette exigence au sein de leur compte, lequel n'est pas géré par AWS en leur nom.

• **Doit être transmis et stocké en format chiffré** • **Ne doit pas être affiché lors de la saisie** • **La sauvegarde et la mise en cache automatiques des mots de passe par les applications doivent être désactivées**				
Une procédure de verrouillage de compte après un nombre de tentatives de connexion échouées est mise en œuvre et ce nombre peut être configuré par l'organisme (5 tentatives par défaut).	O	O	CJIS/NPISAB	Les clients peuvent mettre en œuvre cette exigence au sein de leur compte, lequel n'est pas géré par AWS en leur nom.
La réinitialisation de mot de passe s'appuie sur des questions de vérification de l'identité par courriel automatisé.	O	O	ACCP-ICT	Les clients peuvent mettre en œuvre cette exigence au sein de leur compte, lequel n'est pas géré par AWS en leur nom.

Une politique existe afin de garantir que les mots de passe ne sont pas communiqués par courriel ou au téléphone.	O	O	ACCP-ICT	Les clients peuvent mettre en œuvre cette exigence au sein de leur compte, lequel n'est pas géré par AWS en leur nom.
Lorsqu'un NIP (numéro d'identification personnel) est utilisé comme facteur d'authentification normalisé, les règles suivantes sont appliquées : • **Doit comporter un minimum de six chiffres** • **Ne doit pas contenir de chiffres qui se répètent (p. ex., 112233)** • **Ne doit pas contenir de séquence (p. ex., 12345)** • **Doit expirer au maximum après 365 jours (sauf si le NIP est un deuxième facteur)** • **Doit être différent des trois derniers NIP** • **Doit être transmis et stocké en format chiffré** • **Ne doit pas être affiché lors de la saisie**	H	O	CJIS	Les clients peuvent mettre en œuvre cette exigence au sein de leur compte, lequel n'est pas géré par AWS en leur nom.

Compteur de temps d'activité de système qui redirige l'utilisateur sur la page de connexion après un délai qui peut être configuré par l'organisme (verrouillage de session) (30 minutes par défaut).	O	O	CJIS	Les clients peuvent mettre en œuvre cette exigence au sein de leur compte, lequel n'est pas géré par AWS en leur nom.
Le système d'information affichera un message de notification du système qui peut être configuré par l'organisme.	S	H	CJIS	Les clients peuvent mettre en œuvre cette exigence au sein de leur compte, lequel n'est pas géré par AWS en leur nom.
Surveillance et enregistrement sur une base continue pour les événements suivants : • **Tentatives de connexion réussies et échouées** • **Tentatives réussies et échouées de consultation/modification/ suppression des autorisations, des fichiers, des répertoires ou des ressources du système**	S	O	MITS	AWS applique des exigences de journalisation et de surveillance conformes à diverses normes et exigences y compris ISO 27001, SOC, PCI DSS, FedRAMP, DoD CC SRG (U.S. Department of Defense Cloud Computing Security Requirements Guidance), CJIS et d'autres normes visant ces exigences.

• **Tentatives de modification de mot de passe réussies et échouées** • **Tentatives réussies et échouées de consultation/modification/ suppression des journaux de vérification**				
Utiliser des méthodes efficaces d'identification et d'authentification s'appuyant sur une infrastructure à clés publiques (ICP).	S	H	ACCP-ICT	Les clients peuvent mettre en œuvre cette exigence au sein de leur compte, lequel n'est pas géré par AWS en leur nom.

Versions du document

Date	Description
Mai 2017	Première publication