Le présent document définit les politiques et les lignes directrices appliquées par Leaseweb (les « Politiques ») par rapport à sa relation avec le client, particulièrement pour clarifier la manière dont le client peut utiliser les services et l'équipement, ainsi que le mode d'utilisation considéré comme inacceptable par Leaseweb. Ces politiques, ainsi que Les conditions de vente de Leaseweb, les spécifications de services ainsi que les niveaux de soutien et de service font aussi partie du contrat de vente et s'appliqueront aux services et à tout équipement fourni par Leaseweb.

CHAPITRE A. INTRODUCTION

1. DÉFINITIONS

1.1. En plus des définitions énoncées dans les conditions de vente, des niveaux de soutien et de service et des spécifications de services, les définitions suivantes s'appliquent :

Anonymiseur désigne un outil ou un dispositif qui permet d'accéder à Internet pour le compte d'un utilisateur par l'intermédiaire d'un serveur mandataire.

ARIN désigne l'American Registry for Internet Numbers.

Bombardement électronique désigne (i) l'envoi par courriel de copies d'un seul message à de nombreux destinataires ou (ii) l'envoi de fichiers ou de messages volumineux ou multiples à un seul destinataire dans une intention malveillante.

CCPE désigne le Centre canadien de protection de l'enfance, soit l'organisme de bienfaisance national canadien qui œuvre à combattre et à prévenir la violence à l'égard des enfants. Le CCPE exploite **Cyberaide.ca**, et offre d'autres services d'intervention, de prévention et d'éducation.

CIRA désigne l'Autorité canadienne pour les enregistrements Internet, soit la fondation, constituée en vertu des lois du Canada, qui gère le nom de domaine de premier niveau de code de pays (ccTLD) .ca pour le Canada.

Cyberaide.ca désigne la centrale canadienne de signalement des cas d'exploitation sexuelle d'enfants sur Internet.

DDoS désigne une attaque par déni de service distribué.

DNS désigne un système de noms de domaine, soit un système de dénomination hiérarchique et décentralisé pour les ordinateurs, les services ou d'autres ressources connectées à Internet ou à un réseau privé.

DNS inversé désigne le processus par lequel on arrive à déterminer le nom de domaine associé à une adresse IP. Ce processus est utilisé pour identifier le nom du fournisseur de services à qui est attribuée une adresse IP.

DoS désigne une attaque par déni de service.

DRDoS désigne une attaque par déni de service distribué et réfléchi.

Envoi s'entend de tout matériel du client (y compris son équipement) expédié ou transporté par un fournisseur désigné par ce dernier vers le centre de données ou à partir de celui-ci. Le client est le seul responsable de ses envois.

Expédition s'entend de tous les modes de transport (aérien, ferroviaire, routier et maritime) utilisés pour acheminer l'envoi du client, lesquels sont organisés par le transporteur choisi par ce dernier. Le client est seul responsable de l'expédition.

Fournisseur d'anonymiseur désigne une entreprise ou une organisation qui fournit ou met à disposition des anonymiseurs sur demande.

Fournisseur de RPV désigne une entreprise ou une organisation qui fournit services de RVP.

ICANN désigne l'Internet Corporation for Assigned Names and Numbers (Société pour l'attribution des noms de domaine et des numéros sur Internet), une organisation à but non lucratif et reconnue d'utilité publique qui est notamment responsable de gérer les espaces adresse IP et l'attribution des blocs d'adresses aux organismes d'enregistrement Internet locaux, de tenir à jour les registres d'identifiants de protocole Internet et de gérer l'espace des noms de domaine de premier niveau.

Infrastructure désigne l'équipement, le service et les instances qui prennent en charge le flux et le traitement de l'information, y compris le stockage, les serveurs et les composantes réseau.

IRC désigne le clavardage IRC (Internet Relay Chat).

LCAP désigne la *Loi canadienne antipourriel* et toute réglementation ou modification promulguée en vertu de celle-ci.

Liste noire désigne une liste de rejet qui est un système de contrôle de l'accès de base refusant l'accès à une liste ou à une catégorie précise d'utilisateurs ou d'adresses réseau ou IP, et permettant qu'un courriel envoyé par un utilisateur ou à partir d'une adresse réseau ou IP se trouvant sur ladite liste noire ne parvienne pas à destination.

Logiciel malveillant désigne tout type ou toute forme de logiciel malveillant ou hostile, et notamment des virus informatiques, des vers, des chevaux de Troie et des logiciels-espions (*maliciel*).

Nœud de sortie TOR désigne le nœud final par lequel est acheminé le trafic TOR avant d'atteindre sa destination finale.

NOC » (« *Network Operation Center* » en anglais) désigne le centre d'exploitation du réseau de Leaseweb.

Pourriel désigne l'envoi de télécommunications non sollicitées qui : ne respectent manifestement pas les règles antipourriel et sur les télécommunications non sollicitées, notamment la LCAP et les règles sur les télécommunications non sollicitées du Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) ou, selon le seul jugement de Leaseweb, qui causent des perturbations importantes ou suscitent des plaintes de la part d'autres utilisateurs. L'envoi massif de courriels commerciaux non sollicités et l'utilisation de systèmes de composition automatiques pour effectuer des appels vocaux promotionnels non sollicités sont des exemples d'utilisation interdite.

Registre PTR désigne un registre de pointeurs; il s'agit d'un type de registre de DNS qui transforme une adresse IP en un domaine ou un nom d'hôte.

Renseignements d'authentification désigne les données d'accès, les noms d'utilisateur, les mots de passe, les questions de sécurité, les clés, les jetons, les adresses URL et d'autres renseignements qui peuvent être utilisés pour l'accès au service.

RPV désigne un réseau privé virtuel; il s'agit d'un service qui déploie un réseau privé sur un réseau public afin de permettre aux utilisateurs d'envoyer et de recevoir des données sur des réseaux partagés ou publics comme si leurs appareils informatiques étaient directement connectés au réseau privé.

Test de pénétration s'entend de toute vérification de sécurité technique réalisée par le client sur l'infrastructure de Leaseweb, sous réserve que cette vérification soit conforme aux activités autorisées par Leaseweb en vertu de l'article 24 des présentes politiques.

TOR désigne « The Onion Router », soit un logiciel qui permet de communiquer de façon anonyme en acheminant le trafic par plusieurs nœuds anonymiseurs.

World Wide Web ou Web désigne un système de publication de documents faisant appel aux techniques de l'hypertexte, dans l'Internet.

2. GÉNÉRALITÉS

2.1. Leaseweb encourage un comportement hautement responsable dans le cadre de l'utilisation de ses services et, entre autres, de l'utilisation de l'Internet et du courrier électronique. Leaseweb a créé à cette fin les présentes politiques aussi connues sous le nom de politiques d'utilisation acceptable.

2.2. Chaque client doit se conformer aux annexes du Contrat de vente B2B, y compris les présentes politiques, et il doit s'assurer que les utilisateurs finaux connaissent les politiques et s'y conforment, de sorte que le client soit pleinement responsable de l'utilisation conforme de ses utilisateurs finaux des services de Leaseweb et qu'il puisse être tenu responsable à l'égard de tous ses utilisateurs finaux des services de Leaseweb. Une violation des politiques par un utilisateur final sera également considérée comme une violation des politiques par le client.

2.3. Leaseweb a le droit de publier de nouvelles versions et de modifier de la sorte ses politiques. Ces modifications peuvent s'appliquer aux contrats de vente existants ainsi qu'aux nouveaux contrats de vente pour tous les services, à moins que Leaseweb n'indique le contraire de façon formelle par écrit. Les modifications entreront en vigueur dès qu'elles seront publiées sur le site Web de Leaseweb (https://www.leaseweb.com/fr/about-us/legal/sales-contract); elles seront, en outre, directement applicables et lieront pleinement les parties, en dérogation à la disposition de l'article 2.3 des conditions de vente.

2.4 Le client (et ses utilisateurs finaux) doit (doivent) en tout remps se conformer aux exigences de connaissance du client de Leaseweb, lesquelles seront déterminées à l'entière discrétion de Leaseweb. Cette mesure est nécessaire afin de garantir que le client, son entreprise, son (ses) bénéficiaire(s), son (ses) administrateur(s), son (ses) actionnaire(s) et/ou d'autres membres du personnel concernés soient en règle, y compris en ce qui concerne la conformité aux restrictions et sanctions en matière de contrôle des exportations dans le cadre des exigences de la politique d'utilisation acceptable de Leaseweb. Si Leaseweb a des doutes raisonnables quant au statut conforme du client, de son activité et/ou en ce qui concerne son personnel, et/ou si le client est soumis à des restrictions ou sanctions en matière de contrôle des exportations au niveau local ou mondial, quelle qu'en soit la source, Leaseweb est en droit de suspendre immédiatement le client, de résilier le contrat de vente et de cesser tous les services, sans que Leaseweb ne soit tenue responsable des frais, dépenses et dommages-intérêts découlant de la non-conformité par le client (et/ou de ses utilisateurs finaux) à la politique d'utilisation acceptable de Leaseweb, y compris les exigences de connaissance du client de Leaseweb et/ou de la résiliation du contrat de vente et la cessation des services, tel que Leaseweb en avait avisé le client.

3. PERSONNES-RESSOURCES

3.1. Le client doit désigner (i) des personnes-ressources qu'Leaseweb peut contacter à tout moment en rapport avec des violations (soupçonnées) des politiques par le client ou ses utilisateurs finaux et (ii) des personnes-ressources qu'Leaseweb peut contacter à tout moment en cas d'urgence.

3.2. Le client fournira à Leaseweb un moyen de contacter les personnes-ressources en tout temps et s'assurera que l'information indiquée dans le portail client au sujet de ces personnes-ressources est à jour et reste à jour.

4. RENSEIGNEMENTS D'AUTHENTIFICATION

4.1. Certains services peuvent être accessibles uniquement grâce à l'utilisation des renseignements d'authentification. Le client est l'unique responsable de la mise à jour, de la sécurité et de l'utilisation de ses renseignements d'authentification. Toutes les conséquences et pertes liées à l'utilisation des renseignements d'authentification du client, que le client ait ou non autorisé cette utilisation, sont à la charge et sous la responsabilité exclusive du client, y compris toutes les affaires et communications menées avec Leaseweb grâce à l'utilisation de ses renseignements d'authentification.

4.2. Dans la mesure du possible, le client doit modifier ses renseignements d'authentification dès qu'il les reçoit, et régulièrement par la suite. Le client s'assure d'utiliser les pratiques exemplaires en produisant les renseignements d'authentification. Si le client sait ou soupçonne que la sécurité de ses renseignements d'authentification a été compromise ou que ses renseignements d'authentification ont été utilisés incorrectement, il doit en informer Leaseweb dès que possible et modifier sur-le-champ ses renseignements d'authentification.

CHAPITRE B. POLITIQUE D'UTILISATION ACCEPTABLE

5. UTILISATION DES SERVICES

5.1. Le client garantit, déclare et affirme que lui et ses utilisateurs finaux utilisent l'équipement et les services uniquement :

i. à des fins licites;

ii. conformément au Contrat de vente, aux annexes du contrat de vente B2B de Leaseweb (comprenant les conditions de vente B2B, les politiques, les spécifications de services et les ententes sur les niveaux de service) et aux lois en vigueur (au Canada et ailleurs dans le monde).

5.2. Sans préjudice de la loi applicable au contrat de vente, le client reconnaît et accepte que l'utilisation de l'équipement et des services par lui-même et ses utilisateurs finaux doit être conforme aux lois (obligatoires) du Canada et de la province du Québec, ainsi qu'aux autres lois applicables au client ou à son utilisation de l'équipement et des services.

5.3. Le client doit s'abstenir de toute utilisation de l'équipement et des services qui pourrait avoir un effet préjudiciable à la bonne réputation de Leaseweb, nuire aux opérations commerciales de Leaseweb, exposer Leaseweb à un litige ou faire en sorte que Leaseweb enfreigne les lois en vigueur.

5.4. Leaseweb interdit au client, à ses utilisateurs finaux ou à tout autre tiers l'utilisation de l'équipement et des services pour certaines activités telles que l'hébergement, le stockage, la distribution, le traitement ou toute autre forme de mise à disposition de contenu ou de matériel à des fins liées aux activités suivantes : i) terrorisme; ii) menacer de nuire à des personnes ou à des biens ou adopter un comportement de harcèlement; iii) compromettre la sécurité (ou altérer) des ressources du système ou des comptes d'autres clients ou de tout autre site

Internet ou intranet sans autorisation appropriée; iv) enfreindre les lois locales de contrôle des exportations de logiciels ou d'informations techniques; v) utiliser, transmettre ou distribuer des données ou du matériel protégés par des droits de propriété intellectuelle sans autorisation appropriée; vi) fabriquer, utiliser ou distribuer des logiciels ou d'autres produits contrefaits, piratés ou illégaux; vii) fournir ou offrir une rémunération aux utilisateurs finaux en fonction du volume de téléchargement, à moins que le client sache (ou n'aie aucune raison de douter) que les utilisateurs finaux n'utilisent les services du client qu'à des fins légales et pour la distribution ou la diffusion de leurs propres données ou documents, ou de données ou de documents qu'ils sont dûment autorisés à distribuer ou à diffuser; viii) faire des représentations frauduleuses de produits ou de services; ix) pollupostage, hameçonnage, attaques par déni de service (DoS), attaques par déni de service distribué (DDoS), attaques par déni de service distribué et réfléchi (DRDoS), manipulation de transfert de données ou installation de programmes informatiques sur des systèmes de tiers sans autorisation appropriée; x) téléversement, stockage, distribution ou toute autre forme de mise à disposition de contenu ou de matériel interdit ou illégal dans toute juridiction concernée, y compris tout matériel diffamatoire ou obscène contenant de la zoophilie, de la pédopornographie, de la pédopornographie virtuelle et de l'érotisme enfantin; xi) accès intentionnel à un système informatique ou à un composant de la structure de l'infrastructure sans autorisation ou avec dépassement des niveaux d'accès autorisés de celui-ci; xii) distribution de virus ou de toute autre technologie pouvant nuire à Leaseweb ou aux intérêts ou à la propriété d'autres clients ou personnes; xiii) le moissonnage de données ou toute autre forme de collecte de données, ou l'utilisation de renseignements au sujet d'autres clients sans autorisation; xiv) le contournement de toute mesure mise en place par Leaseweb pour fournir ou gérer les services ou toute interférence avec le fonctionnement des services; xv) activités qui peuvent entraîner le placement ou l'inscription sur une liste noire du client, des adresses IP du client ou des adresses IP attribuées par Leaseweb au client; xvi) examens et tests de pénétration non autorisés; xvii) faciliter, aider ou encourager l'une des activités susmentionnées. Le client et ses utilisateurs finaux ne doivent pas utiliser l'équipement et les services à toutes fins liées à ces activités interdites.

5.5. Le client reconnaît que toute utilisation des services par lui-même et/ou ses utilisateurs finaux en violation de la politique d'utilisation acceptable pourrait entraîner pour lui-même et ses utilisateurs finaux des responsabilités pénales ou civiles, en plus d'autres mesures prises par Leaseweb et définies dans 0 des politiques et dans les conditions de vente.

5.6 Le client, agissant en son nom et en celui de ses bénéficiaires ultimes, sociétés affiliées, succursales, utilisateurs finaux et résidents de certains pays où le client engage sa responsabilité (conformément à la *Affiliates Rule* des États-Unis), ci-après désigné par le « **client c. s.** », s'engage à ne pas :

i. commander, acheter, utiliser, vendre, revendre, accorder de licence ou de sous-licence, exporter, réexporter ou transférer (dans le pays) de quelque manière que ce soit les services configurés avec des GPU (puces) réglementés de Leaseweb. Par « GPU réglementé », on entend tout produit, y compris le matériel, les logiciels et les technologies, qui contrevient directement ou indirectement aux lois américaines sur le contrôle des exportations en vertu de la réglementation américaine sur l'administration des exportations (« *Export Administration Regulations* », « **EAR** ») ou de toute autre règle connexe imposée par le *Bureau of Industry and Security* (« **BIS** »), notamment les produits L4, L40, L40S, H100, H200 et A100.

ii. être établi directement ou indirectement dans certains pays répertoriés dans les catégories de pays définies par le BIS (D:1, D:4, D:5 et E, y compris Hong Kong, considéré comme faisant partie de la Chine) ou être constitué en vertu des lois de ces pays. Les pays figurant à l'annexe 1 de la section 740 de la EAR et ses révisions ultérieures (les « **pays interdits** ») sont les suivants : Afghanistan, Arménie, Azerbaïdjan, Bahreïn, Biélorussie, Birmanie, Cambodge, République centrafricaine, Chine (y compris Hong Kong), République démocratique du Congo, Cuba, Égypte, Érythrée, Géorgie, Haïti, Iran, Irak, Israël, Jordanie, Kazakhstan, Corée du Nord, Kirghizistan, Koweït, Laos, Liban, Libye, Macao, Moldavie, Mongolie, Nicaragua, Oman, Pakistan, Qatar, Russie, Arabie saoudite, Somalie, République du Sud-Soudan, Soudan, Syrie, Tadjikistan, Turkménistan, Émirats arabes unis, Ouzbékistan, Venezuela, Viêt Nam, Yémen et Zimbabwe.

iii. être considéré comme un utilisateur final à des fins militaires ou gouvernementales (au sens de la partie 772 de la EAR), ou comme un utilisateur final des services à des fins militaires, y compris pour des armes de destruction massive (les « **secteurs interdits** »).

iv. commander, acheter, utiliser, vendre, revendre, accorder de licence ou de sous-licence, exporter, réexporter ou transférer (dans le pays) le service de quelque manière que ce soit ni utiliser les services à des fins de production de circuits intégrés (CI) informatiques avancés ou de fonctionnalités similaires destinés au développement de semi-conducteurs ou de superordinateurs dans les pays interdits susmentionnés (partie 744 de la EAR).

5.7 Conformément à la réglementation sur le contrôle des exportations d'articles à double usage en vigueur, les services ne doivent être utilisés qu'à des fins civiles. Le client c. s. garantit qu'il n'utilisera pas les services à des fins militaires ou pour la fabrication d'armes de destruction massive, sauf s'il s'agit d'un utilisateur final militaire ou gouvernemental.

5.8 Conformément à la *Affiliates Rule*, le client c. s. est assujetti aux régimes de sanctions de l'Union européenne, du Département du Trésor des États-Unis, de l'*Office of Foreign Asset Controls* (« **OFAC** »), y compris la *Specially Designated Nationals List*, soit la liste des personnes, entités et groupes soumis à des sanctions de la part de l'OFAC, ainsi qu'à ceux des pays où Leaseweb et le client c. s. sont établis.

5.9 Ces obligations du client c. s. sont assujetties aux garanties du client prévues dans les conditions de vente de Leaseweb, ainsi qu'aux dispositions relatives à la connaissance du client de l'article 2 des politiques et aux droits et recours de Leaseweb en matière de suspension et de résiliation, comme prévu dans les conditions de vente de Leaseweb.

5.10 Les modalités des conditions de licence des processeurs graphiques (UTG) réglementés et non réglementés qui s'appliquent au client sont définies aux articles 40.6 à 40.8 des spécifications des services.

5.11 Leaseweb a mis en place une politique relative aux activités commerciales restreintes en vertu de laquelle la vente, la fourniture ou l'utilisation des services de Leaseweb à des clients c.s. établis ou exerçant leurs activités dans les pays et territoires suivants est interdite : Cuba, Iran, Corée du Nord, Syrie, Russie, Bélarus, Soudan, Myanmar, Venezuela, régions occupées de l'Ukraine (Crimée, Donetsk et Luhansk). De plus, Leaseweb peut limiter la vente, la fourniture ou l'utilisation de ses services dans les pays qui, selon elle, présentent un risque élevé (les « **activités commerciales restreintes** »). Leaseweb se réserve le droit de refuser, de suspendre ou d'annuler toute commande ou de résilier tout contrat de vente impliquant, directement ou indirectement, des activités commerciales restreintes.

6. MESSAGES ÉLECTRONIQUES / ANTIPOLLUPOSTAGE

6.1 Le client ne peut pas (i) envoyer de messages électroniques qui, de quelque façon que ce soit, sont ou peuvent être en infraction avec la LCAP, les règles sur les télécommunications non sollicitées du CRTC ou les lois applicables, (ii) envoyer ou propager et permettre à ses utilisateurs finaux ou tierces parties d'envoyer ou de propager des pourriels via des adresses IP du client, (iii) envoyer ou propager des bombes

électroniques, ou y répondre, et ne doit pas permettre à ses utilisateurs finaux ou tierces parties d'envoyer ou de propager des bombes électroniques via des adresses IP du client ou (iv) modifier les en-têtes de messages électroniques pour dissimuler l'adresse du client ou pour empêcher les destinataires de répondre aux messages.

6.2 Le client doit s'abstenir d'activités qui peuvent entraîner l'inscription du client ou des adresses IP du client sur une liste noire. Leaseweb se réserve le droit de facturer au client les frais de retrait express stipulés sur le site Web UCEProtect pour l'inscription7 au niveau 2 d'une ou de plusieurs plages d'adresses IP de Leaseweb ou l'inscription au niveau 3 de numéros de système autonome (ASN) de Leaseweb ou des frais de consultation de quatre cents dollars canadiens (CA$ 400) par heure pour des mesures correctrices qu'Leaseweb choisit de prendre lorsque, à cause d'activités du client ou des utilisateurs finaux du client, les serveurs ou les adresses IP de Leaseweb sont inscrits dans le logiciel de filtrage ou la liste noire d'une tierce partie ou les plages d'adresses IP et/ou les ASN de Leaseweb sont inscrits sur la liste noire d'UCEProtect.

6.3 Les messages en bloc ne sont permis que si (i) le client a obtenu le consentement explicite de chacun des destinataires au moyen de l'option d'inclusion confirmée ou si (ii) les lois applicables permettent l'envoi de tels messages avec ou sans le consentement implicite des destinataires. Le client est obligé d'offrir dans chaque message électronique un mécanisme de désabonnement fonctionnel et facilement accessible, et le client doit cesser d'envoyer des messages électroniques à un destinataire dès qu'il se désabonne, et ce, rapidement, au plus tard avant l'expiration du délai prescrit par la loi.

7. UTILISATION D'INTERNET

7.1. Il est interdit au client d'afficher ou de transmettre du matériel illégal sur ou via l'Internet ou le World Wide Web.

7.2. Leaseweb a le droit de bloquer activement des ports ou des adresses IP pour le réseau, si elle a des raisons de penser que c'est nécessaire pour préserver ou protéger la sécurité et la performance du réseau, de l'Internet ou du World Wide Web. Le client peut demander par écrit à Leaseweb un aperçu des adresses IP et des ports bloqués.

7.3. Sans préjudice de la généralité de l'article 7.2 de la politique d'utilisation acceptable, Leaseweb doit, en tous les cas, bloquer activement les ports suivants pour son réseau : (i) UDP/137 – Netbios, (ii) UDP/139 – Netbios, (iii) TCP/135 à 139 – Netbios, (iv) TCP/445 – SMB et (v) Port UDP 11211 – Memcached.

7.4. Si Leaseweb a des raisons de soupçonner ou sait que le client subit une attaque DoS, DDoS, DRDoS ou autre et, selon son avis raisonnable, qu'une telle attaque a un effet négatif sur l'infrastructure, Leaseweb a le droit de bloquer immédiatement l'accès à l'infrastructure du client. Si le client fait l'objet d'attaques répétitives et s'il ne réussit pas à prendre des mesures adéquates pour empêcher que de futures attaques aient un effet négatif sur l'infrastructure de Leaseweb, Leaseweb a le droit de résilier sur-le-champ le contrat de vente en envoyant un avis écrit au client.

8. UTILISATION D'IRC

8.1. Il est interdit au client d'afficher ou de transmettre du matériel inapproprié au moyen du clavardage IRC ou d'utiliser autrement IRC d'une manière qui contrevient à la politique d'utilisation acceptable. Aux fins du présent article, les usages interdits d'IRC comprennent les robots IRC « eggdrop » et l'hébergement psybnc sur shell.

8.2. Sans le consentement préalable écrit de Leaseweb, qu'Leaseweb peut accorder ou refuser à son unique et entière discrétion, il est interdit au client d'héberger un serveur IRC, qu'il s'agisse d'un serveur IRC autonome ou connecté aux réseaux IRC mondiaux.

9. UTILISATION DU PORTAIL CLIENT

9.1. Sous réserve des conditions d'utilisation appliquées de temps à autre par Leaseweb, des dispositions du contrat de vente et de l'observation des dispositions par le client, Leaseweb accordera un droit non exclusif, incessible, ne pouvant faire l'objet d'une sous-licence et libre de redevances afin d'utiliser le portail client pendant la durée du contrat. L'utilisation du portail client par le client ou en son nom se fait aux risques du client et sous sa responsabilité.

9.2. Le client doit observer chacune des instructions de Leaseweb concernant l'utilisation du portail client.

10. UTILISATION ET ENREGISTREMENT DES ADRESSES IP DE DOMAINE ET DES NUMÉROS DE SYSTÈME AUTONOME (ASN)

10.1. Le client doit se conformer aux politiques, aux lignes directrices et aux conditions appliquées de temps à autre par l'organisation ou l'entité responsable de la gestion (enregistrement et/ou distribution et/ou mise en service) d'un domaine (Internet), par exemple de l'ICANN.

10.2. Le client doit se conformer aux politiques, aux lignes directrices et aux conditions appliquées de temps à autre par l'organisation ou l'entité responsable de la gestion (enregistrement et/ou distribution et/ou mise en service) d'adresses IP et de numéros de système autonome (ASN), c'est-à-dire les organismes d'enregistrement Internet locaux de l'ACEI.

11. RESTRICTIONS DE L'UTILISATION DES SERVICES D'HÉBERGEMENT WEB PARTAGÉ

11.1. Le client ne peut pas :

a) utiliser les services d'hébergement Web partagé d'une manière susceptible d'entraver ou de perturber les services offerts aux autres clients de Leaseweb ou l'infrastructure de Leaseweb ou de causer une urgence;
b) dépasser les limites des services d'hébergement Web partagé, par exemple l'espace disque ou la bande passante attribués;
c) exécuter des tâches planifiées, telles que des saisies CRON, à des intervalles de moins de quinze (15) minutes;
d) exécuter des processus ou des démons autonomes, non liés, du côté serveur, sur la plateforme d'hébergement Web partagé;
e) envoyer plus de 3 courriels par minute ou 180 courriels par heure;
f) utiliser les services d'hébergement Web partagé pour héberger des scripts de messagerie Mailer Pro et à bouton de commande, des scripts de proxy et des anonymiseurs, des sites autoSurf/PTC/PTS/PPC, des robots d'indexation et de collecte, des indexeurs, des services de bandeau publicitaire (rotation de bandeaux publicitaires commerciaux).

11.2. Si Leaseweb détecte des tentatives infructueuses de connexion aux services d'hébergement Web partagé, elle peut, sans préavis et sans responsabilité ou autre obligation de quelque nature que ce soit, interdire à la source de ces tentatives infructueuses l'accès au réseau.

CHAPITRE C. POLITIQUE DE CONFORMITÉ EN CAS D'ABUS

12. EXIGENCES DE TRAITEMENT DE L'UTILISATION ABUSIVE

12.1. En ce qui a trait à l'utilisation des services de Leaseweb, le client doit adopter et appliquer une procédure de traitement de l'utilisation abusive qui est conforme aux politiques, à la loi applicable au contrat de vente et à toute autre loi applicable au client.

12.2. Le client doit journaliser (date et horodatage) chaque avis d'utilisation abusive (telle que définie ci-dessous) qu'il reçoit de Leaseweb et de la part de tiers, y compris la nature de l'avis (par exemple, une violation de droits d'auteur), ainsi que sa réponse à cette plainte, et le moment où il estime que l'avis est résolu.

12.3. Le client doit tenir à jour le journal relatif à chaque avis d'utilisation abusive pendant au moins trois (3) ans après la date à laquelle il juge un tel avis résolu. À la demande de Leaseweb, le client devra lui fournir une copie de son journal d'avis d'utilisation abusive.

12.4. Le client doit s'assurer de la disponibilité d'un nombre suffisant d'employés convenablement formés pour vérifier si ses utilisateurs finaux se conforment aux politiques et afin d'appliquer sa procédure de traitement des avis d'utilisation abusive et de traiter sans délai le volume d'avis d'utilisation abusive qu'il reçoit.

12.5. Si le client est un fournisseur de RPV ou un fournisseur d'anonymiseur, il est tenu de respecter les exigences suivantes dans le cadre de l'utilisation des services :

i. Les renseignements de son entreprise doivent être visibles et disponibles sur son site Web (on doit notamment y retrouver une adresse courriel accessible au public pour le traitement des cas d'utilisation abusive et des plaintes liées aux droits d'auteur);

ii. Il doit conclure un accord d'utilisation avec ses utilisateurs finaux. Cet accord doit comprendre des dispositions visant à assurer la conformité de l'utilisateur final avec la loi applicable, et notamment la législation sur la propriété intellectuelle, et les politiques;

iii. Il doit ternir des registres précis des registres de DNS inversé et des registres PTR, comprenant ses données d'identification pour toutes les adresses IP utilisées par lui-même et/ou ses utilisateurs finaux pour fournir des services de RPV ou d'anonymiseur;

iv. À la demande de Leaseweb, et à la seule discrétion de Leaseweb, il doit fournir les informations pertinentes requises pour qu'Leaseweb mette à jour ses bases de données WHOIS de référence ainsi que le registre régional d'adresses IP correspondant, et ce, dans un délai raisonnable comme indiqué dans la demande;

v. Il doit se conformer à la politique contre les récidivistes de l'article 14;

vi. Il doit mettre en œuvre et appliquer des mesures raisonnables pour empêcher un utilisateur final – dont le contrat a été résilié en raison de violations répétées – de recommencer à utiliser ses services ou à utiliser des services par son intermédiaire;

vii. Il doit mettre en œuvre et appliquer des mesures techniques visant à empêcher les activités non conformes ou illicites.

12.6. Si le client est un opérateur de nœud de sortie TOR, il est tenu de se conformer aux exigences suivantes dans le cadre de l'utilisation des services : (i) il doit, en tout état de cause, fermer/bloquer activement les ports dont l'utilisation est généralement connue ou qui sont généralement associés à des activités non conformes ou illicites, dont la liste peut être publiée de temps à autre par Leaseweb ou fournie aux clients, (ii) ses registres de DNS inversé doivent commencer par « tor.exit.node. », (iii) il doit ajouter une adresse courriel fonctionnelle au fichier « torrc » pour permettre aux utilisateurs finaux ou aux tiers qui le demandent de le contacter directement.

13. PROCÉDURE DE TRAITEMENT DE L'UTILISATION ABUSIVE

13.1. Si Leaseweb est informée par une tierce partie (y compris tout organisme d'application de la loi) d'une violation (soupçonnée) de la politique d'utilisation acceptable et/ou de toute loi applicable (un **« avis d'utilisation abusive »**) par le client et/ou un utilisateur final, elle doit en aviser le client par courriel ou par toute autre méthode de communication qu'elle juge appropriée.

13.2. Le client doit, pendant la période de réponse ou de traitement énoncée dans l'avis de Leaseweb (la **« période de remédiation »**), prendre des mesures correctrices pour remédier à la violation et informer Leaseweb des mesures qu'il a prises.

13.3. Dans certains cas, Leaseweb peut accorder au client la possibilité de contester la violation présumée en déposant un contre-avis (un **« contre-avis »**). Si le client choisit de déposer un contre-avis, il doit utiliser le formulaire en ligne mis à sa disposition à cette fin. Leaseweb doit examiner l'information soumise et peut, à sa seule discrétion, décider de rejeter le contre-avis du client et exiger que le client prenne des mesures correctrices immédiates si, à la seule discrétion de Leaseweb, les actions ou le contenu du client ou de l'utilisateur final sont indéniablement illégaux et/ou peuvent exposer Leaseweb à des réclamations de tiers et/ou à des litiges.

13.4. Si Leaseweb ne rejette pas le contre-avis du client, le client doit, à la demande de Leaseweb, fournir un dépôt, une garantie bancaire, une garantie de société mère ou toute autre sûreté à la satisfaction de Leaseweb. Le niveau de sûreté est déterminé par Leaseweb, à sa seule discrétion. La sûreté est destinée à couvrir les obligations du client et toute réclamation de Leaseweb, selon l'indemnité précisée dans les conditions de vente. De plus, dans le cas où le client dépose un contre-avis, il doit informer Leaseweb, dans les deux (2) jours suivant sa réponse à Leaseweb, si un avocat le représentera et, le cas échéant, fournir à Leaseweb les coordonnées de l'avocat.

13.5. Le client doit fournir à Leaseweb tous les documents et tous les renseignements relatifs à l'avis d'utilisation abusive sans frais et à première demande.

13.6. Comme condition de continuer à fournir les services et/ou de reprendre la prestation des services, Leaseweb a le droit de demander au client : (i) d'exécuter une déclaration de cessation et d'abstention et/ou, le cas échéant, (ii) de confirmer par écrit que l'utilisateur final du client responsable de la violation a été exclu définitivement de l'utilisation des services.

14. CONTREVENANTS RÉCIDIVISTES ET DIFFUSIONS VIDÉO EN DIRECT

14.1. Dans le cadre de sa procédure de traitement de l'utilisation abusive, le client doit faire tous les efforts raisonnables pour déceler des tentatives répétées de ses utilisateurs finaux de stocker, de transférer ou de distribuer – sur ses services ou par l'entremise de ceux-ci – du matériel ou des données (i) qui enfreignent la politique d'utilisation acceptable ou (ii) qu'il a préalablement supprimés ou désactivés à la suite de la réception d'un avis d'utilisation abusive.

14.2. Le client doit cesser immédiatement de fournir le service à un utilisateur final et mettre fin à l'accès de l'utilisateur final au service si l'on découvre que l'utilisateur final est un contrevenant récidiviste ou qu'il enfreint la politique d'utilisation acceptable de Leaseweb.

14.3. Le client doit, sur demande, démontrer qu'il respecte les exigences suivantes :

a) Confirmer qu'il a élaboré et mis en place une politique relative aux violations répétées du droit d'auteur;

b) Publier une politique ou un énoncé rendu public concernant l'interdiction d'utiliser ses services de manière à porter atteinte au droit d'auteur;
c) Désigner publiquement un responsable chargé du respect des droits d'auteur (et fournir une adresse courriel publique.

14.4. Si le client utilise les services de façon répétée pour la diffusion en continu de vidéos ou de contenus audio en direct, il doit mettre à la disposition des tiers de confiance (ou de leurs agents) un outil en ligne leur permettant d'interrompre immédiatement les diffusions en direct qui enfreignent leurs droits de propriété intellectuelle.

CHAPITRE D. POLITIQUE D'UTILISATION RAISONNABLE

15. CONNECTIVITÉ IP

15.1. Le service de connectivité IP est fourni pour une utilisation homogène, équitable et raisonnable par le client.

15.2. L'utilisation du service de connectivité IP par le client sera jugée inéquitable et déraisonnable si Leaseweb détermine (à sa seule discrétion) que l'utilisation réelle ou projetée du service de connectivité IP par le client dépasse ou est susceptible de dépasser la totalité de la bande passante engagée mensuelle ou du trafic de données engagé mensuel, et qu'une telle utilisation a des répercussions sur la prestation des services par Leaseweb à d'autres de ses clients. Aux fins de l'interprétation du présent article **Error! Reference source not found.** uniquement, si le client n'a pas convenu d'une quantité de bande passante engagée ou de trafic de données engagé (selon le cas), celle-ci sera établie en fonction de la plus petite quantité de bande passante engagée ou du trafic de données engagé offerte par Leaseweb pour le service respectif.

15.3. L'utilisation de la connectivité IP par le client sera jugée incohérente si ses habitudes d'utilisation de la bande passante ou du trafic de données, soit par serveur, soit à l'intérieur d'un groupe de serveurs ou d'instances du client, sont irrégulières.

15.4. Si les habitudes d'utilisation du trafic du client se traduisent par un pourcentage d'acheminement d'un même numéro de système autonome (ASN) vers une certaine destination ASN supérieur aux pourcentages indiqués ci-dessous (le « **seuil d'ASN** »), le trafic de données ou la bande passante dépassant le seuil d'ASN sera facturé à 3,00 EUR (trois euros ou l'équivalent en devise locale) par To ou à 0,75 EUR (soixante-quinze centimes d'euro ou l'équivalent en devise locale) par Mbit/s, en plus du tarif contractuel.

Table 1: Seuils d'ASN

DESTINATION ASN	RÉGION	SEUIL ASN
AS701 (Verizon)	US	10 %
7922 (Comcast)	US	10 %
20115 (Charter)	US	10 %
7018 (AT&T)	US	10 %
AS9121 (Turktelecom)	EU	10 %
AS3320 (DTAG)	EU	5 %
AS3352 (Telefonica)	EU	10 %
AS3215 (Orange)	EU	10 %

16. ÉQUIPEMENT DÉDIÉ

16.1. Les équipements dédiés sont fournis au client dans des bâtis privés et des bâtis partagés. Pour protéger la performance et l'intégrité des bâtis, le client doit s'assurer, en ce qui concerne tout l'équipement dédié, que sa consommation d'électricité, du réseau et de la ressource d'équipement dédié, et notamment des dispositifs de stockage, est équitable et raisonnable.

16.2. La consommation par le client de l'électricité, du réseau et de la ressource d'équipement dédié est jugée inéquitable et non raisonnable si elle dépasse la limite de consommation d'électricité (comme convenu dans l'aperçu du contrat) ou l'utilisation prévue du réseau et de la ressource d'équipement dédié, y compris les dispositifs de stockage, de telle manière que, à la seule discrétion de Leaseweb, elle peut affecter l'utilisation d'un autre équipement du client de Leaseweb dans le bâti partagé et la performance d'une autre infrastructure dans les bâtis ou dépasser l'utilisation prévue de la ressource d'équipement dédié, ce qui en réduit grandement la durée de vie.

16.3. Les équipements dédiés dans les bâtis partagés sont fournis au client dans un bâti partagé avec d'autres clients de Leaseweb et, par conséquent, la consommation d'électricité par le client dépassant la limite de consommation d'électricité peut affecter la performance (comme le temps d'attente, la bande passante de stockage et les opérations d'entrée/sortie par seconde) de l'équipement dédié dans les bâtis partagés. Pour protéger la performance et l'intégrité des équipements dédiés, le client doit s'assurer que sa consommation d'électricité, du réseau et de la ressource d'équipement dédié est équitable et raisonnable.

17. SERVICES INFONUAGIQUES

17.1. La capacité de calcul de la plateforme infonuagique pour les services de nuage public est fournie au client sur une base partagée. Pour protéger la performance et l'intégrité de la plateforme infonuagique, le client doit s'assurer, en ce qui a trait au service de nuage public, que son utilisation de la capacité de calcul est équitable et raisonnable.

17.2. L'utilisation de la capacité de calcul par le client doit automatiquement être jugée inéquitable et non raisonnable si elle dépasse le facteur de surréservation de Leaseweb déterminé dans les spécifications de services de telle manière que, à l'unique discrétion de Leaseweb, elle peut affecter la performance d'une autre infrastructure sur la plateforme infonuagique.

17.3. Les composantes de stockage de la plateforme infonuagique sont fournies au client sur un système de stockage partagé et, par conséquent, l'utilisation par le client des services infonuagiques peut affecter la performance (comme le temps d'attente, la bande passante de stockage et les opérations d'entrée/sortie par seconde) de l'ensemble du système de stockage. Pour protéger la performance et l'intégrité de la plateforme infonuagique, le client doit s'assurer que son utilisation du stockage est équitable et raisonnable.

18. SERVICES DE STOCKAGE EN NUAGE

18.1. Leaseweb offre des services de stockage en nuage à partir des composantes de stockage de la plateforme infonuagique (les « **services de stockage en nuage** »). Ces services offrent différents types de stockage, différentes capacités de stockage et différents niveaux de performance, qui se différencient en fonction du nombre d'opérations d'entrée/sortie par seconde par volume et du temps de latence attribués à chaque niveau. Les services de stockage en nuage sont fournis au client sur un système de stockage partagé et, par conséquent, l'utilisation par le client des services de stockage en nuage peut avoir une incidence sur la performance (comme le temps de latence, la bande passante de stockage et les opérations d'entrée/sortie par seconde) de l'ensemble du système de stockage. Les opérations d'entrée/sortie par seconde par volume sont établies par défaut en fonction d'un profil d'utilisation de blocs de 4 K avec une utilisation en lecture/écriture de 70/30 (le « **profil d'utilisation** »).

18.2. Pour protéger la performance et l'intégrité de la plateforme infonuagique, le client doit s'assurer que son utilisation des services de stockage en nuage est équitable, raisonnable et conforme à son profil d'utilisation. D'autres profils d'utilisation sont pris en charge par Leaseweb; toutefois, leur performance au niveau des opérations d'entrée/sortie par seconde peut varier.

18.3. L'utilisation des services de stockage en nuage par le client sera jugée inéquitable et déraisonnable si son utilisation de la plateforme infonuagique s'écarte constamment de son profil d'utilisation, au point d'avoir des répercussions sur la performance de la plateforme infonuagique dans son ensemble, ce que Leaseweb déterminera à son entière discrétion au moyen de ses propres données et outils. Toute utilisation non conforme jugée inéquitable et déraisonnable entraînera des frais supplémentaires.

19. UTILISATION RAISONNABLE DU SERVICE SPV

19.1. La capacité de calcul de l'environnement infonuagique pour les services SPV est fournie aux clients de Leaseweb sur une base partagée. Afin de protéger le rendement et l'intégrité de l'environnement en nuage, le client veillera à ce que son utilisation de la capacité de calcul dans le cadre du service SPV soit juste et raisonnable.

19.2. L'utilisation de la capacité de calcul par le client sera jugée inéquitable et déraisonnable si son utilisation dépasse continuellement la capacité allouée et constitue une utilisation déraisonnable de l'environnement partagé. Leaseweb, à sa seule discrétion, considérera que le client utilise l'environnement partagé de manière déraisonnable si cela entraîne une utilisation élevée et continue de l'unité centrale et des problèmes avec le service tel que, mais sans s'y limiter, le vol de l'unité centrale. Si le client utilise le service de manière déraisonnable, Leaseweb se réserve le droit d'instaurer des limites d'utilisation de l'unité centrale pour assurer une distribution équitable des ressources.

19.3. Leaseweb, à sa seule discrétion, pourra considérer que l'utilisation de la bande passante par le client est déraisonnable si ce dernier utilise continuellement de grandes quantités de bande passante pour le trafic de ses données et que cela entraîne des problèmes de disponibilité du service SPV. En mettant en place cette politique, Leaseweb s'assure que l'infrastructure du réseau partagé fonctionne de manière optimale pour le client. Si un client utilise le service de manière déraisonnable, Leaseweb se réserve le droit de limiter la quantité de trafic de données ou de suspendre l'utilisation du service.

20. SERVICE D'HÉBERGEMENT WEB PARTAGÉ

20.1. La plateforme d'hébergement Web partagé de Leaseweb est mise à la disposition du client sur une base partagée. Pour protéger la performance et l'intégrité de la plateforme d'hébergement Web partagé de Leaseweb, le client doit s'assurer que son utilisation des services d'hébergement Web partagé est équitable et raisonnable.

20.2. L'utilisation des services d'hébergement Web partagé par le client est jugée inéquitable et non raisonnable si :

i. le client utilise les services d'hébergement Web partagé de manière (à la discrétion raisonnable de Leaseweb) à affecter la performance de la plateforme d'hébergement Web partagé ou à causer une urgence;
ii. la taille de la base données dépasse de 30 % l'espace disque total attribué au client sur la plateforme d'hébergement Web partagé;
iii. le protocole IMAP dépasse 5 connexions par adresse IP;
iv. au moins vingt-cinq pour cent (25 %) des ressources du système sont utilisées en rapport avec les services d'hébergement Web partagé plus longtemps que quatre-vingt-dix (90) secondes à la fois. Les activités qui peuvent causer cette utilisation excessive comprennent notamment des scripts CGI, FTP, PHP et HTTP;
v. le client exécute des demandes MySQL plus longtemps que vingt (20) secondes. Les tables MySQL doivent être indexées de façon appropriée.

21. MULTI-CDN

21.1. Le service multi-CDN doit être utilisé de manière cohérente, équitable et raisonnable par le client.

21.2. Limites de trafic de données : Leaseweb se réserve le droit de limiter la quantité de trafic de données passant par le bouclier de protection du CDN de Leaseweb pour assurer la stabilité et la fiabilité de son réseau. Si le trafic de données passant par le bouclier de protection du CDN d'un client excède de 5 % du trafic de données mensuel convenu, Leaseweb peut i) limiter le trafic de données passant par le bouclier de protection du CDN de Leaseweb, ii) vider le cache du bouclier de protection du CDN de Leaseweb ET/ou; iii) désactiver la configuration du bouclier de protection du CDN de Leaseweb, afin de prévenir toute perturbation des services multi-CDN des autres clients.

21.3. Taille des objets : Le client reconnaît et accepte que les frais du service multi-CDN sont établis en fonction de la livraison d'objets ayant une taille moyenne de 32 Ko ou plus par requête HTTP ou HTTPS. Leaseweb se réserve le droit de facturer des frais supplémentaires au client pour les demandes de trafic de données de 10.000 HTTP ou HTTPS dont la taille moyenne des objets est inférieure à 32 Ko.

21.4. L'utilisation du bouclier de protection CDN de Leaseweb comme service de stockage par le client est strictement interdite.

21.5. L'utilisation du service multi-CDN par le client sera considérée comme incohérente, inéquitable et/ou déraisonnable si i) le client dépasse les limites de trafic du bouclier de protection CDN de Leaseweb indiquées à l'article 15.2; ii) la taille moyenne des objets du client est inférieure à 32 Ko, et/ou; iii) le bouclier de protection du CDN de Leaseweb est utilisé comme service de stockage.

21.6. Si Leaseweb détermine, à sa seule discrétion, que le client n'utilise pas le service multi-CDN conformément à la présente Politique d'utilisation raisonnable du service multi-CDN, Leaseweb sera en droit d'imposer immédiatement et sans préavis des limites de trafic de données que le client peut transmettre ou recevoir par l'entremise du service multi-CDN et de résilier ledit service.

CHAPITRE E. POLITIQUE RELATIVE À LA SÉCURITÉ

22. CONFIGURATION DE L'INFRASTRUCTURE

22.1. Leaseweb encourage un comportement hautement responsable relativement à l'utilisation de ses services et demande aux utilisateurs de ses services de faire de même. C'est pour cette raison qu'elle a établi des exigences en matière de sécurité de l'information pour tous ses services, y compris des normes pour la configuration de base de l'infrastructure, l'utilisation des renseignements d'authentification et le recours à des moyens efficaces de détection et de prévention des logiciels malveillants.

22.2. Il est conseillé au client (i) de sauvegarder régulièrement les configurations de données et de systèmes (critiques) et de stocker ces données en lieu sûr, (ii) de ne pas connecter son infrastructure au moyen d'une connexion sans fil, (iii) de mettre à jour le logiciel exploité ou utilisé sur l'infrastructure et, par conséquent, d'installer régulièrement et sans retard excessif les mises à jour et les correctifs après leur mise à disposition, et (iv) de mettre en œuvre et/ou d'utiliser des moyens adéquats contre les logiciels malveillants sur l'infrastructure.

23. SURVEILLANCE ET RAPPORTS

23.1. Le client doit mettre en œuvre des mesures de journalisation et de surveillance des événements liés à la sécurité.

23.2. Le client doit signaler sur-le-champ au centre des opérations réseau de Leaseweb tout événement lié à la sécurité qui peut avoir une incidence importante sur l'infrastructure de Leaseweb, l'organisation de Leaseweb ou la prestation de services de Leaseweb à d'autres clients. À la demande de Leaseweb, le client doit mettre immédiatement le journal relatif à un tel événement à la disposition de Leaseweb et doit suivre les directives données par Leaseweb dans la mesure où cela peut être nécessaire pour contenir ou corriger l'événement.

24. TEST DE PÉNÉTRATION

24.1. Le client est autorisé à effectuer certains tests de pénétration sur l'équipement de Leaseweb, sous réserve que les conditions énoncées à l'article 24 soient respectées. La fréquence des tests de pénétration est limitée à un maximum d'une fois par mois.

24.2. Les activités autorisées dans le cadre de tests de pénétration sont les suivantes : i) test des applications Web du client; ii) analyse des vulnérabilités; iii) test à données aléatoires sur les services; iv) balayage des ports des services; v) test de conformité PCI-DSS; vi) test de surveillance de la sécurité du client et de détection des menaces à la sécurité du client.

24.3. Les activités interdites dans le cadre d'un test de pénétration sont, sans s'y limiter, les suivantes : i) tout test sur les services d'autres clients; ii) tout test direct sur l'infrastructure de réseau partagée; iii) tout test sur l'infrastructure virtuelle partagée; iv) tout test sur les services d'hébergement Web partagés; v) tout test de déni de service; vi) l'hameçonnage ou toute autre forme d'attaque ou de piratage psychologique contre les employés de Leaseweb.

24.4. Tous les coûts liés aux tests de pénétration sont aux frais du client. Le client est le seul responsable des activités de son vérificateur envers Leaseweb et les tiers. Lors de la réalisation des tests, le vérificateur doit agir de manière responsable et faire preuve de diligence et de prudence envers Leaseweb et ses activités. En aucun cas le vérificateur du client n'effectuera des activités étant généralement connues ou réputées comme pouvant causer des dommages au service fourni par Leaseweb et ses clients ou comme pouvant provoquer une interruption, une suspension ou une dégradation d'un ou de plusieurs services fournis par Leaseweb à ses clients.

24.5. Le client s'engage à : i) indemniser et dégager Leaseweb de toute responsabilité en cas de poursuite, de perte, de coûts, de dommages, de sentences, de dépenses, d'honoraires (y compris les frais juridiques encourus et/ou attribués à Leaseweb), de procédures, de réclamations ou de demandes qui résultent des tests effectués par le vérificateur pour le compte du client; ii) fournir à Leaseweb toute l'autorité, l'information et l'assistance raisonnablement nécessaires à la défense, à la résolution ou au règlement de cette réclamation, et ce, à ses frais; et iii) prendre des mesures raisonnables, à la demande de Leaseweb, pour rétablir la posture financière dans laquelle Leaseweb aurait été si les tests menés par le vérificateur n'avaient pas eu lieu.

24.6. Si, pendant les tests de pénétration, l'équipement et/ou l'environnement de Leaseweb deviennent instables, le vérificateur du client est tenu d'interrompre immédiatement toutes les activités de vérification et d'aviser Leaseweb de la situation à l'adresse suivante : support@leaseweb.com.

24.7. Si les résultats du test de pénétration révèlent certains éléments pouvant avoir une incidence sur les activités de Leaseweb, le client est tenu de l'en informer à l'adresse suivante : support@leaseweb.com.

24.8. Pour effectuer toute autre activité liée à la sécurité technique qui n'est pas mentionnée à l'article 24 des présentes, le client doit en faire la demande par courriel à Leaseweb à l'adresse suivante : support@leaseweb.com.

CHAPITRE F. POLITIQUE D'EXPLOITATION DES INSTALLATIONS

25. INTRODUCTION

25.1. Les centres de données n'ont pas ou ont très peu d'espace d'entreposage. Leaseweb ne peut garantir la sécurité de l'équipement colocalisé qui n'est pas sécurisé dans l'espace d'hébergement ou contenu dans le centre de données et n'assume aucune responsabilité en ce qui a trait à celui-ci.

25.2. Leaseweb a adopté la politique d'exploitation des installations pour la sûreté et la sécurité des clients, des employés du client, des sous-traitants du client et/ou de l'infrastructure.

26. EXPÉDITIONS

26.1. Chaque client doit observer les politiques d'expédition et de réception adoptées de temps à autre par Leaseweb relativement à l'expédition d'équipement à destination et en provenance du centre de données.

26.2. Le client doit aviser Leaseweb de tout envoi d'équipement vers le centre de données, au moins deux (2) jours ouvrables avant la date de livraison prévue de l'équipement, au moyen du formulaire d'avis d'expédition accessible dans le portail Clients. En ce qui concerne les activités administratives effectuées par ou pour le compte de Leaseweb liées à l'envoi, le client s'engage à payer à Leaseweb les frais d'expédition suivants : i) soixante-dix dollars canadiens (70 $ CA), si le client avise Leaseweb de l'envoi dans les délais prévus; ou ii) trois cent quarante dollars canadiens (340 $ CA), si le client n'avise pas Leaseweb de l'envoi dans les délais prévus.

26.3. Tous les frais relatifs aux expéditions d'équipement par le client à destination ou en provenance d'un centre de données seront à la charge du client.

26.4. Le client est responsable du nettoyage et de l'élimination de tous les matériaux et équipements utilisés pour l'expédition de son envoi. Le client doit s'assurer que le matériel d'expédition est retiré du centre de données le jour même de la livraison. Si le client ne respecte pas cette disposition, Leaseweb lui facturera des frais de nettoyage.

26.5. Le client doit utiliser sa propre raison sociale et ses informations commerciales comme référence du destinataire/importateur pour tout envoi que lui ou l'un de ses tiers effectue, ainsi que pour toute documentation douanière accompagnant tout colis ou courrier adressé au centre de données et destiné à être reçu par le client. L'envoi de matériel par le client et/ou par l'un de ses tiers au centre de données est aux risques et aux frais du client. Il incombe au client de remplir et de soumettre tous les documents relatifs au transport en bonne et due forme. Il est interdit au client d'indiquer ou de mentionner Leaseweb comme destinataire ou importateur des envois effectués par le client ou par l'un de ses fournisseurs tiers. Leaseweb n'est pas responsable des expéditions vers son centre de données ou à partir de celui-ci effectués par le client ou ses fournisseurs. Pour éviter toute ambiguïté, le client et ses fournisseurs tiers ne peuvent pas désigner Leaseweb comme importateur attitré. Le client a l'entière responsabilité de se conformer à toute la réglementation en matière de douanes, d'exportation et d'importation.

26.6. Les modalités du service d'emballage offert par Leaseweb pour le transport de l'équipement du client à partir d'un centre de données de Leaseweb sont définies à l'article 15 de l'entente sur les niveaux de service

27. ENTREPOSAGE

27.1. Les centres de données n'ont pas – ou ont très peu – d'espace d'entreposage. Leaseweb ne peut garantir la sécurité de l'équipement colocalisé qui n'est pas sécurisé dans l'espace d'hébergement ou contenu dans le centre de données.

27.2. Si le client n'est pas prêt à installer l'équipement, Leaseweb peut exiger que le client entrepose l'équipement dans un espace de stockage désigné et à ses frais. Si l'équipement est entreposé pendant plus de quatorze (14) jours civils, le client doit payer à Leaseweb les frais d'entreposage de l'équipement.

28. CONDUITE DANS LE CENTRE DE DONNÉES

28.1. Sauf pour une urgence, un client ayant une carte d'accès 24 heures par jour, 7 jours par semaine doit fournir à Leaseweb un avis d'au moins une (1) heure pour accéder au centre de données et/ou à l'espace d'hébergement et un client n'ayant pas de carte d'accès 24 heures par jour, 7 jours par semaine doit fournir à Leaseweb un avis d'au moins vingt-quatre (24) heures pour accéder au centre de données et/ou à l'espace d'hébergement.

28.2. Le client doit s'identifier à la réception du centre de données en montrant une pièce d'identité valide (permis de conduire, passeport ou pièce d'identité du pays) et expliquer le but de sa visite. Le client doit signer le registre des visiteurs à l'arrivée et au départ du centre de données, en indiquant l'heure d'arrivée et de départ. La réception lui remet une carte d'accès qu'il doit porter tout au long de sa visite et garder visible. Avant de partir, le client doit remettre la carte d'accès à la réception, faute de quoi des frais de service peuvent lui être facturés.

28.3. Chaque jour, le client ne peut permettre qu'à trois (3) personnes au maximum d'accéder au centre de données. Des frais de service sont exigibles et payables par le client pour chaque personne qui entre dans le centre de données, à l'exception des personnes qui détiennent une carte d'accès 24 heures par jour, 7 jours par semaine ou qui accompagnent le détenteur d'une telle carte d'accès. Les frais ne seront imposés qu'à la première personne. L'accès sera facturé par intervalles de trente (30) minutes, avec un minimum d'une (1) heure.

28.4. Le client doit fournir à Leaseweb une liste de personnes autorisées à accéder à l'espace d'hébergement et à l'équipement colocalisé, et peut mettre à jour cette liste à l'occasion en remettant un avis écrit à Leaseweb. Le client est responsable de toutes les personnes qui obtiennent un accès à son nom.

28.5. Leaseweb peut exiger, à sa seule discrétion, qu'un de ses représentants escorte un représentant du client accédant au centre de données et/ou à l'espace d'hébergement. De plus, le règlement interne du centre de données peut prévoir que le propriétaire ou le bailleur du centre de données peut, dans certaines circonstances, exiger qu'un membre de son personnel escorte un représentant du client accédant au centre de données et/ou à l'espace d'hébergement.

28.6. Si le personnel de Leaseweb fournit un accompagnateur pendant la visite du client au centre de données et/ou à l'espace d'hébergement, un tel accompagnement est considéré comme un service supplémentaire pour lequel Leaseweb peut facturer au client des frais de service supplémentaires (frais d'escorte) en plus de tous les frais d'escorte imposés à Leaseweb par le propriétaire du centre de données. Si un représentant du client est accompagné d'un accompagnateur fourni par le propriétaire ou le bailleur du centre de données pendant sa visite à l'espace d'hébergement, le client doit payer à Leaseweb tous les frais d'escorte qui peuvent lui être imposés.

28.7. Le client doit (i) en tout temps agir de manière professionnelle, (ii) ne pas entraver d'une manière quelconque l'utilisation ou l'exploitation par Leaseweb du centre de données ou l'utilisation ou l'exploitation de tout équipement installé par d'autres parties, y compris l'équipement d'autres clients. Si le client exige de déplacer, d'enlever ou de débrancher l'équipement d'une autre partie pour entretenir son propre équipement, il doit contacter Leaseweb et lui demander ses directives avant un tel déplacement, enlèvement ou débranchement, compte tenu d'un avis de 48 heures. Le client doit également (iii) s'abstenir d'exploiter tout équipement qui peut constituer un danger pour la sécurité, (iv) ne pas effectuer de tests qui peuvent endommager ou perturber le réseau de Leaseweb, l'espace d'hébergement et/ou le centre de données, (v) s'assurer de fermer les portes après l'utilisation afin de maintenir un environnement clos et sûr, et par conséquent efficace pour les systèmes de protection contre les incendies et de régulation de climatisation, et (vi) verrouiller le bâti avant de partir. S'il a un doute, le client doit consulter le gestionnaire de l'installation du centre de données ou, en l'absence du gestionnaire de l'installation, un autre employé de Leaseweb.

28.8. Leaseweb peut, à sa seule discrétion, faire quitter les lieux à un membre du personnel du client ou à un sous-traitant ou agent tiers du client si une telle personne ne se conforme pas à une politique de Leaseweb ou aux directives données par un employé de Leaseweb.

28.9. En cas d'urgence, par exemple un incendie, qui est généralement indiqué par le son d'un système d'alarme, le client doit immédiatement évacuer le centre de données.

28.10. Il est interdit de fumer dans tout le centre de données. Il est interdit de manger et de boire dans les zones du centre de données où sont situés l'espace d'hébergement et/ou l'équipement.

28.11. Dans les zones du centre de données où sont situés l'espace d'hébergement et/ou l'équipement, le client doit s'abstenir de toute activité qui peut causer l'émission de particules de poussière. Cette interdiction est notamment due au fait que des particules de poussière peuvent déclencher un système d'alarme automatique. S'il a un doute, le client doit consulter le gestionnaire de l'installation du centre de données ou, en l'absence du gestionnaire de l'installation, un autre employé de Leaseweb.

28.12. Sauf exigence expresse de toute garantie d'assurance (produit), le client ne doit apporter aucun matériau d'emballage dans les zones où sont situés l'espace d'hébergement et/ou l'équipement et le client doit ouvrir les boîtes (en carton) dans la zone de chargement. Si le client, relativement à une garantie d'assurance (produit), exige d'apporter des matériaux d'emballage dans les zones où sont situés l'espace d'hébergement et/ou l'équipement, il doit en informer Leaseweb à l'avance. Leaseweb désignera ensuite un membre de son personnel pour accompagner le client pendant qu'il se trouve dans les zones où sont situés l'espace d'hébergement et/ou l'équipement. Le client a l'obligation d'enlever tous les matériaux d'emballage des zones où sont situés l'espace d'hébergement et/ou l'équipement, au plus tard une (1) heure après être entré dans les zones en question.

28.13. Le client doit immédiatement signaler les irrégularités et/ou les alarmes, remarquées pendant sa présence dans le centre de données, au gestionnaire de l'installation du centre de données ou, en l'absence du gestionnaire de l'installation, à un autre employé de Leaseweb.

29. EXIGENCES RELATIVES À L'ÉQUIPEMENT

29.1. Sauf entente contraire expresse et écrite de la part Leaseweb, tout l'équipement doit être installé et entretenu par le client ou en son nom conformément aux critères suivants : (i) Les lignes de télécommunication doivent être tendues à partir d'un répartiteur organisé et protégé; (ii) Les pièces de rechange doivent être gardées à l'intérieur des limites de l'espace d'hébergement; (iii) Le courant alternatif et le courant continu doivent être distribués dans l'espace d'hébergement, dans la mesure du possible; (iv) La densité de l'équipement doit correspondre à la charge maximale admissible au sol dans l'installation; (v) Tous les câbles doivent être attachés et fixés de manière ordonnée; (vi) L'équipement doit être entièrement conforme aux normes de l'industrie des télécommunications et aux exigences et spécifications de Leaseweb; et (vii) Tout l'équipement colocalisé et le câblage s'y rattachant doivent être installés de manière à ce que l'armoire puisse être fermée et verouillée; et (viii) l'équipement doit être conforme aux lois, aux règles et aux règlements applicables dans le territoire où il se trouve (et notamment le Canada [y compris la Loi sur la radiocommunication], la décision Télécom CRTC 82-14 et la norme de certification SC-03), comme modifiés de temps à autre.

29.2. Il est expressément interdit au client d'installer une unité d'alimentation c.a. permanente dans l'espace d'hébergement ou l'ensemble du centre de données.

29.3. Le client doit s'assurer que l'équipement alimenté en c.a. ait un facteur de puissance de 0,85 ou plus.

CHAPITRE G. POLITIQUE D'ENQUÊTE ET D'EXÉCUTION

30. ENQUÊTE

30.1. Leaseweb se réserve le droit d'effectuer une enquête en cas (i) de violations présumées des politiques, (ii) de risques (potentiels) pour la sécurité de son infrastructure et/ou (iii) de demande valide des autorités pertinentes (d'application de la loi).

30.2. Dans le cadre d'une telle enquête, Leaseweb peut, en agissant raisonnablement, (i) recueillir de l'information auprès du client ou à son sujet, (ii) si c'est pertinent, recueillir de l'information d'une partie plaignante et/ou (iii) examiner le journal de sécurité du client mentionné à l'article 23. Le client a l'obligation de coopérer entièrement à de telles enquêtes de Leaseweb.

31. MESURES PRISES PAR LEASEWEB

31.1. Dans la mesure légalement permise, Leaseweb est autorisée à accorder aux autorités pertinentes d'application de la loi l'accès au contenu, à l'information et/ou à l'infrastructure du client, ainsi qu'à tout renseignement qu'elle a recueilli lors de l'enquête en vertu de l'article 30.1.

31.2. À la demande d'une tierce partie, Leaseweb a le droit de divulguer l'information d'identification du client à une telle partie relativement à une violation (présumée) de la politique d'utilisation acceptable de Leaseweb dans la mesure exigée par la loi (à déterminer à la discrétion de Leaseweb).

31.3. Leaseweb a le droit de prendre des mesures, légales ou autres, contre le client et/ou l'utilisateur final si l'utilisation du service par le client ou ses utilisateurs finaux enfreint les politiques ou si le client omet présumément de se conformer à toute obligation en vertu des politiques. Leaseweb détermine à sa seule discrétion les mesures appropriées, notamment les suivantes : (a) suspension ou cessation d'une partie ou de la totalité des services conformément aux conditions de vente, (b) blocage (sélectif) d'adresses IP ou de ports; (c) réinstallation des services, (d) imposition de limites de l'utilisation du service (par exemple, imposition de limites de la vitesse de transmission et/ou de réception des données par le client dans le cadre du service), (e) redémarrage du service, (f) blocage de l'accès au niveau du routeur et/ou du commutateur de l'infrastructure du client, (g) refus au client de l'accès (physique) à l'infrastructure, (h) instructions obligatoires données au client relativement à l'utilisation des services, (i) modification ou mise à jour des registres PTR, DNS inverse ou WHOIS de référence et/ou (j) mise en quarantaine des fichiers infectés par des logiciels malveillants.

32. AVIS DE NON-RESPONSABILITÉ

32.1. Sans préjudice de ce qui précède ou de toute autre disposition des politiques, Leaseweb n'effectue pas d'examen, de suivi et de contrôle à titre préventif du contenu envoyé ou reçu par les clients qui utilisent les services (et n'a pas l'intention de le faire). Leaseweb n'accepte aucune responsabilité à l'égard du contenu des communications transmises ou mises à la disposition du client ou de ses utilisateurs finaux, peu importe qu'elles proviennent du réseau ou des services.

32.2. Aucune des dispositions du présent 0 ou d'autres chapitres des politiques ne doit imiter tout autre droit ou recours éventuel de Leaseweb ou lui porter atteinte de quelque manière que ce soit.

CHAPITRE H RÈGLEMENT SUR LES DONNÉES (APPLICABLE AUX CLIENTS ÉTABLIS DANS LES PAYS MEMBRES DE L'UNION EUROPÉENNE SEULEMENT)

33. PROCESSUS DE CHANGEMENT DE FOURNISSEUR

33.1. *Les articles 33.1 à 33.9 des politiques s'appliquent aux clients établis dans les pays membres de l'Union européenne seulement.* Leaseweb collaborera de bonne foi avec le client pour faciliter le changement de fournisseur.

33.2. Leaseweb, dans sa capacité de fournisseur de services infonuagiques fournissant des services d'infrastructure à la demande (IaaS) non gérés, n'a pas accès aux systèmes d'exploitation, aux logiciels et aux applications du client stockés sur son infrastructure. Par conséquent, le client doit effectuer lui-même le transfert de ses données dans les délais impartis, soit pendant la période de transition et, au plus tard, avant la fin de la période de récupération des données, conformément à l'article 26 et au paragraphe 1 de l'article 30 du *Règlement sur données*. Leaseweb assurera la continuité des services en vertu du contrat de vente en vigueur pendant que le client effectuera le transfert de ses données et de ses actifs numériques exportables.

33.3. Conformément à son modèle de prestation de services d'IaaS, Leaseweb veille à maintenir un niveau de service équivalent en prenant des mesures raisonnables pendant le processus de changement de fournisseur. Ces mesures assurent aux nouveaux clients et aux clients ayant soumis une demande de changement, un niveau minimal de fonctionnalité des services avant, pendant et après le processus de changement de fournisseur. Si le client soumet une demande à Leaseweb pour des services dont la plupart des fonctionnalités principales doivent être personnalisées pour répondre à des besoins spécifiques, ou dont tous les composants ont été développés pour répondre à ceux-ci, les obligations de Leaseweb relatives au maintien d'un niveau de service équivalent énoncées dans le présent article ne s'appliquent pas.

33.4. Les clients conservent le droit d'accéder aux données générées par leur utilisation du service ou de tout autre service connexe et de les récupérer dans des formats exploitables par une machine.

33.5. Afin de respecter ses obligations en matière de transparence en vertu du *Règlement sur les données* applicables dans les pays de l'Union européenne où se trouvent ses infrastructures, Leaseweb dirige les clients vers son site Web (https://www.leaseweb.com/fr/about-us/legal/sales-contract) où l'on trouve les contrats de vente en format imprimable et téléchargeable. À des fins de transparence, les clients peuvent les consulter avant de commander des services. Ce site Web est mentionné dans le contrat de vente.

33.6. En plus d'être décrits au présent article des politiques, les droits et les obligations de Leaseweb et du client relativement au processus de changement de fournisseur sont énoncés dans les articles 10.5, 21.6 à 21.11 et 22.10 des conditions de vente.

34. MODALITÉS DU *RÈGLEMENT SUR LES DONNÉES*

34.1. *Les articles 34.1 à 34.2 des politiques s'appliquent aux clients établis dans les pays membres de l'Union européenne seulement.* En ce qui a trait aux obligations de transparence énoncées dans le *Règlement sur les données*, Leaseweb renvoie le client aux articles 8 et 28 des conditions de vente applicables : i) dans les pays où les services sont offerts; et ii) à l'information sur les mesures techniques et organisationnelles mises en place par Leaseweb concernant l'accès aux données non personnelles par les autorités gouvernementales internationales ou au transfert de celles-ci (article 28 du *Règlement sur les données* concernant les obligations contractuelles de transparence en matière d'accès aux données et au transfert de celles-ci à l'international). Pour obtenir de plus amples informations, veuillez consulter les pages Web suivantes : https://www.leaseweb.com/fr/about-us/legal/sales-contract, https://www.leaseweb.com/fr/about-us/legal/personal-data-protection-acts et https://www.leaseweb.com/fr/about-us/security-certifications.

34.2. En règle générale, les services ne sont pas considérés comme des « produits connectés » ou des « services connexes » au sens du *Règlement sur les données*. Toutefois, dans la mesure où les services peuvent être qualifiés de « services connexes » au sens du *Règlement sur les données*, l'information relative à ces « services connexes » est réputée avoir été fournie au client par son accès et par son recours aux services.

CHAPITRE I. LOCALISATION ET SOUVERAINETÉ DES DONNÉES

35. LOCALISATION DES DONNÉES

35.1. Les infrastructures physiques de Leaseweb sont situées au Canada aux endroits énumérés ci-dessous. Elles sont assujetties aux lois du Canada et de la province de Québec.

a) Centre de données MTL-01(MCO), 20, Place du Commerce, Île-des-Sœurs, Montréal (Québec) H3E 1Z6;
b) Centre de données MTL-02 (MNE), 7207, boulevard Newman, LaSalle (Québec) H8N 2K3;
c) Centre de données MTL-03(MCL), 5945, boulevard Couture, Montréal (Québec) H1P 1A8.

35.2. Pour les services de colocation : Le client peut choisir l'emplacement du centre de données où sera installé l'équipement de colocation lorsque Leaseweb dispose de plusieurs centres de données dans une région.

36. SOUVERAINETÉ DES DONNÉES

36.1. Pour assurer la souveraineté, Leaseweb traite et stocke les données du client à ses centres de données situés au Canada seulement, conformément aux lois du Québec et du Canada.

CHAPITRE J. MESURES DE SÉCURITÉ TECHNIQUES ET ORGANISATIONNELLES

37. MESURES DE SÉCURITÉ TECHNIQUES ET ORGANISATIONNELLES: GÉNÉRALITÉS

37.1. Leaseweb a instauré des mesures de sécurité techniques et organisationnelles, conformément aux exigences du RGPD de l'Union européenne, entre autres. Conformément au RGPD de l'Union européenne, Leaseweb a mis en œuvre des mesures de sécurité techniques et organisationnelles appropriées pour protéger la sécurité, la confidentialité et l'intégrité des informations personnelles (du client) et continuera à mettre en œuvre de telles mesures, notamment celles énumérées ci-dessous.

37.2. Leaseweb veille à offrir à ses clients un niveau de sécurité adéquat, ainsi que des mesures de cybersécurité et de résilience commerciale, conformément à ses certifications et rapports d'assurance ISO 27001, SOC1, PCI DSS.

37.3. Les certifications de sécurité requises de la part des fournisseurs de centre de données de Leaseweb sont indiquées sur notre site Web à l'adresse suivante: https://www.leaseweb.com/en/why-leaseweb/platform/data-centers.

38. MESURES TECHNIQUES

38.1. Leaseweb a mis en place les mesures techniques suivantes :

a) **Chiffrement des données :**
- Chiffrement intégral du disque de tous les terminaux des utilisateurs gérés par Leaseweb (données au repos).
- Mise en place de protocoles de chiffrement et de sécurité robustes pour la transmission de données via le protocole TLS ou le réseau privé virtuel (données en transit).

b) **Contrôle des accès :**
- Autorisations d'accès octroyées selon le principe du droit d'accès minimal et du privilège et du besoin de connaître.
- Mise en place de politiques et de procédures de gestion des accès pour l'intégration et le départ des membres de son personnel.
- Mise en place de politiques robustes en matière d'authentification et de mot de passe, lesquelles font l'objet d'un suivi.
- Mise à disposition d'outils qui permettent aux membres du personnel de Leaseweb d'effectuer leur travail en toute sécurité (gestionnaire de mots de passe, RPV client, protection des terminaux sur tous les terminaux des membres du personnel de Leaseweb).

c) **Développement sécurisé :**
- Processus d'approbation à trois niveaux pour les modifications de code (principe des six yeux).
- Sécurité : configuration des serveurs selon le modèle d'infrastructure en tant que code, dans la mesure du possible.
- Audit semestriel de toutes les équipes de développement par l'équipe de sécurité de Leaseweb, selon un modèle de maturité de la sécurité.
- Séparation des environnements de développement, de test et de production.
- Contrôle des versions des codes bases de Leaseweb.

d) **Sécurité des réseaux :**
- Segmentation du réseau sur les réseaux internes de Leaseweb.
- Utilisation de pare-feu sur le réseau interne de Leaseweb.
- Utilisation de systèmes de détection d'intrusion sur le réseau interne de Leaseweb.

e) **Gestion des vulnérabilités :**
- Installation d'un logiciel antivirus doté de fonctionnalités de reconnaissance électronique de date sur tous les terminaux des membres du personnel de Leaseweb afin de détecter et d'empêcher toute utilisation abusive des vulnérabilités.
- Réalisation d'exercices de surveillance des vulnérabilités, de tests d'intrusion et de simulations de cyberattaques (équipe des rouges).

38.2. Leaseweb peut mettre à jour ces mesures de temps à autre pour s'adapter à l'évolution des menaces et des technologies.

39. MESURES ORGANISATIONNELLES

39.1. Leaseweb a mis en place les mesures organisationnelles suivantes :

a) **Gouvernance de la sécurité de l'information :**
- Système de gestion de la sécurité de l'information (« SGSI »), conformément à la norme ISO 27001.
- Audit annuel du SGSI par des auditeurs internes et externes.
- Échanges périodiques sur les menaces et les vulnérabilités avec les parties intéressées, notamment les fournisseurs de services de sécurité, les gouvernements et autres organisations du secteur.
- Mise en place d'un service de sécurité informatique dédié.

b) **Suppression des données :**
- Effacement des données sur les équipements de Leaseweb utilisés par le client après la résiliation du contrat de vente.
- Destruction physique des disques durs endommagés.
- Installations de déchiquetage de papier sécurisées.

c) **Formation du personnel :**
- Formations de sensibilisation à la sécurité périodiques et obligatoires portant sur différents sujets, comme la sensibilisation à la protection de la vie privée.
- Simulations de tentatives d'hameçonnage périodiques pour tout le personnel de Leaseweb.

d) **Gestion des risques :**
- Évaluations périodiques des risques à la sécurité.
- Tenue et mise à jour d'un registre des risques à la sécurité.

e) **Gestion des fournisseurs :**
- Centres de données et bureaux sécurisés afin de prévenir tout accès non autorisé.
- Évaluations périodiques afin de déterminer et de gérer les risques liés aux fournisseurs existants et aux nouveaux fournisseurs.

f) **Sécurité physique :**
- Centres de données et bureaux sécurisés afin de prévenir tout accès non autorisé.
- Révision périodique des autorisations d'accès en personne à nos installations sécurisées.

g) **Documentation et archivage :**
- Tenue de registres des politiques et procédures de sécurité.
- Consignation des registres dans notre documentation interne et mise à jour périodique de ceux-ci.

h) **Surveillance continue de l'environnement informatique interne de Leaseweb :**
- Outils de gestion des informations et des événements de sécurité (« GIES »).
- Surveillance de l'environnement informatique interne par un centre opérationnel de sécurité (« COS ») tiers.

i) **Audits et certifications :**
- Audits internes : Audits des mesures de sécurité internes effectués par Leaseweb chaque année.
- Audits externes :

- Certifié PCI-DSS 4.0.
- Certifié ISO 27001:2022.

39.2. Leaseweb peut mettre à jour ces mesures de temps à autre pour s'adapter à l'évolution des menaces et des technologies.

CHAPITRE K : LISTE DES SOUS-TRAITANTS DE LEASEWEB

40. SOUS-TRAITANTS EMBAUCHÉS PAR LEASEWEB

40.1 Leaseweb peut faire appel à des sous-traitants, notamment à ses sociétés affiliées ou à des tiers, pour la prestation de ses services. Le type de services fournis au client détermine le choix des sous-traitants retenus pour la prestation des services.

40.2 Leaseweb fait appel aux sous-traitants suivants pour l'ensemble de ses services :

Sociétés affiliées sous-traitantes	**Services**	**Emplacement**
Leaseweb Global B.V. Adresse : Hessenbergweg 95, 1101CX Amsterdam	Services d'infrastructure à la demande (IAAS)	Pays-Bas
Leaseweb Networks B.V. Adresse : Hessenbergweg 95, 1101CX Amsterdam	Fourniture de services réseau à la demande de Leaseweb	Pays-Bas