citrix

Annexe sur la sécurité des Services Citrix

Version 2.0
En vigueur à compter du 20 avril 2020

Table des matières

Champ d’application **3**

Programme de sécurité et cadre stratégique **3**

Contrôle d’accès **4**

Développement et maintenance du système **5**

Gestion des biens **6**

Sécurité des ressources humaines **7**

Sécurité des opérations **8**

Sécurité physique **9**

Continuité des activités et récupération d’urgence **10**

Réponse aux incidents **11**

Gestion des fournisseurs **11**

Conformité **12**

Audits et demandes des clients **13**

Coordonnées de Citrix **14**

La présente Annexe sur la sécurité des Services Citrix (l'« Annexe ») décrit les contrôles de sécurité mis en place dans le cadre des Citrix Cloud Services, des services de support technique ou des services de conseil (les « Services ») fournis aux clients au titre de la licence et/ou du contrat de services Citrix approprié(e) et de la commande applicable passée pour les Services (collectivement dénommés le « Contrat »). La présente Annexe ne s'applique pas aux services Bêta, Labs ou Tech Preview (y compris les Citrix Cloud Labs) et aux systèmes informatiques internes de Citrix non compris dans la prestation de Services.

Les termes en lettres capitales ont la signification définie dans le Contrat ou définie ici. Le terme « Contenu Client » désigne les données chargées dans le compte du Client à des fins de stockage ou les données disponibles dans l'environnement informatique du Client auxquelles Citrix peut accéder afin d'exécuter des Services. Le terme « Journaux » désigne les enregistrements de Services, y compris, mais sans s'y limiter, des données et informations concernant les performances, la stabilité, l'utilisation, la sécurité et le support ainsi que des informations techniques concernant les appareils, systèmes, logiciels associés, services ou périphériques liés à l'utilisation des Services par le Client.

1. Champ d'application

La présente Annexe décrit les contrôles de sécurité administratifs, physiques et techniques utilisés par Citrix pour préserver la confidentialité, l'intégrité et la disponibilité de ses Services. Ces contrôles s'appliquent aux systèmes et aux environnements d'opérations et de Services Citrix. Le programme de sécurité des Services Citrix repose sur la norme ISO/IEC 27002.

Dans un souci de renforcement et d'amélioration continus de ses pratiques de sécurité, Citrix se réserve le droit de modifier les contrôles décrits dans les présentes. Ces modifications ne diminueront en rien le niveau de sécurité pendant la durée applicable des Services.

2. Programme de sécurité et cadre stratégique

Citrix dispose d'un programme de sécurité et d'un cadre stratégique établis et approuvés par les dirigeants de Citrix issus de différents secteurs d'activité de l'entreprise.

2.1 Surveillance des risques de sécurité

Le Comité de surveillance des cyber-risques de Citrix (Cyber Risk Oversight Committee, CROC) contrôle les activités de gestion des risques de sécurité. Le CROC rassemble des dirigeants des différentes équipes interfonctionnelles de l'entreprise. Chaque année, la direction passe en revue les membres du comité afin d'assurer que tous les secteurs d'activité de l'entreprise sont bien représentés.

Le CROC se réunit au moins une fois par trimestre pour fournir des directives et des informations en matière d'identification, d'évaluation et de résolution des risques de sécurité, à la fois dans les opérations de l'entreprise et dans l'infrastructure de prestation de services.

2.2 Gestion des risques de sécurité

Citrix applique un programme de gestion des risques de sécurité (Security Risk Management, SRM) qui identifie les éventuelles menaces pouvant affecter les produits, les services et l'infrastructure de Citrix, qui évalue l'importance des risques liés à ces menaces, qui développe des stratégies d'atténuation des risques et qui met ces stratégies en œuvre en partenariat avec les équipes Produit et Ingénierie de Citrix.

Le programme SRM s'appuie sur des cadres reconnus dans le secteur, comme les normes ISO/IEC 31000 et ISO/IEC 27005.

2.3 Sécurité des informations

Citrix a nommé un Responsable de la sécurité des informations (Chief Information Security Officer, CISO), chargé de la surveillance de la sécurité et de la stratégie, de la conformité et de l'application de la politique de sécurité. Le Directeur de la surveillance de la sécurité et des réponses aux incidents dirige les procédures de réponse aux incidents, et notamment les enquêtes, la maîtrise et la résolution des incidents.

2.4 Sécurité physique et environnementale

En lien avec l'équipe de gestion des installations, l'équipe de sécurité de Citrix contrôle l'accès physique aux installations Citrix.

3. Contrôle d'accès

Citrix impose des mesures de contrôle d'accès visant à garantir l'octroi et le maintien des privilèges adéquats pour accéder aux systèmes, biens, données et installations de l'entreprise afin de les protéger contre d'éventuels dommages, dangers ou pertes. Citrix applique le principe du privilège minimum (sécurité basée sur les rôles) afin de restreindre l'accès des utilisateurs aux systèmes qui sont strictement nécessaires à la réalisation des tâches liées à leur fonction ou à leur rôle.

Les responsables définissent les rôles de manière à assurer une répartition adéquate des tâches. Les tâches et les privilèges sont répartis entre plusieurs personnes afin de limiter les risques de fraude et d'erreurs.

3.1 Nouveaux comptes, rôles et demandes d'accès

Citrix exige une demande officielle d'accès aux systèmes ou aux données de l'entreprise. Chaque demande d'accès nécessite, au minimum, l'autorisation du responsable de l'utilisateur afin de confirmer que le rôle de ce dernier requiert effectivement un accès. Les administrateurs d'accès confirment que les autorisations nécessaires sont obtenues avant d'accorder l'accès aux systèmes ou aux données.

3.2 Contrôle des comptes

Citrix conserve et met à jour un enregistrement des privilèges de sécurité des employés et sous-traitants autorisés à accéder aux systèmes Citrix incluant du Contenu Client. Le principe du privilège minimum s'applique.

Citrix contrôle au moins deux fois par an les comptes des utilisateurs et les autorisations affectées pour les principaux systèmes. Tout changement requis suite aux contrôles fait l'objet d'une demande d'accès officielle afin de confirmer que l'utilisateur et son rôle requièrent effectivement un accès au(x) système(s) concerné(s).

3.3 Compte, rôle et suppression des droits d'accès

Citrix exige que l'accès des utilisateurs soit rapidement désactivé, révoqué ou supprimé en cas de changement de rôle (le cas échéant), de résiliation du contrat de travail, de fin de l'engagement ou de départ de l'entreprise.

Les demandes de suppression des droits d'accès sont documentées et contrôlées.

3.4 Informations d'authentification

Citrix exige une authentification multifacteur pour l'accès distant par les employés aux systèmes Citrix et applique les pratiques suivantes en matière de traitement et de gestion des mots de passe :

- Les mots de passe sont renouvelés régulièrement, comme défini dans la configuration requise par Citrix.
- Les mots de passe doivent respecter des exigences de longueur (notamment une longueur minimale de 10 caractères) et de complexité (les noms communs ou mots du dictionnaire sont interdits).
- Les ID utilisateurs désactivés ou arrivés à expiration ne peuvent pas être transmis à d'autres personnes.
- Citrix applique des procédures de désactivation des mots de passe qui ont été divulgués par erreur.
- Citrix contrôle les tentatives répétées d'accès aux Services à l'aide de mots de passe non valides et bloque de façon automatisée les tentatives répétées d'accès.

Citrix a adopté des pratiques destinées à garantir la confidentialité et l'intégrité des mots de passe lors de leur attribution, distribution et stockage, notamment :

- Citrix requiert le hachage des mots de passe tout au long de leur cycle de vie.
- Citrix interdit le partage des mots de passe.

4. Développement et maintenance du système

Citrix dispose d'un processus Secure by Design, qui repose sur des normes et procédures de contrôle des modifications conçues pour répondre aux exigences de sécurité des systèmes d'information, de révision et de test des codes et de sécurité concernant l'utilisation des données de test. Ce processus est géré et contrôlé par une équipe de sécurité spécialisée, qui est également responsable de la révision de la conception, de la modélisation des menaces, de la révision et du contrôle manuels des codes ainsi que des tests d'intrusion.

4.1 Principes Secure by Design

Citrix a adopté une méthodologie officielle de cycle de vie du développement, qui régit le développement, l'acquisition, l'implémentation et la maintenance des systèmes informatiques et des besoins technologiques associés.

Citrix utilise un système basé sur les logiciels pour gérer les révisions et les approbations open source, qui implique d'effectuer des analyses et des audits périodiques de ses produits logiciels. Citrix a documenté des stratégies, accessibles à l'ensemble des employés, concernant l'utilisation de logiciels open source, la formation et l'encadrement des développeurs sur les bonnes pratiques en matière d'open source.

4.2 Gestion des modifications

La procédure de gestion des modifications d'infrastructure et de logiciels mise en place par Citrix répond aux exigences de sécurité. Elle impose que les modifications d'infrastructure et de logiciel soient autorisées, officiellement documentées, testées (le cas échéant), contrôlées et approuvées avant migration vers l'environnement de production. La gestion et le suivi des modifications d'infrastructure et de logiciels s'effectuent par le biais des systèmes de gestion des activités.

La procédure de gestion des modifications est séparée de manière appropriée et l'accès à la migration des modifications en production est réservé au personnel autorisé.

5. Gestion des biens

5.1 Gestion des biens physiques et virtuels

Citrix gère un inventaire dynamique des systèmes physiques et virtuels gérés par Citrix et utilisés pour exécuter les Services (les « Biens des Services »). Il incombe aux propriétaires des systèmes de maintenir et de mettre à jour leurs Biens de Services conformément aux normes de sécurité Citrix.

Des procédures officielles ont été mises en place pour permettre la destruction sécurisée des données Citrix et Client. Citrix détruit les données lorsqu'elles ne sont plus requises, selon leur classification et selon des processus de suppression conçus pour empêcher la reconstruction ou la lecture des données.

Les biens technologiques de Citrix sont nettoyés et mis au rebut lorsqu'ils ne sont plus nécessaires dans leur espace désigné ou attribué. Les biens technologiques comprennent, mais sans s'y limiter, les appareils informatiques individuels, les appareils informatiques multifonction, les périphériques d'acquisition d'images et les appliances réseau. Leur mise au rebut est assurée par les services de risques de sécurité globaux et de sécurité des informations.

5.2 Gestion des applications et des systèmes

Les propriétaires d'applications et de systèmes sont responsables du contrôle et de la classification des données qu'ils stockent, consultent, détruisent ou transmettent. Les employés et sous-traitants doivent réaliser d'autres contrôles, notamment :

- Classer le Contenu Client dans l'une des deux principales catégories d'informations confidentielles de Citrix et appliquer les restrictions d'accès appropriées
- Limiter l'impression du Contenu Client et détruire les documents imprimés dans des conteneurs sécurisés
- Ne pas stocker d'informations confidentielles ou d'entreprise sur un équipement ou un appareil ne respectant pas les exigences des stratégies et normes de sécurité Citrix
- Sécuriser les ordinateurs et données lorsqu'ils sont sans surveillance

5.3 Conservation des données

Le Contenu Client stocké dans le cadre des Citrix Cloud Services est accessible par le Client pendant une période limitée après la résiliation des Services. Il est ensuite supprimé (à l'exception des copies de sauvegarde) après envoi de la confirmation de la future suppression au Client. La documentation spécifique sur les services contient des informations supplémentaires. Le Contenu Client peut également être conservé suite à la réalisation des Services si requis à des fins juridiques. Citrix se conformera aux exigences de la présente Annexe jusqu'à la suppression définitive du Contenu Client.

6. Sécurité des ressources humaines

Tous les employés et sous-traitants de Citrix sont tenus de préserver la sécurité du Contenu Client. Le Code de conduite professionnelle de Citrix exige de tous ses employés et sous-traitants qu'ils adhèrent aux stratégies et normes de sécurité Citrix. Il souligne notamment l'importance de la protection des informations confidentielles et personnelles des Clients, partenaires, fournisseurs et employés de Citrix.

Tous les employés et sous-traitants de Citrix sont soumis à des obligations de confidentialité concernant les informations des Clients. Par ailleurs, l'équipe de sécurité de Citrix communique régulièrement aux employés des informations concernant la sécurité des données et du matériel physique afin de les sensibiliser à la sécurité sur des points précis.

6.1 Vérification des antécédents

Citrix vérifie les antécédents de l'ensemble des fournisseurs qu'il recrute, à l'échelle mondiale, et demande à ses fournisseurs tiers de faire de même, sauf restrictions imposées par les lois locales ou les réglementations sur le travail.

6.2 Formation

Tous les employés doivent suivre une formation sur la protection des données et sur les stratégies d'entreprise visant à préserver la sécurité des informations confidentielles de Citrix, qui comprennent les informations confidentielles de nos Clients, partenaires, fournisseurs et employés. Cette formation porte sur les pratiques de confidentialité et les principes applicables au traitement des informations personnelles par les employés, notamment la nécessité de restreindre l'utilisation, l'accès, le partage et la conservation des informations à caractère personnel. Les membres de l'équipe d'ingénierie suivent une formation spécifique portant sur la sécurisation du développement, de l'architecture et du code.

6.3 Application

Tous les employés sont tenus de respecter les stratégies et les normes de Citrix en matière de sécurité et de confidentialité. Tout manquement pourra faire l'objet de sanctions disciplinaires pouvant aller jusqu'à la résiliation du contrat de travail.

7. Sécurité des opérations

7.1 Sécurité des réseaux et des systèmes

Citrix a établi des normes de sécurisation renforcée pour les réseaux et les systèmes afin d'en sécuriser leur configuration. Selon ces normes, les procédures requises comprennent, sans s'y limiter :

- Modification ou désactivation des paramètres et/ou des comptes par défaut
- Mise en place de bannières de connexion
- Utilisation contrôlée de l'accès des administrateurs
- Limitation des comptes de service au seul usage pour lequel ils ont été créés
- Configuration de paramètres de journalisation et d'alerte à des fins d'audit

Citrix demande l'installation de logiciels anti-programmes malveillants sur les serveurs et les postes de travail et scanne le réseau à la recherche de logiciels malveillants.

Les contrôles réseau régissent l'accès au Contenu Client. Ils comprennent, le cas échéant : la configuration d'une zone non approuvée intermédiaire entre Internet et le réseau interne qui comprend un mécanisme de sécurité pour restreindre l'accès et le trafic non autorisé, la segmentation du réseau pour empêcher l'accès non autorisé au Contenu Client, et la séparation des serveurs Web et d'application des serveurs de base de données correspondants dans une structure hiérarchisée limitant le trafic entre les niveaux.

7.2 Journalisation

Citrix collecte des Journaux afin de confirmer le bon fonctionnement de nos Services, d'aider au dépannage des problèmes du système, mais aussi de protéger et de sécuriser nos réseaux et le Contenu Client. Ces Journaux peuvent inclure l'ID d'accès, l'heure de l'accès, l'accord ou le refus de l'accès, des données de diagnostic telles que les fichiers de trace et d'incident, et d'autres informations et activités pertinentes.

Les Journaux peuvent être utilisés sous une forme identifiable (i) pour fournir, sécuriser, gérer, mesurer et améliorer les Services et analyses associées, (ii) sur demande du Client ou de ses utilisateurs finaux, et/ou (iii) pour se conformer aux stratégies Citrix, aux lois en vigueur, à la réglementation ou aux demandes gouvernementales. Cela peut inclure le contrôle des performances, de la stabilité, de l'utilisation et de la sécurité des Services et composants associés. Les Clients ne peuvent pas intervenir dans ce contrôle ou le bloquer.

Pour plus d'informations sur la gestion du Contenu Client et sur le traitement des Journaux, veuillez consulter la section Confidentialité et conformité du Citrix Trust Center, qui contient plusieurs papiers blancs sur la Journalisation Citrix.

7.3 Protection des données en transit

Citrix a déployé des protocoles de transmission sécurisés pour la transmission d'informations via des réseaux publics dans le cadre des Services. Les Services sont protégés par cryptage et leur accès via Internet est sécurisé par des connexions TLS (Transport Layer Security).

8. Sécurité physique

8.1 Installations Citrix

Citrix réalise les contrôles suivants afin d'empêcher tout accès non autorisé à ses installations :

- L'accès aux installations est limité aux personnes autorisées.
- Les visiteurs doivent s'inscrire dans un journal de visites numérique et être en permanence accompagnés ou surveillés.
- Les employés, sous-traitants et invités doivent porter des badges d'identification visibles à tout moment lorsqu'ils se trouvent dans les installations.
- Une équipe de sécurité gère et contrôle l'accès aux installations en dehors des heures de bureau.
- Des gardiens de sécurité, des systèmes de détection d'intrusions et/ou des caméras de surveillance contrôlent les points d'entrée des bâtiments, les plateformes de chargement et d'expédition ainsi que les zones d'accès au public (les moyens de contrôle d'accès peuvent varier selon les installations et leur emplacement).

Par ailleurs, les installations Citrix disposent des équipements suivants :

- Systèmes ou dispositifs d'extinction et de détection des incendies
- Systèmes ou dispositifs de contrôle climatique (température, humidité, etc.)
- Système principal de fermeture d'eau ou vannes d'isolation accessibles
- Sources secondaires d'alimentation (groupe électrogène, onduleur, etc.)
- Issues de secours et voies d'évacuation

Les armoires d'équipements situées dans les bureaux sont surveillées et sécurisées par des badges d'accès.

8.2 Centres de données

Outre les contrôles réalisés dans les installations détenues et gérées par Citrix et décrits ci-dessus, Citrix met en place des contrôles supplémentaires dans les centres de données qu'elle utilise pour fournir ses Services.

Citrix utilise des systèmes visant à prévenir les pertes de données dues à des pannes d'alimentation ou des interférences, y compris une infrastructure de services globaux et redondants configurée avec des sites de récupération d'urgence. Les centres de données et fournisseurs d'accès à Internet (FAI) sont évalués pour optimiser les performances de bande passante, de latence et d'isolation des récupérations d'urgence.

Les centres de données se trouvent dans des installations sécurisées indépendantes des opérateurs FAI et assurant la sécurité physique, la redondance de l'alimentation et de l'infrastructure et des SLA de disponibilité de la part des fournisseurs clés.

Lorsque Citrix utilise des centres de données ou des services de cloud tiers pour fournir les Services, Citrix fait appel à des fournisseurs qui doivent respecter ou dépasser les exigences de sécurité physique et environnementale en vigueur dans les installations Citrix.

9. Continuité des activités et récupération d’urgence

9.1 Continuité des activités

Citrix a mis en place des stratégies de continuité des activités en cas d’interruptions ou de situations difficiles. Les systèmes sont conçus pour que les services restent opérationnels lors de tels événements.

Citrix effectue au moins tous les deux ans une analyse de l’impact commercial pour chaque service, ainsi qu’une évaluation annuelle. L’analyse de l’impact commercial permet de créer un plan de continuité des activités (PCA) qui identifie et établit, pour chaque service, les besoins en ressources, les paramètres et méthodes de récupération, les besoins de relocalisation et les dispositifs de sécurité requis tout au long du processus afin d’éviter les pannes ou les interruptions. Tous les ans, ou dès qu’un changement organisationnel important se produit, la direction de chaque service étudie et approuve le PCA.

Citrix tient à jour des plans d’urgence et de secours pour l’ensemble de ses installations. En cas d’indisponibilité des installations, les employés ont la possibilité de travailler à distance, soit dans d’autres installations Citrix, soit dans le lieu de leur choix. Des stratégies de récupération supplémentaires sont documentées dans les PCA le cas échéant.

9.2 Récupération d’urgence

Citrix s’efforce de minimiser l’impact des perturbations de ses services ou de ses opérations en appliquant des procédures et des contrôles garantissant la stabilité et la fluidité des restaurations et récupérations des systèmes et données d’entreprise Citrix. Citrix met en place une redondance pour l’ensemble de ses données, infrastructures et systèmes critiques. Le plan de récupération d’urgence (PRU) utilise les évaluations effectuées dans l’analyse de l’impact commercial mentionnée précédemment pour identifier et documenter les paramètres de temps de récupération, les méthodes et priorités, ainsi que les dispositifs de sécurité requis tout au long du processus afin d’éviter les pannes ou les interruptions.

Le plan définit la structure et l’approche globales de la restauration des systèmes et données critiques, notamment mais sans s’y limiter :

- Les rôles et responsabilités des personnes ou des équipes
- Les coordonnées du personnel ou des intervenants tiers essentiels
- Les formations et plans exigés pour le personnel essentiel
- Les objectifs de récupération, les priorités de restauration et les indicateurs de réussite
- Le schéma de la récupération et de la restauration complètes

Tous les ans, ou dès qu’un changement organisationnel important se produit, la direction étudie et approuve le PRU.

10. Réponse aux incidents

Citrix tient à jour un plan de réponse aux incidents de cyber-sécurité décrivant les processus de détection, de signalement, d'identification, d'analyse et de réponse aux Incidents de sécurité affectant les réseaux et/ou les systèmes gérés par Citrix ou le Contenu Client. Une formation et des tests de réponse aux Incidents de sécurité ont lieu au moins une fois par an.

Le terme « Incident de sécurité » désigne tout accès non autorisé au Contenu Client, ayant pour conséquence la perte de confidentialité, d'intégrité ou de disponibilité. Si Citrix détermine que le Contenu Client sous son contrôle a été exposé à un Incident de sécurité, le Client en sera notifié dans les délais prévus par la loi. Dans sa notification, Citrix décrira, si ces informations sont connues, la nature de l'incident, la période et l'éventuel impact pour le Client.

Citrix conserve un enregistrement de chaque Incident de sécurité.

11. Gestion des fournisseurs

Citrix peut faire appel à des sous-traitants et à des agents pour réaliser les Services. Les sous-traitants et les agents doivent être autorisés à accéder au Contenu Client uniquement lorsque cela est nécessaire pour réaliser les Services et seront liés par des accords écrits les obligeant à fournir au minimum le niveau de protection de données requis par Citrix dans cette Annexe, le cas échéant. Citrix reste responsable à tout moment de la conformité de ses sous-traitants et agents avec les termes du Contrat, le cas échéant. La liste des sous-traitants ultérieurs de Citrix pouvant avoir accès au Contenu Client est disponible dans le Citrix Trust Center.

11.1 Onboarding

Le programme de gestion des risques liés aux tiers de Citrix offre une approche systématique de la gestion des risques de sécurité qu'implique le recours à des fournisseurs tiers. Citrix s'efforce d'identifier, d'analyser et d'atténuer les risques de sécurité avant de faire appel à ces tiers.

Citrix conclut des contrats avec ses fournisseurs afin de documenter les mesures de sécurité pertinentes et les obligations, conformément aux dispositions de la présente Annexe.

11.2 Évaluation continue

Citrix effectue des évaluations de sécurité périodiques visant à garantir la bonne application des mesures de sécurité tout au long de la relation avec les fournisseurs. Les modifications apportées aux services fournis ou aux contrats existants nécessitent une évaluation des risques de sécurité afin de confirmer que les changements ne présentent pas de risques supplémentaires ou inutiles.

11.3 Offboarding

Dans un délai de 90 jours précédant la résiliation ou l'expiration d'un contrat avec un fournisseur, Citrix informe l'équipe d'approvisionnement de l'entreprise qui devra coordonner la résiliation des contrats existants afin d'assurer un traitement correct et sécurisé des données et des biens de Citrix.

12. Conformité

12.1 Traitement des données à caractère personnel

Les données à caractère personnel sont des informations concernant une personne identifiée ou identifiable. Le Client détermine les données à caractère personnel qu'il inclut dans le Contenu Client. Lors de l'exécution des Services, Citrix agit comme un sous-traitant et le Client reste le responsable du traitement des données à caractère personnel figurant dans le Contenu Client. Citrix agira conformément aux instructions du Client concernant le traitement des données à caractère personnel, comme spécifié dans le Contrat.

Des informations complémentaires relatives au traitement des données à caractère personnel soumises au Règlement général sur la protection des données (RGPD), y compris les mécanismes employés pour le transfert international de ces données, sont incluses dans le Contrat de traitement des données de Citrix.

12.2 Emplacement des Services

Les Clients des Citrix Cloud Services exercent un contrôle sur le choix de l'emplacement géographique de leur environnement Cloud Services (*voir aussi la section Considérations géographiques de Citrix Cloud*). À aucun moment pendant l'abonnement aux Services Cloud, Citrix ne pourra modifier l'emplacement géographique de l'environnement choisi par le Client sans le consentement de ce dernier. Il convient de noter que, dans le cadre de la prestation générale des Services et dans la mesure où cela est nécessaire à la prestation des Services, le Contenu Client pourra être transféré aux États-Unis ou dans d'autres pays où Citrix et/ou ses fournisseurs de services opèrent.

12.3 Divulgation du Contenu Client

Citrix peut divulguer du Contenu Client si la loi l'exige, y compris en réponse à une assignation, une ordonnance judiciaire ou administrative ou tout autre instrument juridiquement contraignant (« Demande »). Sauf si la loi l'interdit, Citrix informera rapidement le Client de toute Demande et fournira au Client l'assistance raisonnablement nécessaire pour y répondre rapidement.

12.4 Sécurité du Client et exigences réglementaires

Les Services sont conçus pour être livrés au sein d'un environnement informatique plus large. De ce fait, les Clients demeurent entièrement responsables de tous les aspects sécuritaires non expressément gérés par Citrix, y compris, mais sans s'y limiter, les contrôles d'accès, pare-feu, applications et réseaux que les Clients peuvent utiliser en parallèle avec les Services.

Il incombe aux Clients de déterminer si leur utilisation des Services (y compris l'octroi à Citrix d'un accès à du Contenu Client dans le cadre des Services) est soumise à des exigences réglementaires ou de sécurité autres que celles spécifiées dans le Contrat, y compris dans la présente Annexe. Par conséquent, les Clients doivent veiller à ne pas soumettre ni stocker de Contenu Client régi par des lois imposant des contrôles spécifiques non inclus dans la présente Annexe, et notamment la Réglementation américaine sur le trafic d'armes au niveau international (ITAR), ou toute autre réglementation similaire de tout pays qui restreint l'importation ou l'exportation de produits ou services liés à la défense. En outre, les Clients ne fourniront ni ne stockeront de données médicales protégées, d'informations sur les cartes de paiement ou de données à distribution contrôlé régies par les réglementations gouvernementales, sauf mention contraire spécifiée dans le Contrat et la Description du Service applicable et si les parties ont conclu au préalable d'autres accords (tels qu'un

Contrat d’associé commercial HIPAA), comme peut le demander Citrix pour traiter ces données.

13. Audits et demandes des clients

Une fois par an maximum, Citrix répondra aux demandes d’audit sous la forme de réponses aux évaluations des risques client. Les Clients peuvent également accéder à tout moment au package Due Diligence de Citrix pour consulter un package de sécurité et un questionnaire mis à jour. Le package Due Diligence de Citrix a été créé pour répondre aux demandes des clients en matière de sécurité. Il inclut des informations immédiatement accessibles sur la gestion de la sécurité. Il comprend trois documents pour chaque produit : un questionnaire SIG (Standardized Information Gathering) créé par Shared Assessments et compilant plus de 300 questions, un aperçu des mesures et contrôles de sécurité de Citrix, ainsi qu’un package réunissant une sélection de stratégies et de contrôles. Le questionnaire SIG de Shared Assessments est largement utilisé par nos Clients et dans de nombreux secteurs. Le package Due Diligence peut être téléchargé sur le Citrix Trust Center.

14. Coordonnées de Citrix

Fonction	Coordonnées
Support technique	https://www.citrix.com/contact/technical-support.html
Signalement d'un incident de sécurité	secure@citrix.com
Vulnérabilités suspectées dans les produits Citrix	https://www.citrix.com/about/trust-center/security.html#lightbox-38764 (Cliquer sur le bouton « Signaler un problème de sécurité ».)

citrix

Équipe commerciale
Amérique du Nord | 800-424-8749 International | +1 408-790-8000

Bureaux
Siège social | 851 Cypress Creek Road Fort Lauderdale, FL 33309, États-Unis Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, États-Unis