Cloud Software Group

Annexe sur la sécurité des Services

Version 3.0

En vigueur à compter du 30 septembre 2022

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 5

Sécurité des ressources humaines 6

Sécurité des opérations 7

Cryptage 8

Sécurité physique 8

Continuité des activités et récupération d'urgence 9

Réponse aux incidents 10

Gestion des fournisseurs 10

Conformité 11

Audits et demandes des clients 12

Contacts 12

La présente Annexe sur la sécurité des Services Cloud Software Group, Inc. (« Cloud Software Group », « Nous », « Notre » ou « Nos ») (l'« Annexe ») décrit les contrôles de sécurité mis en place dans le cadre de l'exécution des services de cloud, des services de support technique ou des services de conseil (les « Services ») fournis aux clients (« Client », « Vous », « Votre » ou « Vos ») au titre de la licence et/ou du contrat de services Cloud Services Group 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 Cloud Labs) et à Nos systèmes informatiques internes non compris dans la prestation de Services.

Les termes en lettres capitales ont la signification définie dans le Contrat ou définie ici. « Contenu Client » désigne toutes les données auxquelles Nous accédons ou que Nous recevons ou que Vous envoyez ou téléchargez pour stockage ou traitement afin que Nous puissions fournir les Services. Il comprend également des informations techniques exclusives associées à votre environnement, telles que les configurations système ou réseau et les contrôles que Vous sélectionnez. « Journaux » désigne les informations relatives aux performances, à la stabilité, à l'utilisation, à la sécurité, au support, au matériel, aux logiciels, aux services ou aux périphériques associés à l'utilisation de Nos produits ou Services.

1. Champ d'application

La présente Annexe décrit les contrôles de sécurité administratifs, physiques et techniques que Nous utilisons pour préserver la confidentialité, l'intégrité et la disponibilité de Nos Services. Ces contrôles s'appliquent à Nos systèmes et environnements d'opérations et de Services. Cloud Software Group utilise la norme ISO/IEC 27002 comme référence pour son programme de sécurité des Services et a obtenu des certifications et des évaluations de l'industrie pour des Services spécifiques. Des informations supplémentaires sont disponibles dans la section « Confidentialité et conformité » de Notre Trust Center.

Dans un souci de renforcement et d'amélioration continus de ses pratiques de sécurité, Nous nous réservons le droit de modifier les contrôles décrits dans la présente Annexe. Ces modifications ne diminueront en rien le niveau de sécurité pendant la durée applicable des Services.

2. Programme de sécurité et cadre stratégique

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

2.1 Surveillance des risques de sécurité

Le Comité de surveillance des cyber-risques (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 de vérifier 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

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

2.3 Sécurité des informations

Cloud Software Group a nommé un Responsable de la sécurité des informations (Chief Information Security Officer, CISO), chargé de la supervision de la sécurité ainsi que de la stratégie, de la conformité et de l'application des politiques. 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

L'équipe de sécurité Cloud Software Group supervise l'accès physique à Nos installations.

3. Contrôle d'accès

Nous imposons 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. Nous appliquons 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

Cloud Software Group 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 vérifier le rôle et l'accès de ce dernier. Les administrateurs d'accès confirment que les autorisations nécessaires sont obtenues avant d'accorder l'accès aux systèmes ou aux données. Le principe du privilège minimum s'applique.

3.2 Contrôle des comptes

Nous contrôlons 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

Nous exigeons 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'identification

Cloud Software Group exige une authentification multifacteur pour l'accès distant par les employés à Nos systèmes et applique les pratiques suivantes en matière de traitement et de gestion des mots de passe :

- Les mots de passe sont renouvelés régulièrement, conformément aux exigences du système que Nous définissons.

- Les mots de passe doivent répondre aux exigences de longueur et de complexité, y compris un mélange de chiffres, de caractères spéciaux et de lettres majuscules et minuscules, un nombre minimal de caractères et l'interdiction de mots courants ou du dictionnaire.
- Les ID utilisateur désactivés ou arrivés à expiration ne peuvent pas être transmis à d'autres personnes.
- Nous appliquons des procédures de désactivation pour les mots de passe qui ont été divulgués par erreur.
- Nous contrôlons les tentatives répétées d'accès aux Services à l'aide de mots de passe non valides et bloquons de façon automatisée les tentatives répétées d'accès.

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

- Exiger le hachage et/ou cryptage des mots de passe tout au long de leur cycle de vie
- Interdire le partage des mots de passe

4. Développement et maintenance du système

Nous disposons 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

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

Nous utilisons 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. Nous avons 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

Notre procédure de gestion des modifications d'infrastructure et de logiciel 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 déploiement dans l'environnement de production. La gestion et le suivi des modifications d'infrastructure et de logiciel 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

Cloud Software Group maintient un inventaire dynamique des systèmes physiques et virtuels que nous gérons et utilisons pour exécuter les Services (les « Biens de Services »). Il incombe aux propriétaires des systèmes de maintenir et de mettre à jour leurs Biens de Services conformément à Nos normes de sécurité.

Des procédures officielles ont été mises en place pour permettre la destruction sécurisée des données Cloud Software Group et Client. Nous détruisons 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.

Nos biens technologiques 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 de stockage, les périphériques d'imagerie 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 de Nos Services de cloud 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 sont tenus de préserver la sécurité du Contenu Client. Notre Code de conduite professionnelle exige de tous les employés et sous-traitants qu'ils adhèrent à Nos stratégies et normes de sécurité. Il souligne notamment l'importance de la protection des informations confidentielles et personnelles des Clients, partenaires, fournisseurs et employés.

Tous les employés et sous-traitants sont soumis à des obligations de confidentialité concernant les informations des Clients. Par ailleurs, l'équipe de sécurité Cloud Software Group 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

Nous faisons actuellement appel à des fournisseurs de vérifications des antécédents pour toutes les nouvelles embauches dans le monde entier et exigeons les mêmes vérifications pour le personnel de nos fournisseurs tiers, 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 de Nos informations confidentielles, 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 Nos stratégies et normes 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

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

- Modification ou désactivation des paramètres et/ou des comptes par défaut
- 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

Nous demandons l'installation de logiciels anti-programmes malveillants sur les serveurs et les postes de travail et analysons 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

Nous collectons 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.

Nous collectons et utilisons les Journaux (i) pour fournir, sécuriser, gérer, mesurer et améliorer les Services, (ii) à la demande du Client ou de ses utilisateurs finaux, (iii) pour la facturation, la gestion des comptes, les rapports internes et la stratégie produit, et/ou (iv) pour se conformer aux accords, politiques, lois applicables, réglementations ou demandes gouvernementales. Cela peut inclure le contrôle des performances, de la stabilité, de l'utilisation et de la sécurité des Services et composants associés. 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 Clients ne peuvent pas intervenir dans ce contrôle ou le bloquer.

Pour plus d'informations sur la gestion du Contenu Client et le traitement des Journaux, veuillez consulter notre Trust Center (Cloud Assurance Data Protection & Security section) qui contient plusieurs livres blancs sur la journalisation des Services de cloud Citrix.

7.3 Gestion des certificats, des informations d'identification et des secrets

Cloud Software Group maintient des politiques qui couvrent le cycle de vie des certificats, des informations d'identification et des secrets pour garantir la protection, la disponibilité et la confidentialité. Les gardiens de secrets doivent être documentés et reconnaître formellement qu'ils acceptent les responsabilités liées à la gestion des secrets.

Ces responsabilités sont les suivantes, mais sans s'y limiter :

- Les certificats doivent être délivrés par une autorité de certification agréée.
- Les clés cryptographiques ne peuvent pas être stockées ou transmises en texte brut et doivent utiliser des protocoles cryptographiques approuvés solides.
- Les informations d'identification et les secrets doivent faire l'objet d'un renouvellement au moins une fois par an et être stockés dans un outil de gestion d'authentification privilégié approuvé.

7.4 Gestion des vulnérabilités

Nous surveillons régulièrement les applications et les systèmes à la recherche de vulnérabilités grâce à une analyse automatisée des vulnérabilités et des ports.

Les vulnérabilités identifiées doivent être corrigées dans un délai qui dépend du degré de gravité et des recommandations du fournisseur. Dans les cas où un correctif, une mise à jour ou une atténuation permanente n'est pas disponible, des contre-mesures appropriées seront utilisées pour réduire le risque d'exploitation de la vulnérabilité.

8. Cryptage

8.1 Protection des données en transit

Cloud Software Group 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).

8.2 Protection des données au repos

Nous exigeons que tous les postes de travail utilisés pour fournir les Services soient cryptés grâce à un cryptage complet du disque de 128 bits au minimum. Le Contenu Client ne peut être stocké sur aucun appareil portable à moins qu'il ne soit crypté.

Certains Services de cloud cryptent certains éléments de données par défaut et peuvent également fournir d'autres fonctionnalités de cryptage que les clients peuvent mettre en œuvre. Veuillez consulter la documentation des Services de cloud applicables pour plus de détails.

9. Sécurité physique

9.1 Installations

Nous réalisons les contrôles suivants afin d'empêcher tout accès non autorisé aux 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 agents 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 Cloud Software Group 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
- Issues de secours et voies d'évacuation

Les armoires de données situées dans les bureaux sont protégées par des badges d'accès.

9.2 Centres de données

Outre les contrôles réalisés dans les installations détenues et gérées par Cloud Software Group et décrits ci-dessus, Nous mettons en place des contrôles supplémentaires dans les centres de données utilisés pour fournir les Services.

Nous utilisons 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 Nous utilisons des centres de données ou des services de cloud tiers pour fournir les Services, Nous faisons appel à des fournisseurs qui doivent respecter ou dépasser les exigences de sécurité physique et environnementale en vigueur dans Nos installations.

10. Continuité des activités et récupération d'urgence

10.1 Continuité des activités

Cloud Software Group 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.

Nous effectuons 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.

Nous tenons à jour des plans d'urgence et de secours pour l'ensemble de Nos installations. En cas d'indisponibilité des installations, les employés ont la possibilité de travailler à distance, soit dans d'autres installations Cloud Software Group, soit dans le lieu de leur choix. Des stratégies de récupération supplémentaires sont documentées dans les PCA le cas échéant.

10.2 Récupération d'urgence

Nous nous efforçons de minimiser l'impact des perturbations des services ou des opérations en appliquant des procédures et des contrôles garantissant la stabilité et la fluidité des restaurations et récupérations de Nos systèmes et données d'entreprise. Cloud Software Group 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.

11. Réponse aux incidents

Cloud Software Group 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 Nos réseaux et/ou systèmes gérés ou le Contenu Client. Une formation et des tests de réponse aux Incidents de sécurité ont lieu au moins une fois par an.

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

Nous conservons un enregistrement de chaque Incident de sécurité.

12. Gestion des fournisseurs

Cloud Software Group 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 Nous dans cette Annexe, le cas échéant. Nous restons responsables à tout moment de la conformité des sous-traitants et agents avec les termes du Contrat, le cas échéant. La liste des sous-traitants Cloud Software Group pouvant avoir accès au Contenu Client est disponible sur Notre Trust Center.

12.1 Intégration

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

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

12.2 Évaluation continue

Nous effectuons 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.

12.3 Fin de la relation

Nous nous efforçons d'informer l'équipe d'approvisionnement de l'entreprise au moins 90 jours avant la résiliation ou l'expiration d'un contrat avec un fournisseur (sauf si une résiliation anticipée est nécessaire). L'équipe d'approvisionnement de l'entreprise coordonne la résiliation des contrats existants afin d'assurer un traitement correct et sécurisé de Nos données et biens.

13. Conformité

13.1 Traitement des données à caractère personnel

Les données à caractère personnel sont des informations concernant une personne identifiée ou identifiable. Vous déterminez les données à caractère

personnel que Vous incluez dans le Contenu Client. Lors de l'exécution des Services, Nous agissons comme un sous-traitant et Vous restez le responsable du traitement des données à caractère personnel figurant dans le Contenu Client. Nous agirons conformément à Vos instructions 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 l'Addendum relatif au traitement des données de Cloud Software Group.

13.2 Emplacement des services

Les Clients des Services de cloud conservent le contrôle sur le choix de l'emplacement géographique de leurs Services de cloud. À aucun moment pendant l'abonnement aux Services de cloud, Nous ne pourrons modifier l'emplacement géographique de l'environnement que Vous aurez choisi sans Votre consentement. Il convient de noter que certains Services de cloud peuvent ne pas permettre le choix de certains emplacements géographiques, et 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.

13.3 Divulgation du Contenu Client

Nous pouvons 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, Nous Vous informerons rapidement de toute Demande et Vous apporterons l'aide raisonnablement nécessaire pour y répondre rapidement.

13.4 Sécurité du Client et exigences réglementaires

Les Services sont conçus pour être fournis au sein d'un environnement informatique Client plus large. De ce fait, les Clients conservent l'entière responsabilité de tous les aspects sécuritaires non expressément gérés par Citrix, y compris, mais sans s'y limiter, l'intégration technique avec les Services, la gestion et les contrôles de l'accès des utilisateurs, et l'ensemble des applications et réseaux que les Clients peuvent utiliser en parallèle avec les Services.

Il Vous incombe de déterminer si Votre utilisation des Services (y compris le fait de Nous fournir 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 contrôlée 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 Nous pouvons le demander pour traiter ces données.

14. Audits et demandes des clients

Une fois par an maximum, Cloud Software Group répondra aux demandes d'audit sous la forme de réponses aux évaluations des risques Client. Les Clients peuvent également accéder à tout moment à Notre package Due Diligence pour consulter un package de sécurité et un questionnaire mis à jour. Notre package Due Diligence a été créé pour les demandes de sécurité des clients et fournit des informations de sécurité facilement accessibles, y compris un questionnaire SIG (Standardized Information Gathering) Lite de Shared Assessments pour Nos Services de cloud. Le package Due Diligence peut être téléchargé sur Notre Trust Center dans la section Cloud Assurance - Data Protection and Security.

15. Contacts

Fonction	Contact
Support technique	https://www.citrix.com/contact/technical-support.html
Signalement d'un incident de sécurité	secure@citrix.com
Vulnérabilités suspectées dans Nos Services	https://www.citrix.com/fr-fr/about/trust-center/ (Cliquez sur le bouton « Signaler un problème de sécurité ».)

Équipe commerciale
Amérique du Nord | 800-424-8749 Dans le monde entier | +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