Dernière révision : 1er mars 2018

Pièce Sécurité des Services Citrix

La Pièce Sécurité des Services Citrix (la Pièce) décrit les contrôles de sécurité technique et organisationnelle utilisés dans le cadre des services Citrix Cloud, des services de support technique ou des services de conseil sous licence, abonnement ou contrat de service Citrix. La Pièce est intégrée à titre de référence dans lesdits contrats de service (les « Contrats »). La Pièce ne s'applique pas aux services Bêta, Labs ou Tech Preview, y compris les Citrix Cloud Labs.
Les termes en lettres capitales ont la signification définie dans le Contrat ou définie ici, y compris dans l'Article 7, Définitions, ci-dessous.

Article 1. Contrôles de sécurité Citrix

Cet Article décrit les contrôles physiques, logiques et administratifs utilisés par Citrix pour sécuriser les Services et les obligations de sécurité associés aux Clients. Le programme de sécurité des Services Citrix repose sur la norme ISO/IEC 27002.

Les contrôles spécifiés dans l'Article 1.A s'appliquent à tous les Services. Les contrôles supplémentaires spécifiés dans la Section 1B s'appliquent à tous les Citrix Cloud Services généralement disponibles (collectivement, les « Services Cloud »).

Citrix se réserve le droit de modifier les contrôles spécifiés dans l'Article 1 sous réserve que les contrôles utilisés pendant la durée d'un service pour lequel le Client a payé protègent le contenu du Client au moins aussi bien que ceux spécifiés dans l'Article 1 à la date d'effet de ladite durée.

1.A. Contrôles de sécurité d'entreprise – Tous les services

Domaine	Contrôle(s)
Gestion du Programme de sécurité	**Propriété de la sécurité**. Citrix a nommé un ou plusieurs responsables de la sécurité pour coordonner et surveiller les contrôles de sécurité des Services. **Rôles et responsabilités en matière de Sécurité**. Le personnel Citrix ayant accès au Contenu Client doit respecter des obligations de sécurité. **Stratégies de sécurité du Service.** Citrix définit un cadre de sécurité global (Global Security Framework - GSF), qui fournit les principes de sécurité généraux établis et approuvés par la direction de Citrix. Les stratégies mentionnent les exigences de sécurité de façon claire et concise. Les normes définissent le processus ou la méthodologie à suivre pour adhérer aux

Domaine	Contrôle(s)
	exigences de stratégie. Le programme de sécurité GSF fait l'objet de révisions et d'évaluations régulières. Citrix tient à jour un résumé du programme GSF et peut le fournir aux clients sur demande. **Gestion des risques du produit.** Citrix évalue les domaines de risque clés associés aux Services, y compris, par exemple et le cas échéant, l'évaluation des risques de confidentialité, les révisions open source et l'analyse du contrôle des exportations.
Gestion des biens	**Inventaire des biens**. Citrix tient à jour un inventaire de l'équipement géré par Citrix utilisé pour exécuter les Services (les « Biens »). Il incombe aux propriétaires du système identifiés de maintenir et mettre à jour l'inventaire, le cas échéant. **Gestion des biens et des données** Citrix identifie et classifie le Contenu Client pour s'assurer que l'accès est correctement restreint. Citrix impose des restrictions en matière d'impression du Contenu Client et de mise au rebut des documents imprimés contenant du Contenu Client. Le personnel Citrix doit obtenir l'autorisation avant de stocker du Contenu Client sur des périphériques portables, d'accéder à distance à du Contenu Client ou de traiter du Contenu Client en dehors des locaux gérés par Citrix ou ses fournisseurs de services.
Gestion de l'accès	**Stratégie d'accès.** Citrix conserve un enregistrement des privilèges de sécurité des personnes ayant accès au Contenu Client et suit le principe de moindre privilège. **Autorisation d'accès** Citrix conserve et met à jour un enregistrement du personnel autorisé à accéder aux systèmes Citrix contenant du Contenu Client. Le nouvel accès aux systèmes est contrôlé et approuvé par la direction avant d'être accordé. Citrix contrôle régulièrement les comptes utilisateur et les autorisations affectées pour les principaux systèmes. Citrix identifie le personnel pouvant accorder, modifier ou annuler l'accès autorisé aux données et aux ressources. Citrix s'assure que si plusieurs personnes ont accès à des systèmes renfermant du Contenu Client, ces personnes possèdent des identifiants/sessions distincts.

Domaine	Contrôle(s)
	Moindre privilège Citrix restreint l'accès au Contenu Client aux personnes nécessitant ayant besoin de cet accès pour réaliser les tâches liées à leur fonction. **Intégrité et confidentialité** Citrix demande aux utilisateurs de sécuriser les ordinateurs et les données pendant leur absence. Citrix demande à ce que les mots de passe restent confidentiels au cours de leur cycle de vie. **Authentification** Citrix applique les pratiques standard du secteur pour identifier et authentifier les utilisateurs accédant aux systèmes d'information. Si les mécanismes d'authentification sont basés sur des mots de passe, Citrix suit les pratiques standard en matière d'utilisation et de gestion des mots de passe, y compris les règles suivantes : Les mots de passe sont renouvelés régulièrement, comme défini par les exigences système et les normes Citrix. Les mots de passe doivent respecter les exigences en matière de longueur et de complexité, notamment une longueur minimale de 8 caractères. Le personnel ne doit pas partager les mots de passe. Les identifiants désactivés ou arrivés à expiration ne peuvent pas être transmis à d'autres personnes. Citrix gère des procédures de désactivation des mots de passe qui ont été corrompus ou révélés par inadvertance. Citrix contrôle les tentatives répétées d'accès aux Services via un mot de passe non valide. Citrix applique des pratiques destinées à garantir la confidentialité et l'intégrité des mots de passe lorsqu'ils sont attribués, distribués et stockés.
Prévention des pertes	**Logiciels malveillants**. Citrix utilise un logiciel antivirus et d'autres outils pour éviter que des logiciels malveillants accèdent sans autorisation au Contenu Client, y compris tout logiciel malveillant provenant de réseaux publics. **Mise au rebut des supports.** Citrix met au rebut les supports lorsqu'ils ne sont plus utiles, en tenant compte de leur classification et en utilisant des processus de mise au rebut sécurisés.

Domaine	Contrôle(s)
Sécurité physique et de l'environnement (contrôle d'accès, contrôle de disponibilité)	**Accès physique aux locaux Citrix**. Citrix limite l'accès des locaux aux personnes autorisées. Les employés, sous-traitants et invités doivent porter des badges d'identification visibles à tout moment lorsqu'ils se trouvent dans les locaux. Citrix contrôle les points d'entrée des locaux via diverses méthodes, notamment des gardiens de sécurité, des systèmes de détection d'intrusions et des caméras de surveillance. **Protection contre les interruptions**. Citrix utilise des systèmes visant à prévenir les pertes de données dues à une panne d'alimentation ou une interférence sur la ligne, y compris une infrastructure de service globale et redondante configurée avec des sites de récupération d'urgence ; l'évaluation des centres de données et des fournisseurs d'accès à Internet (FAI) pour optimiser les performances de bande passante, de latence et d'isolation des récupérations d'urgence ; l'installation des centres de données dans des locaux sécurisés faisant appel à un FAI neutre et offrant une sécurité physique, une redondance de l'alimentation et une redondance de l'infrastructure ; et les contrats de temps d'activité de prestataires clés. **Centres de données hébergés.** Lorsque Citrix utilise des centres de données partagés tiers pour fournir les Services, Citrix demande au fournisseur de services de respecter ou de dépasser les exigences de sécurité physique et environnementale en vigueur dans les locaux Citrix. Les exigences de sécurité minimales incluent, sans toutefois s'y limiter : • Restrictions et protections d'accès physique (authentification, journaux, surveillance, etc.) • Séparation appropriée des environnements • Mécanismes d'élimination, de détection et de prévention des incendies • Systèmes de contrôle du climat (température, humidité, etc.) **cloud Computing.** Lorsque Citrix utilise des solutions XaaS [infrastructure en tant que service (IaaS), plate-forme en tant que service (PaaS), logiciel en tant que Service (SaaS)] pour fournir les Services, Citrix s'engage avec des fournisseurs de Xaas qui fournissent un niveau de contrôle matériel de l'accès physique identique à ses centres de données hébergés.
Sécurité des applications et du développement	**Développement et maintenance du système.** Citrix tient à jour un processus Secure by Design (sécurité dès la conception), qui se compose de normes et de 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 relative à l'utilisation des données test. Ce processus est géré et contrôlé par une équipe d'ingénierie de sécurité spécialisée, qui est également responsable de la révision de la conception, de la modélisation des menaces, de la

Domaine	Contrôle(s)
	révision et du contrôle manuels et des tests de pénétration. **Gestion Open Source**. Citrix utilise un système basé sur logiciel pour gérer les révisions et approbations open source. En outre, Citrix effectue des analyses et des audits périodiques de ses produits logiciels pour confirmer la conformité open source. **Gestion des modifications.** Citrix tient à jour des procédures de contrôle des modifications qui répondent aux exigences de sécurité des systèmes d'information, de test, d'acceptation des tests et de sécurité relative à l'utilisation des données test. Les modifications logicielles et de configuration sont gérées et suivies à l'aide de systèmes de ticket standard.
Opérations sécurisées	**Conception du réseau**. Citrix implémente des mécanismes conçus pour appliquer les normes et stratégies de gestion de l'accès dans les Services, y compris les contrôles réseau sur l'accès au Contenu Client. Cela comprend, 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 ; et la séparation des serveurs Web et d'application des serveurs de base de données correspondants dans une structure à niveaux limitant le trafic entre les niveaux.
Gestion des incidents	**Réponse aux incidents**. Citrix tient à jour un programme de réponse aux incidents visant à contenir, analyser, corriger et communiquer les incidents de sécurité impactant les réseaux gérés par Citrix et/ou les systèmes ou le Contenu Client. **Notification des incidents**. Si Citrix détermine que le Contenu Client sous son contrôle a été exposé à un Incident de Sécurité, le Client en sera notifié dans la période requise par la loi applicable. **Enregistrement des incidents**. Citrix tient à jour un enregistrement des Incidents de Sécurité connus avec une description de l'incident, la période, les conséquences de l'incident, le nom de la personne ayant rapporté l'incident, le nom de la personne à qui l'incident a été rapporté et la procédure de récupération des données et des services, le cas échéant.
Gestion des fournisseurs	**Intégration**. Citrix effectue des évaluations de sécurité des fournisseurs de services qui accèdent au Contenu Client et/ou aux composants des Services qui traitent le Contenu Client. Citrix nécessite que les fournisseurs de services connectés aux Services respectent le niveau de sécurité dans cette Section applicable aux services qu'ils fournissent. Les fournisseurs de services pouvant accéder au Contenu Client soumis aux lois de l'Union européenne doivent s'auto-certifier auprès des programmes de confidentialité UE-US et UE-Suisse ou exécuter les clauses contractuelles types. **Maintenance continue.** Les fournisseurs de services sont évalués périodiquement, en fonction de la sensibilité et des risques associés à leurs services.

Domaine	Contrôle(s)
	Départ. À l'issue de la relation avec le fournisseur, le fournisseur de services doit retourner tout le Contenu Client en sa possession ou certifier que le Contenu Client a été détruit en toute sécurité.
Continuité des activités et récupération d'urgence	**Continuité des activités.** Citrix tient à jour des plans d'urgence et de contingence des locaux dans lesquels se trouvent les systèmes d'information Citrix qui traitent le Contenu Client. **Récupération d'urgence.** Le stockage redondant de Citrix et ses procédures de récupération des données sont conçus pour tenter de reconstruire le Contenu Client dans son état d'origine ou selon l'état de sa dernière réplication.
Obligations relatives à la sécurité du Client	Il incombe au Client de gérer la sécurité non incluse expressément dans les Services. Sont concernés, entre autres : • la limitation de l'accès de Citrix uniquement au Contenu Client nécessaire pour permettre au Client de recevoir les Services ; • la protection de ses composants réseau et de service contre les interférences, y compris la surveillance et la sécurisation de ses réseaux et de l'équipement de traitement ; • le téléchargement du Contenu Client le cas échéant, pendant et après la durée des Services. • Citrix crypte les données en transit par défaut ou fournit aux clients des moyens pour crypter les données en transit. Des informations complémentaires sont disponibles dans la documentation produit des Services. Le Client doit s'assurer que les données en transit sont correctement sécurisées.

1.B. Contrôles de sécurité de Services Cloud supplémentaires

Domaine	Contrôle(s)
Protection des données (contrôle de la disponibilité, contrôle de la transmission, suppression des données)	**Procédures de basculement**. Citrix met en œuvre des mécanismes destinés à traiter la perte de disponibilité du Contenu Client, y compris le stockage de copies du Contenu Client dans un lieu différent de celui où se trouve l'équipement informatique principal qui traite le Contenu Client. **Données au-delà des frontières**. Citrix crypte ou autorise le Client à crypter le Contenu Client transmis sur les réseaux publics intégrés à un Service. **Conservation.** Citrix peut conserver le Contenu Client qui suit la période de Service et l'archiver à des fins d'accès des clients si cela est nécessaire pour des raisons légales. Citrix doit se conformer aux exigences de la présente Pièce jusqu'à la suppression définitive du Contenu Client. Soumis aux Retours définis ci-après, Citrix n'est pas tenu de conserver le

Domaine	Contrôle(s)
	Contenu Client après la fin du Service. **Retours.** Sous réserve de disponibilité et de la Description des Services applicable, le Client dispose de trente (30) jours pour télécharger le Contenu Client après l'expiration. **Suppression des données**. Citrix supprimera de manière sécurisée le Contenu Client lorsque celui-ci ne sera plus nécessaire pour des raisons légales.
Opérations sécurisées	**Consignation des événements**. Citrix collecte des journaux dans le cadre de certains Services. 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 de panne, et d'autres activités pertinentes. Les journaux sont utilisés (**i**) pour alimenter, sécuriser, gérer, mesurer et améliorer les Services et analyses associées, (**ii**) comme demandé ou exigé par le Client et ses Utilisateurs, et/ou (**iii**) pour se conformer aux stratégies Citrix, à la loi applicable, à la réglementation ou aux demandes gouvernementales. Cela peut inclure le contrôle des performances, de la stabilité, de l'utilisation et la sécurité des Services et composants associés. Le Client ne peut pas bloquer ou intervenir dans ce contrôle. Citrix peut compléter les Journaux avec des informations collectées auprès de tiers aux fins spécifiées ci-dessus. Les Journaux peuvent être utilisées à des fins non spécifiées dans la présente Pièce uniquement sous forme agrégée.
Continuité des activités et récupération d'urgence	**Sauvegardes.** Sauf mention contraire spécifiée dans la Description des Services respective, les Services doivent être maintenus dans des clusters actifs-actifs haute disponibilité couvrant plusieurs sites physiques. Les systèmes qui ne sont pas exécutés dans une configuration active-active sont sauvegardés selon les Objectifs de niveau de service du Service spécifique.

Article 2. **<u>Traitement des Données à caractère personnel</u>**

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. En exécutant les Services, Citrix agit comme un sous-traitant et le Client reste le responsable du traitement des Données à caractère personnel contenues 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, y compris les mécanismes employés pour le transfert international de ces données, sont incluses dans la Pièce I intitulée « Conditions du règlement général sur la protection des données ».

Article 3. Emplacement des Services

Le Contenu Client peut être transféré, stocké et/ou traité aux États-Unis ou dans d'autres pays où Citrix et/ou ses fournisseurs de services opèrent. Les exigences relatives à la Pièce continuent de s'appliquer, quel que soit l'endroit où Citrix stocke ou traite le Contenu Client.

Les parties peuvent négocier en bonne foi des accords de traitement ou de transfert de données supplémentaires nécessaires pour faciliter le transfert légal des données au niveau international, conformément à la fourniture des Services par Citrix.

Article 4. Divulgation du Contenu client

Le Client accepte que Citrix divulgue le Contenu Client comme défini dans la présente section.
Citrix peut employer des sous-traitants et des agents pour effectuer ces Services. Les sous-traitants et les agents doivent être autorisés à accéder au Contenu Client uniquement lorsque cela est nécessaire pour effectuer les Services et seront liés par des accords écrits les obligeant à fournir au moins le niveau de protection de données requis par Citrix dans cette Pièce, 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.

Citrix peut également divulguer du Contenu Client (a) à des entités affiliées à des fins conformes au Contrat ; (b) dans le cadre d'une fusion, d'une acquisition, d'une vente, d'une liquidation ou de toute autre réorganisation anticipée ou effective de tout ou partie de son activité, tout en restant soumis à l'obligation de protéger le Contenu Client conformément aux conditions du Contrat ; ou (c) à des fins juridiques, y compris l'application de ses droits, la détection et la prévention des fraudes, la protection contre les violations de droits ou de propriété de Citrix, des Clients, des Utilisateurs ou du public ; et (c) 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.

Article 5. Obligations du Client

1. Généralités. Le Client peut utiliser les Services et y accéder dans le cadre autorisé par le présent Contrat. Le Client respectera toutes les lois applicables dans le cadre de l'utilisation des Services.

2. Autorisations. Il incombe au Client d'obtenir toutes les autorisations nécessaires pour permettre à Citrix d'exécuter les Services, y compris la fourniture des notes et l'obtention des accords ou licences nécessaires pour que Citrix puisse accéder au Contenu Client et le traiter comme défini dans la présente Pièce.

3. Réglementation. Il incombe au Client de déterminer si un Contenu Client est soumis à des exigences réglementaires ou de sécurité autres que celles spécifiées dans le présent Contrat, y compris la présente Pièce. Le Client ne soumettra ni ne stockera tout Contenu Client régi par 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, le Client ne fournira ni ne stockera tout Contenu Client soumis à d'autres exigences réglementaires, telles que les règlements sur les données de santé protégées (Protected Health Information, PHI), les données de carte de paiement (Payment Card Information, PCI) ou les données de diffusion contrôlées régies par les réglementations gouvernementales, sauf mention contraire spécifiée dans la Commande du Client et la Description du Service applicable et si les parties ont accepté au

préalable d'autres accords (tels qu'un Contrat d'associé commercial, BAA), comme peut le demander Citrix pour traiter ces données. Les Clients du service ShareFile peuvent contacter Citrix à l'adresse privacy@sharefile.com pour demander un BAA.

4. Environnement de sécurité du Client. Les Services sont conçus pour être livrés uniquement au sein d'un environnement sécuritaire élargi du Client. Le Client assurera une fonctionnalité de sécurité appropriée pour tous les composants non expressément gérés par Citrix, y compris mais sans s'y limiter, les contrôles d'accès, pare-feu, applications et réseaux utilisés en conjonction avec les Services. Voir la section 1.A. intitulée « Obligations relatives à la sécurité du Client », ci-dessus.

5. Notification de sécurité. Il incombe au Client d'informer rapidement Citrix de tout incident de sécurité impliquant les Services et/ou le Contenu Client, comme défini dans l'article VI, « Coordonnées de Citrix », ci-dessous.

6. Conformité de l'Utilisateur. Le Client est responsable du respect des termes de la présente Commande et du présent Contrat par ses Utilisateurs.

Article 6. Coordonnées de Citrix

FONCTION	COORDONNÉES
Support client	https://www.citrix.com/contact/technical-support.html
Signalement d'un incident	secure@citrix.com
Vulnérabilités suspectées dans les produits Citrix	secure@citrix.com

Article 7. Définitions

Les termes en lettres capitales ont la signification définie dans le présent Contrat ou ci-dessous. En cas de conflit entre les termes restants du Contrat et toute définition ci-dessous, la définition s'applique à la présente Pièce.

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.

Journal désigne un enregistrement d'événements liés aux Services, y compris des enregistrements mesurant les performances, la stabilité, l'utilisation, la sécurité et le support.

Incident de sécurité désigne tout accès non autorisé au Contenu Client, ayant pour conséquence la perte de confidentialité, d'intégrité ou de disponibilité.