**Aperçu de la sécurité de l'information à OneSpan**
**Version : Septembre 2023**

L'optimisation des efforts et des ressources en matière de sécurité pour protéger correctement les systèmes d'information et les actifs informationnels de OneSpan nécessite une approche structurée pour identifier les différents actifs à protéger, leur importance pour OneSpan et les risques auxquels ils sont exposés. Au moins une fois par an, nous identifions les mesures de sécurité déjà en place, nous évaluons leur efficacité afin de mesurer le risque résiduel et nous hiérarchisons les changements qui seraient nécessaires pour ramener le risque à un niveau acceptable pour OneSpan.

*Gouvernance*
La politique de gestion des risques liés à la sécurité de l'information de OneSpan formalise la responsabilité de chacun, des cadres supérieurs aux utilisateurs individuels, dans la réduction des risques liés à la sécurité de l'information. Cette politique est approuvée par le comité directeur de la sécurité de l'information, elle est révisée chaque année pour tenir compte des changements dans l'environnement de risque d'OneSpan et elle décrit un processus formel d'identification, d'évaluation et de suivi des principaux risques liés à la sécurité de l'information. Si nécessaire, un plan de traitement des risques est mis en œuvre pour ramener les niveaux de risque en deçà du seuil de tolérance acceptable.

Le comité directeur de la sécurité de l'information de OneSpan est composé de dirigeants clés qui agissent dans le cadre d'une charte officielle. Son rôle est de superviser le programme de sécurité de l'information de l'entreprise et la position de OneSpan en matière de sécurité. Son rôle consiste également à suivre l'évolution des risques liés à la sécurité de l'information, ainsi qu'à approuver et à suivre les initiatives de réduction des risques. Le comité directeur de la sécurité de l'information se réunit régulièrement, au moins une fois par trimestre, avec le responsable de la sécurité de l'information de OneSpan.

Le conseil d'administration de OneSpan supervise également l'avancement du programme de sécurité de l'information et la variation des risques liés à la sécurité de l'information par le biais de briefings trimestriels sur la sécurité de l'information, au minimum. Le comité d'audit, composé uniquement d'administrateurs indépendants, est le principal responsable de cette surveillance.

*Assurance*
OneSpan souscrit une assurance habituelle contre les risques de cybersécurité qui comprend l'accès à une unité d'assistance à la gestion des violations de données si nécessaire et utilise les services d'un courtier d'assurance indépendant qui fournit également des conseils en matière d'assurance.

*Examens et certifications*
Pour les systèmes d'information et les actifs informationnels internes de OneSpan, nous procédons à des examens internes réguliers et mettons en œuvre une surveillance continue de la sécurité. Afin de fournir une assurance supplémentaire, OneSpan effectue des examens indépendants périodiques des principaux éléments de son programme de sécurité. Ces examens sont effectués par des personnes indépendantes du domaine examiné. Les domaines à examiner et le calendrier de ces examens sont déterminés en fonction de leur criticité.

Pour les produits et services destinés aux clients, outre les examens et tests internes, nous nous soumettons à divers examens et certifications externes. Certains de nos produits sont certifiés en vertu de normes techniques spécifiques ou de directives sectorielles, telles que la réglementation bancaire européenne dite PSD2. En outre, nos plateformes Cloud pour les solutions SaaS sont contrôlées chaque année par des auditeurs externes indépendants. Les auditeurs examinent nos plateformes au regard des normes Service Organization Controls (SOC) 2 et ISO 27001, 27017 et 27018. Nous recevons des certifications annuelles dans le cadre de ces audits.

En outre, nous menons des activités d'autocertification pour les normes ou réglementations qui ne sont pas couvertes par les auditeurs externes, telles que le règlement général sur la protection des données (RGPD) dans l'Union européenne et l'Espace économique européen et les réglementations du Health Insurance Portability and Accountability Act (HIPAA) aux États-Unis.

*Mesures techniques et organisationnelles*

La liste des mesures techniques et organisationnelles de OneSpan se trouve ici (https://www.onespan.com/fr/support/securite/psirt/processus).

*Engagement d'un délégué à la protection des données (DPD) externe et indépendant*
Pour aider à assurer la conformité avec la législation applicable en matière de protection des données et pour aider à traiter les violations de données impliquant des données à caractère personnel, le fournisseur a contracté un responsable externe indépendant de la protection des données avec une certification de DPD d'une tierce partie et une certification d'auditeur principal GDPR. Le DPD a également suivi des cours de certification de responsable de la sécurité de l'information. Le DPD suit une formation annuelle de mise à jour et surveille les changements dans la loi sur la protection des données, soutenu par un système d'information sur la protection des données qui comprend une orientation globale des données et une gestion de la protection des données (OneTrust).

*Risques des tiers*

Le programme de gestion des risques de sécurité des fournisseurs de OneSpan couvre tous les fournisseurs qui doivent se connecter aux systèmes de OneSpan ou accéder aux informations confidentielles de OneSpan. Des examens de sécurité sont effectués périodiquement, en fonction de la criticité du fournisseur, afin d'identifier les problèmes de sécurité potentiels liés aux systèmes ou aux pratiques du fournisseur.

*Formation*
Afin de réduire la probabilité et l'impact des incidents de sécurité, OneSpan a mis en place un programme global de formation à la sécurité qui comprend une formation obligatoire à la sécurité et à la protection des données pour l'ensemble du personnel au moment de l'embauche et chaque année par la suite. Des formations supplémentaires sont proposées aux employés en fonction de leur rôle. Il s'agit notamment d'une formation au développement sécurisé pour les développeurs, à l'appui du cycle de développement sécurisé de OneSpan, ainsi que d'une formation à la réponse aux incidents.

En réponse aux diverses attaques de phishing qui sont souvent à l'origine des failles de sécurité, et en plus des divers contrôles techniques en place, OneSpan a mis en place des campagnes de phishing récurrentes qui ciblent ses employés afin d'améliorer leur capacité à reconnaître et à signaler les messages de phishing. Les employés qui réagissent de manière inappropriée aux campagnes de phishing internes reçoivent une formation corrective supplémentaire.