Willis Towers Watson

Cybersécurité de l’information et confidentialité des données – Aperçu

Version 3.1

Les renseignements fournis dans le présent document sont destinés à Willis Towers Watson et à ses filiales. Il s’agit d’un document confidentiel réservé à l’usage des clients actuels et éventuels de Willis Towers Watson et de ses filiales pour évaluer les capacités de prestataire de services de Willis Towers Watson.

Willis Towers Watson

Introduction

Willis Towers Watson reconnaît qu'une gestion efficace de la sécurité de l'information et des risques qui s'y rattachent est essentielle au maintien de la confiance que lui témoignent ses clients. Nous adoptons une démarche proactive à l'égard de la protection et de la sécurité de l'information, et notre stratégie en la matière est fondée sur le principe de défense en profondeur. Nous accordons une très grande importance au maintien de la confidentialité des renseignements que nous fournissent nos clients et nos collègues, et nous continuons à investir massivement dans notre programme de sécurité de l'information et de confidentialité des données.

La présente vue d'ensemble s'adresse aux clients actuels et éventuels de Willis Towers Watson et de ses filiales. Elle présente un résumé des mesures de protection que nous avons mises en place et qui sont essentielles au maintien de notre réputation de conseiller de confiance.

Portée

Notre programme de sécurité de l'information est de portée générale, et il s'applique à l'ensemble de Willis Towers Watson dans le monde, y compris à ses filiales, à ses collègues, aux entrepreneurs et aux tiers fournisseurs qui peuvent traiter de l'information en son nom ou avoir accès de manière accessoire aux renseignements.

Code de conduite

Notre engagement à protéger la confidentialité des renseignements sur nos clients est une composante clé de notre code de conduite. En vertu de ce code, tous nos collègues doivent respecter la confidentialité des renseignements sur les activités, les employés et les clients de nos entreprises clientes. Ils doivent aussi respecter les lois en vigueur dans les pays et les régions où ils fournissent des services à nos clients et se conformer aux politiques en la matière en plus des exigences réglementaires qui les concernent. Tous les collègues doivent lire le code de conduite et fournir une attestation à cet égard lorsqu'ils se joignent à Willis Towers Watson ainsi que tous les ans par la suite, une fois qu'ils ont terminé la formation sur la protection des données et la confidentialité et sur la sécurité de l'information.

Fonction Sécurité

La sécurité est l'affaire de tous chez Willis Towers Watson : tous les collègues ont un rôle à jouer pour protéger l'information confiée à l'entreprise. À nos collègues s'ajoute une équipe composée de personnes compétentes dont les rôles et les responsabilités sont axés sur l'exécution de fonctions particulières dans le cadre de notre programme général de sécurité de l'information.

Notre chef de la sécurité de l'information est à la tête de la fonction Sécurité, et il est responsable d'établir la stratégie de l'entreprise et de mettre en œuvre notre programme mondial de sécurité de l'information. Le comité responsable de la sécurité de l'information et de la confidentialité des données assure une supervision additionnelle de nos politiques et de nos programmes en la matière, tandis que notre conseil d'administration est responsable de l'orientation globale de Willis Towers Watson en matière de sécurité.

Une fois l'an, le comité passe en revue et approuve nos politiques en matière de sécurité de l'information et de confidentialité des données. Ces politiques servent à définir les normes de contrôle pertinentes dans l'ensemble de l'entreprise.

Programme de gestion de la sécurité de l'information (PGSI)

Willis Towers Watson dispose d'un programme de gestion de la sécurité de l'information bien défini : fondé sur le risque, il est conforme à la norme ISO 27001:2013. Ce programme a pour but de protéger l'information conformément aux principes de sécurité suivants :

Confidentialité : Protéger l'actif informationnel contre toute divulgation et tout accès non autorisés.

Intégrité : Protéger l'actif informationnel contre toute modification non autorisée, pour assurer l'exactitude et l'intégralité de l'information et des méthodes de traitement.

Disponibilité : S'assurer que l'actif informationnel est seulement utilisé par des personnes autorisées ou dans le cadre de processus autorisés, au besoin.

Notre programme de gestion de la sécurité de l'information et les politiques, les lignes directrices et les procédures connexes sont conçus pour aider nos collègues à offrir constamment des services de première qualité à l'interne comme à nos clients, tout en garantissant un niveau de sécurité adéquat. Le programme général de sécurité de l'information de Willis Towers Watson fait l'objet d'évaluations dans le cadre du processus d'audit interne et externe en vue de l'obtention et du maintien du certificat ISO/IEC 27001:2013. Nous faisons l'objet de multiples audits tout au long de l'année, lesquels attestent de la rigueur de notre situation en matière de sécurité de l'information.

Programme de confidentialité des données

Les principes en matière de confidentialité des données auxquels nous adhérons tiennent compte des lois sur la confidentialité et la protection des données qui s'appliquent à nos activités. Ces principes touchent entre autres les éléments suivants :

Avis et autorisation :	Expliquer à chaque client les types de renseignements personnels dont nous avons besoin pour notre travail et obtenir du client l'autorisation de procéder.
Pertinence :	Limiter la collecte des renseignements personnels au minimum requis pour notre travail et les utiliser aux seules fins autorisées par le client.
Transparence et restriction d'utilisation :	Fournir les avis qui s'imposent au sujet des renseignements recueillis et des fins auxquelles ces renseignements vont servir.
Sécurité :	Maintenir des mesures de sécurité adéquates pour protéger les renseignements personnels contre toute perte accidentelle ou tout accès, toute utilisation ou toute divulgation non autorisés.
Accès :	Nous faisons en sorte que seules les personnes et les entités autorisées aient accès aux renseignements.
Transfert sécuritaire :	Exiger des filiales ou des sous-traitants à qui nous transmettons des renseignements personnels qu'ils les protègent de façon appropriée, et obtenir l'autorisation de partager ces renseignements, au besoin.
Conformité réglementaire :	Le bureau mondial responsable de la protection de la vie privée travaille avec nos équipes responsables de la conformité afin de s'assurer que celles-ci sont au fait des changements législatifs et de toutes les exigences futures, et qu'elles se conforment à celles applicables à Willis Towers Watson.

Rôles et responsabilités

Tous les collègues de Willis Towers Watson ont un rôle actif à jouer pour veiller à la sécurité de l'information conformément à ses politiques et à toute autre directive pouvant être publiée dans l'avenir.

Chez Willis Towers Watson, la sécurité de l'information s'appuie sur les principes « savoir, protéger et signaler ».

Savoir – les exigences et les comportements en matière de sécurité de l'information de cybersécurité que les collègues de Willis Towers Watson doivent respecter, en lisant la présente politique et en suivant la formation obligatoire à ce sujet.

Protéger – les renseignements de Willis Towers Watson et ceux de nos clients, de vos collègues et les vôtres en adhérant aux exigences et en adoptant les comportements souhaités.

Signaler – tout incident mettant en jeu la sécurité de l'information et la cybersécurité ainsi que toute activité suspecte en suivant le processus de réaction aux incidents visant la cybersécurité de Willis Towers Watson.

Annexe

La présente annexe renferme des renseignements supplémentaires sur les programmes de sécurité de l'information et de confidentialité des données mis en œuvre par Willis Towers Watson. Elle présente certains contrôles qui ont été mis en place relativement à des enjeux intéressant les responsables de la sécurité et de la confidentialité chez nos clients.

Fonctions de soutien externalisées

Willis Towers Watson fait appel à divers fournisseurs de services TI pour gérer et soutenir certains secteurs de son environnement TI. Nous exigeons de ces fournisseurs qu'ils se conforment à nos normes et à nos politiques en matière de sécurité ainsi qu'aux meilleures pratiques de leur secteur. Notre fonction Sécurité évalue les risques pour la sécurité que représente chacun des fournisseurs externes de services TI.

Willis Towers Watson assure la surveillance des relations avec les fonctions de soutien TI externalisées. Notre programme de surveillance est conçu pour veiller à ce que ces fournisseurs exercent leurs activités conformément aux engagements contractuels convenus avec Willis Towers Watson sur le plan des opérations, de la sécurité et des affaires. Les mesures de surveillance peuvent entre autres comprendre ce qui suit : examen des rapports d'audits externes, examens sur place des installations et des processus du fournisseur, examens périodiques des paramètres d'exploitation et des fiches de rendement, audits internes et participation aux processus de gestion des changements et des problèmes.

Intervention en cas d'incident de cybersécurité

Le service d'intervention en cas d'incident relatif à la cybersécurité est constitué du centre mondial de sécurité opérationnelle (GSOC), de l'équipe mondiale d'intervention en cas d'incident majeur (GMIRT), de l'équipe mondiale responsable du traitement des incidents liés à la sécurité de l'information et à la cybersécurité (GIIHT), de l'équipe responsable du traitement des cybermenaces (CTI) et de l'équipe chargée de la cybersécurité des plateformes (CPST) où des analystes et des spécialistes font le tri des incidents de sécurité, mènent des enquêtes et traitent ces incidents. Ce service repose sur une plateforme de gestion des incidents de sécurité permettant de faire des analyses poussées des activités afin de détecter et de prévenir les attaques et les infiltrations, et d'y réagir. Cette plateforme fait l'objet d'une surveillance permanente, 24 heures sur 24, 7 jours sur 7, par l'équipe du centre mondial de sécurité opérationnelle (GSOC), laquelle possède une expertise en matière d'enquêtes techniques, ainsi que par l'équipe mondiale d'intervention en cas d'incident majeur (GMIRT), spécialisée en criminalistique numérique.

Willis Towers Watson (WTW) s'est dotée d'un plan mondial d'intervention en cas d'incident de cybersécurité, afin d'identifier et de gérer les cybermenaces ainsi que les incidents touchant la sécurité des données, notamment ceux susceptibles de nuire à la sécurité de l'information et à la confidentialité des données, à l'échelle mondiale. Ce plan définit les rôles et les responsabilités des parties prenantes de WTW chargées de traiter les incidents liés à la cybersécurité et à la sécurité des données, d'établir le degré de gravité des incidents et leurs catégories de menace, et il décrit le processus de gestion des incidents, y compris les procédures de recours à un palier hiérarchique supérieur et de communication. Le plan mondial d'intervention en cas d'incident de cybersécurité est revu et mis à l'essai tous les ans. Suivant ce plan, chaque incident doit être consigné, les personnes intéressées doivent être avisées, une enquête doit être menée et les mesures requises doivent être prises.

Les incidents sont gérés quotidiennement grâce aux conseils des intervenants de WTW comme les équipes des services d'intervention en cas d'incident relatif à la cybersécurité, et en collaboration avec les équipes du Service de la conformité et du Service juridique du bureau mondial responsable de la protection de la vie privée (Bureau de l'avocat-conseil et responsable de la protection de la vie privée), pour répondre aux préoccupations immédiates et établir les schémas habituels, les tendances et les éléments qui peuvent être améliorés. Les mesures prises dans le cadre du processus ci-dessus dépendent d'un nombre de situations sous-jacentes, comme la nature et la gravité d'un incident. Voici une illustration du processus typique d'un incident de sécurité concernant une divulgation de données non autorisée :

- **Signalement** : Les employés de WTW doivent signaler les incidents de sécurité visant des données dont ils sont témoins, notamment la divulgation de données non autorisée, au moyen des portails de signalement prévus qui dirigent les rapports à l'équipe du centre mondial de sécurité opérationnelle (GSOC) aux fins d'évaluation.

- **Triage** : L'évaluation du GSOC des incidents de sécurité signalés visant des données comprend le triage et le classement par catégories selon la nature et la gravité des incidents. Le GSOC fait appel aux intervenants de WTW concernés et aux autres équipes de protection de la cybersécurité, p. ex., l'équipe mondiale d'intervention en cas d'incident majeur (GMIRT), l'équipe responsable du traitement des cybermenaces (CTI) et l'équipe chargée de la protection de la vie privée, selon le cas.

- **Examen juridique** : Les incidents justifiant la mobilisation du Bureau de l'avocat-conseil et responsable de la protection de la vie privée comprennent ceux liés aux divulgations de données non autorisées. Le GSOC fait appel à l'équipe de la protection de la vie privée de la région dans laquelle survient l'incident et lui envoie les renseignements relatifs à l'incident, y compris les documents pertinents, p. ex., les contrats. L'équipe de la protection de la vie privée vérifie l'information au sujet de l'incident et donne des conseils. Elle apporte également son aide dans le cadre des mesures requises, y compris les obligations juridiques liées aux atteintes à la protection des données, p. ex., atténuation, correction, déclaration réglementaire, signalement aux agents d'application de la loi, notification aux personnes concernées ou au propriétaire des données, notifications contractuelles aux clients, etc. L'équipe de la protection de la vie privée communique également avec les organismes de réglementation au sujet des incidents à signaler, conformément aux exigences des lois locales applicables.

- **Atténuation** : Le GSOC coordonne les efforts avec les intervenants de WTW et les groupes de résolution, p. ex., les responsables d'unité fonctionnelle, l'équipe de la protection de la vie privée, pour envisager les moyens d'atténuer les effets d'un incident, comme ceux que peut provoquer une divulgation de données non autorisée. Par exemple, si les données ont été transmises à un destinataire non autorisé connu, WTW cherche alors la confirmation que les données ne sont pas utilisées à des fins abusives, p. ex., le destinataire a supprimé les données, ne les a pas diffusées, n'a pas conservé de copies des données.

- **Correction à plus long terme :** Une fois les mesures prioritaires prises, des mesures de correction à plus long terme peuvent être envisagées, en fonction de la cause fondamentale de l'incident, p. ex., examens et améliorations du processus, formation supplémentaire pour les personnes responsables de l'incident.

Programme de gestion des documents

Willis Towers Watson a la responsabilité de conserver des documents partout dans le monde et elle s'est dotée pour cette raison d'un programme mondial de gestion des documents qui

chapeaute l'établissement de politiques et de normes adéquates.

Ce programme est guidé par les principes suivants :

- Conserver tous les documents commerciaux susceptibles d'influer nettement sur les obligations de la société, et ce, sans dépasser la durée nécessaire pour se conformer aux exigences juridiques, réglementaires et commerciales; les documents en question sont ainsi disponibles lorsqu'on en a besoin.
- Détruire les documents à la fin de leur période de conservation normale, sauf si ces documents ont été mis en suspens pour des raisons juridiques.
- Identifier et protéger les documents essentiels et incorporer les procédures pertinentes dans tout plan de reprise après sinistre.
- Assurer la protection de tous les documents, y compris ceux contenant des données confidentielles devant être protégées.

À propos de Willis Towers Watson

Willis Towers Watson (NASDAQ : WLTW) est une société mondiale de premier plan en services-conseils, en courtage et en solutions qui aide ses clients partout dans le monde à transformer le risque en parcours de croissance. Nos racines remontent à 1828, et Willis Towers Watson compte 45 000 employés dans plus de 140 pays et marchés.

Nous concevons et réalisons des solutions qui permettent de gérer le risque, d'optimiser les avantages sociaux, de cultiver les talents et d'augmenter la capacité des capitaux afin de protéger les organisations et les personnes et de les rendre plus solides. Notre vision unique nous permet de reconnaître ce qui se trouve aux carrefours stratégiques entre les talents, les actifs et les idées, la formule dynamique qui favorise les résultats d'entreprise.

Ensemble, réalisons votre potentiel.

Consultez notre site à l'adresse www.willistowerswatson.com.