Programme de sécurité des services infonuagiques

Compte tenu de la technologie moderne, des coûts d'implantation et de la nature, de l'étendue, du contexte et des motifs du traitement des données des clients, de même que du risque de probabilité variable et de l'importance des droits et libertés des personnes physiques, ComputerTalk a implanté les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité adapté au risque.
ComputerTalk utilise des mesures techniques, organisationnelles et de sécurité raisonnables conçues pour protéger les données personnelles des clients en possession de ou autrement traitées par ComputerTalk contre l'accès, l'altération, la divulgation ou la destruction non autorisés.

ComputerTalk a implanté et maintiendra un programme de sécurité de l'information qui respecte les principes de sécurité de système généralement acceptés inclus dans les normes PCI DSS et SOC 2 conçus pour protéger les données du client adaptés à la nature et à la portée des services infonuagiques que fournit ComputerTalk.

Structure Générale de la sécurité des données

a) Sensibilisation et formation sur la sécurité. ComputerTalk a développé et maintiendra un programme de sécurité de l'information et de sensibilisation offert à tous les employés au moment de l'embauche et annuellement par la suite. Le programme de sensibilisation est livré de manière électronique et inclut un test et des exigences minimales pour le réussir.

b) Politiques et procédures. ComputerTalk maintiendra des politiques et des procédures appropriées afin d'appuyer le programme de sécurité de l'information. Les politiques et les procédures seront revues chaque année et mises à jour au besoin.

c) Gestion des modifications. ComputerTalk utilisera un processus de gestion des modifications fondé sur les normes de l'industrie pour assurer que toutes les modifications à l'environnement du Client soient revues, testées et approuvées de manière appropriée.

d) Stockage des données et copie de sauvegarde. ComputerTalk créera des copies de sauvegarde des données critiques du Client selon des procédures de sauvegarde documentées. Les données de sauvegarde ne seront pas emmagasinées dans un média portable. Les données de Client stockées sur un média de sauvegarde seront protégées d'un accès non autorisé. Les données de sauvegarde pour les serveurs de production essentiels qui ne sont pas des bases de données seront conservées approximativement trente (30) jours. Les données de sauvegarde pour les serveurs de base de données essentiels et les données ponctuelles seront conservées durant un minimum de sept (7) jours.

e) Protection anti-virus et anti logiciel malveillant. ComputerTalk utilisera des solutions de protection antivirus et anti logiciel malveillant qui respectent les normes de l'industrie pour assurer que tous les serveurs dans l'environnement de service infonuagique de ComputerTalk soient protégés de manière appropriée contre les logiciels malveillants

comme des chevaux de Troie, des virus et des vers. ComputerTalk utilisera des pratiques conformes aux normes de l'industrie pour assurer que les services infonuagiques de ComputerTalk livrés aux Clients ne contiennent pas de programme, routine, sous-routine ou données (incluant des logiciels malveillants ou 'maliciel', des virus, des vers et des chevaux de Troie) qui sont conçus pour perturber l'exploitation appropriée des services ou qui, à la suite d'un certain événement, du passage du temps ou la prise d'action ou le défaut de prendre action, détruira, endommagera ou rendra inutilisables les données ou les services du Client. Les Clients reconnaissent que l'utilisation de clés de licence ne contreviendra pas à cette section.

f) Gestion de la vulnérabilité et des correctifs. ComputerTalk maintiendra un programme de gestion de la vulnérabilité fondé sur des pratiques conformes aux normes de l'industrie qui évaluent automatiquement l'environnement de services infonuagiques. Des balayages systématiques du réseau et des serveurs seront planifiés et complétés au moins une fois par trimestre. Les résultats du balayage, seront analysés pour confirmer les vulnérabilités identifiées et la correction sera programmée dans un délai qui tient compte du niveau relatif du risque. ComputerTalk surveillera divers services consultatifs de vulnérabilité pour s'assurer que les vulnérabilités identifiées récemment soient évaluées de manière appropriée pour déterminer un possible impact sur les Services. Les vulnérabilités critiques ou à risque élevé seront abordées promptement au moyen de processus de gestion des correctifs et de gestion des modifications.

g) Tests d'intrusion. ComputerTalk effectuera des tests d'intrusion internes, externes, d'application web et de segmentation sur les ressources d'information et l'infrastructure TI au moins une fois l'an et après toutes modifications significatives selon les normes applicables et les exigences réglementaires. Les risques et vulnérabilités de l'information identifiés seront traités de manière appropriée à l'aide de plans d'action de gestion du risque afin de remédier proactivement à cette menace.

h) Destruction des données. ComputerTalk suivra des processus conformes aux normes de l'industrie pour la destruction sécuritaire des données du Client qui deviennent obsolètes ou qui ne sont plus requises en vertu de l'entente. De l'équipement obsolète ou hors service qui contenait autrefois les données du Client et dont la destruction est prévue sera détruit de manière sécuritaire par un fournisseur de service qualifié qui procure un certificat de destruction sécuritaire.

Sécurité du réseau

ComputerTalk utilisera des contrôles de sécurité efficaces fondés sur les normes de l'industrie pour assurer que les données du Client soient segmentées et isolées des autres environnements de clients à l'intérieur de l'environnement des services infonuagiques. Ces contrôles incluent, sans être limités à:

a) Services des pare-feu séparés. Les environnements de Client sont séparés au moyen d'instances de pare-feu physiques et contextuelles. ComputerTalk emploie une technologie de pare-feu avancée avec détection active de menaces pour réduire

l'éventualité d'une menace à la sécurité qui aurait un effet sur l'environnement des services infonuagiques.

b) Système de détection d'intrusion. ComputerTalk a implanté des systèmes de détection de l'intrusion à travers l'environnement de service infonuagique de ComputerTalk.

c) Aucun réseau sans fil. Les réseaux sans fil ne sont pas utilisés dans l'environnement des services infonuagiques.

d) Chaîne de connexion entre le Client et l'environnement de service infonuagique de ComputerTalk. ComputerTalk utilise des circuits SSL/TLS, VPN, et/ou MPLS pour sécuriser les connexions entre les navigateurs, les applis clients et les applis mobiles et le service infonuagique de ComputerTalk. Les connexions qui empruntent un réseau non sécurisé (par. ex. l'Internet) utiliseront SSL/TLS.

e) Chaîne de connexion entre le service infonuagique de ComputerTalk et des tierces parties. La transmission ou l'échange des données du Client avec le Client ou toute tierce partie autorisée par le Client à recevoir les données du Client sera effectuée au moyen de méthodes sécuritaires (par ex., SSL/TLS, HTTPS, SFTP).

f) Enregistrements chiffrés. ComputerTalk chiffre les enregistrements d'appels et les sessions de clavardage. Le Client est responsable de conserver les données sensibles à l'extérieur des enregistrements effectués au moyen de la barre d'outils de l'agent (iceBar), comme l'utilisation d'une fonction de pause.

g) Protection par chiffrement. ComputerTalk utilise des méthodes conformes aux normes de l'industrie pour gérer le chiffrement.

h) Journalisation et surveillance. ComputerTalk journalisera les événements de sécurité du point de vue opérationnel pour tous les serveurs qui fournissent le service infonuagique de ComputerTalk aux Clients. ComputerTalk surveillera et investiguera tout événement qui pourrait laisser croire à un incident ou un enjeu de sécurité. Les enregistrements d'événements sont conservés durant un an.

Contrôle d'accès utilisateur

i) Contrôle d'accès. ComputerTalk implantera les contrôles d'accès appropriés pour s'assurer que seuls les utilisateurs autorisés ont accès aux données du Client dans l'environnement de service infonuagique de ComputerTalk.

Accès des utilisateurs du Client. Le Client est responsable de la gestion de l'accès des utilisateurs à l'application. Le Client définit les noms d'utilisateur, les rôles et les caractéristiques des mots de passe (longueur, complexité et délai d'expiration) pour ses utilisateurs. Le Client est entièrement responsable de toute défaillance causée par lui-même, ses agents, ses contracteurs ou ses employés (incluant sans limitation tous ses utilisateurs), de maintenir la sécurité de tous les noms d'utilisateurs, mots de passe et autre information sur le compte sous son contrôle. Sauf dans le cas d'un manquement à la sécurité causé par une négligence grave ou une action ou une inaction volontaire de la part de ComputerTalk, le Client est entièrement responsable de toute utilisation du

service infonuagique de ComputerTalk par ses noms d'utilisateurs et mots de passe, peu importe si elle est autorisée par le Client, et de tous les frais résultants d'une telle utilisation. Le Client avisera immédiatement ComputerTalk s'il se rend compte de toute utilisation non autorisée du service infonuagique de ComputerTalk.

j) Accès des utilisateurs de ComputerTalk. ComputerTalk créera des comptes d'utilisateur individuels pour chacun des employés qui ont un besoin fonctionnel d'accéder aux données du Client ou aux systèmes du Client à l'intérieur de l'environnement de service infonuagique de ComputerTalk. Les principes directeurs suivants en lien avec la gestion de compte d'utilisateurs seront suivies par ComputerTalk:

- Les comptes d'utilisateur sont demandés et autorisés par le personnel de gestion de ComputerTalk.
- Des contrôles fermes de mots de passe sont systématiquement appliqués.
- Les connexions doivent être établies au moyen d'une technologie d'accès à distance sécuritaire conforme aux normes de l'industrie qui utilise des mots de passe forts qui expirent tous les quatre-vingt-dix (90) jours.
- Les comptes dormants ou inutilisés sont désactivés après quatre-vingt-dix (90) jours de non-usage.
- Des temporisateurs de session sont systématiquement appliqués.
- Les comptes d'utilisateur sont rapidement désactivés lors de la cessation d'emploi ou du transfert de rôle d'un employé qui élimine le besoin fonctionnel d'accès.

Continuité des activités ou reprise après catastrophe

Protection contre les interruptions. Le service infonuagique de ComputerTalk sera déployé et configuré selon une conception de haute disponibilité. L'environnement de services infonuagiques est physiquement et logiquement séparé de l'environnement de réseau d'entreprise de ComputerTalk. Un événement d'interruption qui implique l'environnement d'entreprise n'a pas d'effet sur la disponibilité du service infonuagique de ComputerTalk.

Continuité des activités. ComputerTalk maintient un processus de Gestion de la continuité des activités (GCA) qui identifie les risques, les menaces et les vulnérabilités potentiels qui pourraient avoir un effet sur les opérations d'affaires de
ComputerTalk. L'objectif général est de s'assurer que l'entreprise soit plus souple face à de potentielles menaces et que l'entreprise puisse reprendre ou continuer son exploitation dans des conditions défavorables ou anormales.

Reprise après catastrophe. ComputerTalk offre différentes options de reprise après catastrophe pour satisfaire aux exigences des clients. En général, la plupart des clients choisissent de fonctionner à partir de l'architecture à haute disponibilité d'un seul centre de données. Des copies de sauvegarde chiffrées hors site permettent un retour en service rapide dans les mêmes lieux ou dans un autre centre de données de ComputerTalk. Les solutions de clients qui ne peuvent tolérer le moindre temps d'arrêt sont hébergées dans divers centres de données physiques et sont conçus pour fonctionner sur un seul.

Réponse aux incidents de sécurité

Programme de réponse aux incidents de sécurité. ComputerTalk maintiendra un programme de réponse aux incidents de sécurité conforme aux normes de l'industrie conçu pour identifier et répondre à des incidents de sécurité présumés ou actuels qui impliquent les données du Client. Le programme sera actualisé, testé et, au besoin, mis à jour au minimum un fois l'an. "Incident de sécurité" signifie un événement confirmé qui résulte de l'utilisation, la suppression, l'altération, la divulgation ou l'accès non autorisé aux données du Client.

Notification. Advenant une brèche confirmée qui implique la publication ou la divulgation non autorisée de données du Client ou tout autre événement de sécurité qui requière une notification en vertu d'une loi applicable, ComputerTalk avisera le Client dans un délai de 72 heures et coopérera de manière raisonnable afin que le Client puisse procéder aux notifications requises en lien avec un tel événement à moins qu'une loi ou à un ordre de la cour n'empêche spécifiquement ComputerTalk de le faire.

Détails de la notification. ComputerTalk fournira au Client les détails suivants au sujet de l'incident de sécurité confirmé: (i) la date à laquelle l'incident de sécurité a été identifié et confirmé; (ii) la nature et l'impact de l'incident de sécurité; (iii) les actions déjà entreprises par ComputerTalk; (iv) les mesures correctives qui doivent être prises; et (v) l'évaluation des alternatives et des prochaines étapes.

Communications continues. ComputerTalk continuera de fournir des rapports de situation appropriés aux Clients concernant la résolution de l'incident de sécurité et travaillera assidûment de bonne foi pour corriger l'incident de sécurité et pour prévenir de tels incidents de sécurité dans le futur. ComputerTalk coopérera, à la demande raisonnable du Client, à l'investigation et à la résolution de l'incident de sécurité.

Protection de l'environnement des services infonuagiques

Utilisation de fournisseurs de centres de données en colocation. ComputerTalk engage des fournisseurs de services tiers pour l'espace en colocation. Les fournisseurs de colocation et de services connexes font l'objet d'une revue annuelle pour s'assurer qu'ils continuent de satisfaire aux besoins de ComputerTalk et de ses Clients. Chaque fournisseur de colocation maintient une certification fondée sur son modèle d'entreprise indépendante. Sur demande écrite, des certifications de sécurité et de conformité et ou des rapports d'attestation pour la colocation pertinents aux services du Client seront fournis. Ils peuvent requérir la signature d'ententes de non-divulgation additionnels.

Sécurité physique. Chaque environnement de services infonuagiques est logé dans une installation sécuritaire et renforcée au moyen des exigences de sécurité physique minimales suivantes: (a) points d'entrée sécuritaires et surveillés; (b) présence de caméras de surveillance dans l'installation; (c) validation de l'accès sur les lieux avec vérification de l'identité; (d) accès réservé aux personnes qui font partie de la liste d'accès approuvée par ComputerTalk; (e) présence sur les lieux d'employés du centre d'exploitation du réseau 24 heures par jour, 7 jours par semaine et 365 jours par année.

Contrôles environnementaux. Chaque environnement de services infonuagiques est équipé pour fournir des sources d'énergie électrique externes redondantes, des blocs d'alimentation

redondants, un groupe électrogène de secours et des contrôles de température et d'humidité redondants.