Mesures de sécurité entourant une interconnexion

Aux fins de l'exécution du présent contrat, il est nécessaire de mettre en place une interconnexion entre l'environnement informatique du CLIENT et celui du CONSULTANT.

Le CLIENT autorise l'interconnexion entre l'environnement informatique du CONSULTANT et son réseau interne, sous réserve du respect par le CONSULTANT des règles de sécurité des TI du CLIENT suivantes.

1. Rôle et responsabilité

   1.1 Le CONSULTANT met en place les mesures technologiques, physiques et administratives nécessaires pour assurer la confidentialité, l'intégrité et la disponibilité des informations du CLIENT qui transitent sur son infrastructure.
   1.2 Le CONSULTANT s'engage à respecter les lois applicables en matière de propriété intellectuelle et de protection des droits d'auteur et à ne pas copier les logiciels du CLIENT que ce soit pour en faire le commerce ou pour un usage personnel.
   1.3 Le CONSULTANT nomme un coordonnateur de la sécurité responsable du respect de la présente entente et de la mise en place de l'ensemble des mesures reliées à la sécurité.

2. Contrôle des accès

   2.1 Le CONSULTANT maintien, et met à jour mensuellement, une liste des individus autorisés à utiliser les services rendus disponibles par l'interconnexion et les privilèges autorisés, laquelle est remise au CLIENT.
   2.2 Les droits d'accès de chacune des ressources du CONSULTANT sont limités en fonction du besoin de savoir ou de faire tout en tenant compte du risque et seront accordés suite à une demande écrite approuvée par le gestionnaire en autorité chez le CLIENT.
   2.3 Le coordonnateur de sécurité du CONSULTANT avise immédiatement le gestionnaire de l'unité concerné du CLIENT lors de la cessation de l'assignation d'une ressource ou de l'ajout d'une nouvelle ressource à la réalisation du contrat.
   2.4 Lorsque l'interconnexion est établie par un réseau public, l'accès aux ressources TI du CLIENT par une ressource du CONSULTANT via cette interconnexion doit être géré par un mécanisme d'authentification faisant appel à deux facteurs*.
      * On définit "facteur" comme étant un mécanisme d'authentification basé sur quelque chose que l'on connaît et sur quelque chose que l'on possède, ou sur quelque chose qui caractérise l'individu (élément biométrique).
   2.5 La ressource du CONSULTANT ne peut pas, à sa connaissance et sans une autorisation expresse écrite du client, avoir simultanément accès en écriture dans les environnements de développement et de production du CLIENT.
   2.6 La ressource du CONSULTANT ne doit pas effectuer des tentatives délibérées de contourner une mesure de protection existante.

3. Sécurité de l'environnement et du réseau

   3.1 Les postes de travail de chacune des ressources du CONSULTANT qui accèdent aux ressources TI du CLIENT doivent être installés selon une configuration tenue à jour qui permet de détecter et de prévenir l'exécution de logiciels malveillants et qui empêche l'accès au poste de la ressource après un délai d'inactivité.
   3.2 Toute communication entre le réseau de télécommunication du CLIENT et le réseau de télécommunications du CONSULTANT doit traverser un point de contrôle de sécurité d'entreprise.
   3.3 Les points de contrôle de sécurité protégeant l'interconnexion par un réseau public doivent être configurés de façon à ce qu'ils ne permettent que les communications provenant des utilisateurs du CONSULTANT dûment autorisés.
   3.4 L'interconnexion doit être configurée de manière à s'assurer que seule une ressource du CONSULTANT puisse accéder au réseau interne du CLIENT.
   3.5 L'information confidentielle doit être chiffrée lorsque la mise en place d'un contrôle d'accès et de journaux rigoureux ne peut pas préserver la confidentialité de l'information.
   3.6 Lorsqu'il y a un risque d'interception, les communications d'information confidentielle qui s'effectuent entre l'infrastructure du CLIENT et celle du CONSULTANT doivent être chiffrées de bout en bout avec une technique de chiffrement robuste.**
      ** Un "chiffrement robuste" est un chiffrement basé sur un algorithme éprouvé et accepté par l'industrie, ainsi que sur une longueur de clé et une pratique appropriée de gestion des clés.

4. Gestion des incidents

   Le CONSULTANT ou sa ressource doit aviser immédiatement l'unité de support TI du CLIENT de tout soupçon d'intrusion, intrusion ou tentative d'intrusion, tout virus, tout acte qui pourrait affecter les systèmes d'information ou tout autre incident de sécurité des TI et permettre au responsable de la sécurité du CLIENT d'effectuer toute vérification nécessaire afin d'enquêter sur cet incident.

5. Gestion des changements

   Avant de procéder à un changement de processus, de technologie ou d'environnement susceptible d'altérer la sécurité de l'environnement du CLIENT, le CONSULTANT informe le CLIENT du changement proposé pour discuter des compatibilités, faisabilité et impacts sur les systèmes en place et obtenir son autorisation.

6. Approbation de la configuration

   Le CONSULTANT doit démontrer à un spécialiste de sécurité des TI reconnu du CLIENT que la configuration de l'interconnexion est conforme aux exigences de sécurité établies par la présente entente. Si l'interconnexion n'est pas conforme aux exigences décrites à la présente ou si son installation n'est pas passée formellement par ce processus d'approbation, elle doit être désactivée.

7. Surveillance et audit

7.1 Le CONSULTANT reconnaît que le CLIENT ou un tiers désigné par lui peut, suite à un avis écrit du CLIENT, procéder à une vérification du respect de la présente entente et, à cette fin, le CLIENT aura accès aux locaux du CONSULTANT ainsi qu'aux dossiers contenant les renseignements fournis par le CLIENT ou recueillis par les ressources du CONSULTANT dans le cadre de l'exécution du présent contrat, y compris, s'il y a lieu, les accès aux bases de données contenant les renseignements.

7.2 Le CONSULTANT reconnaît également que le CLIENT peut procéder aux vérifications nécessaires en vue de s'assurer de la protection de ses actifs informationnels, incluant notamment la surveillance du trafic et des transactions sur le réseau du CLIENT.

8 Non-respect et terminaison de l'entente

8.1 L'accès ne sera pas donné aux ressources du CONSULTANT tant que l'entente contractuelle et les contrôles supportant l'interconnexion ne seront pas complétés.

8.2 Le CONSULTANT reconnaît que le défaut de respecter les exigences de sécurité applicables du CLIENT constituera une violation de ses obligations contractuelles qui peut causer au CLIENT un préjudice sérieux ou irréparable. Par conséquent, le CONSULTANT reconnaît que le CLIENT pourra avoir notamment un recours immédiat à l'injonction et ce, sous réserve de tous ses autres recours.

8.3 Cette autorisation est accordée exceptionnellement et temporairement. Le CLIENT peut y mettre fin sans préavis.

8.4 À l'expiration du contrat, ou en tout temps sur demande écrite du CLIENT, le CONSULTANT s'engage à lui retourner tous les renseignements que ce dernier lui a fournis ou qu'il a recueillis. Le CONSULTANT s'engage également à détruire toute copie de ces renseignements et à fournir au CLIENT un document établissant qu'aucune copie des renseignements n'a été conservée.

8.5 Si une ressource du CONSULTANT prend des copies des logiciels appartenant au CLIENT pour travailler sur ses propres équipements, le CONSULTANT s'engage à ce que ces copies et les données appartenant au CLIENT soient détruites de façon à ne plus être accessibles et intelligibles à la fin du contrat, ou en tout temps sur demande écrite du CLIENT, et à fournir à ce dernier un document établissant qu'aucune copie des logiciels contenant ces renseignements n'a été conservée.