Conditions de sécurité de l'information de CAE pour les fournisseurs

Les présentes conditions de sécurité de l'information de CAE pour les Fournisseurs (« **Conditions de sécurité** ») font partie des conditions générales du service des achats CAE (« **CG** ») qui font partie d'un contrat exécutoire (« **Contrat** ») entre CAE inc. ou l'entité affiliée à CAE inc. désignée dans le bon de commande (« **CAE** ») et le destinataire (« **Fournisseur** ») et s'appliquent à chaque bon de commande (« **Bon de commande** ») s'y référant qu'un représentant autorisé des achats ou de l'approvisionnement stratégique mondial (« **Représentant** ») de CAE peut émettre au Fournisseur. Chaque Bon de commande doit contenir une description des services (« **Services** »), des biens, des matériaux ou des articles (« **Biens** ») demandés par CAE.

Les obligations en vertu des Conditions de sécurité s'appliquent à tout moment où le Fournisseur, pendant l'exécution du Contrat, traite, stocke ou héberge des Renseignements confidentiels et à tous les emplacements à partir desquels le Fournisseur exploite son entreprise, qu'ils soient sous le contrôle direct du Fournisseur ou sous le contrôle du fournisseur de services tiers du Fournisseur.

a. Programme de sécurité de l'information

1) Le Fournisseur doit définir, mettre en œuvre et maintenir à jour un programme complet de sécurité de l'information qui se définit comme un ensemble de politiques, de normes, de procédures et de contrôles visant à protéger les exigences de confidentialité, d'intégrité et de disponibilité liées aux Renseignements confidentiels (telles que définies dans les CG) reçues pour ou pendant l'exécution du Contrat.
2) Le programme de sécurité du Fournisseur doit déterminer et attribuer les rôles et les responsabilités en matière de sécurité des informations. Il doit établir des mécanismes de coordination entre les entités organisationnelles et être approuvé par un cadre supérieur du Fournisseur responsable et imputable du risque lié à la sécurité de l'information. Le Fournisseur doit revoir son programme de sécurité au moins une fois par an et le mettre à jour pour refléter les changements organisationnels ou les problèmes repérés chaque année.
3) Dans le cadre de son programme de sécurité, le Fournisseur doit élaborer, communiquer et réviser périodiquement une politique d'audit et d'imputabilité qui aborde tous les éléments couverts par la portée de son programme de sécurité des informations.
4) Le Fournisseur doit fournir un avis écrit préalable à CAE dans le cas où le Fournisseur a l'intention de changer l'endroit où les renseignements confidentiels sont traités, stockés ou hébergés.
5) Sous réserve de l'avis donné par le Fournisseur à CAE conformément à la sous-section c.6), le Fournisseur doit aviser CAE dans les 48 heures de toute incapacité à respecter ses obligations énoncées dans les Conditions de sécurité.

b. Évaluation de la performance des contrôles de sécurité

1) Le Fournisseur doit, à la demande de CAE, accorder à CAE ou à un tiers mandaté par CAE, la permission de procéder à un examen, une évaluation ou un audit de la conformité du Fournisseur aux Conditions de sécurité. Le Fournisseur doit coopérer et donner accès à la documentation, aux locaux ou au personnel pertinents, comme le demande raisonnablement CAE ou le tiers mandaté par CAE, au cours de l'examen, de l'évaluation ou de l'audit. En outre, le Fournisseur doit fournir rapidement à CAE les résultats de toutes les évaluations effectuées par ou pour le Fournisseur concernant son programme de cybersécurité.
2) Le Fournisseur doit définir un plan d'évaluation et de test de sécurité qui définit la portée de l'évaluation de la mise en œuvre et de l'efficacité des contrôles de sécurité, des améliorations possibles de ces contrôles dans le cadre de l'organisation et de son environnement. Un rapport doit être produit à la suite de l'évaluation et une copie doit être fournie rapidement à CAE.
3) Le Fournisseur doit élaborer un plan d'action et des étapes pour remédier aux vulnérabilités et aux faiblesses constatées lors de l'évaluation. Le plan d'action et les étapes existantes doivent être mis à jour régulièrement en fonction des résultats des évaluations de la sécurité, de l'analyse de l'incidence sur les opérations et des activités de surveillance de la sécurité.
4) Le Fournisseur doit aviser CAE par écrit trente (30) jours avant d'effectuer tout changement dans le contenu de ses contrôles de sécurité et/ou de son programme de cybersécurité qui pourrait entraîner une réduction de la protection, de la sécurité et de la sauvegarde des Renseignements confidentiels de CAE.

c. Gestion des risques

1) Dès que possible, mais en tous les cas avant le début de l'exécution des Services ou de la livraison des Biens, le Fournisseur doit divulguer par écrit à CAE tout incident de sécurité, toute violation ou toute réclamation résultant d'un incident de sécurité de l'information survenu au cours des douze mois précédant la date du Bon de commande. Un incident lié à la sécurité de l'information comprend également les situations où le Fournisseur

soupçonne que les exigences de confidentialité, d'intégrité et de disponibilité associées au réseau ou aux systèmes du Fournisseur ont été violées.

2) Le Fournisseur doit élaborer et mettre en œuvre un programme d'intervention en cas d'incident informatique comprenant un ensemble de politiques, de processus, de flux de travail et de procédures qui traitent de l'objet, de la portée, de la coordination, des rôles et responsabilités et des capacités qui comprennent la préparation, la détection, l'analyse, le confinement, l'éradication et la récupération. Le programme doit inclure un plan d'intervention en cas d'incident informatique contenant une feuille de route pour la mise en œuvre de la capacité de réponse aux incidents, une description de la structure organisationnelle dédiée à la réponse aux incidents, une approche de haut niveau de la réponse aux incidents, une définition des incidents à signaler, des mesures d'évaluation des capacités de réponse aux incidents, et doit intégrer les leçons tirées des capacités de traitement des incidents précédents dans ses procédures, formations et tests de réponse aux incidents. Ces documents doivent être communiqués à tout le personnel impliqué dans le processus d'intervention en cas d'incidents informatiques, puis revus et mis à jour au moins une fois par an.

3) Le Fournisseur doit fournir une formation d'intervention en cas d'incident informatique à son personnel, conformément aux rôles et responsabilités qui lui sont attribués.

4) Le Fournisseur doit suivre et documenter les incidents de sécurité liés à l'information.

5) Le Fournisseur doit tester au moins une fois par an ses capacités de réponse aux incidents pour évaluer leur efficacité et documenter les résultats.

6) Le Fournisseur doit informer CAE dans les 24 heures d'un incident de sécurité ou d'atteinte à la sécurité susceptible de nuire à la sécurité des Renseignements confidentiels, comme décrit plus en détail à la section 22 des CG.

d. Continuité des opérations/Plan de secours informatique

1) Le Fournisseur doit déterminer, planifier, documenter, tester et mettre en œuvre des procédures de continuité des opérations et de reprise après sinistre informatique qui permettront une reprise rapide des fonctions et processus essentiels de l'entreprise en cas d'interruption.

e. Tiers

1) Sans limiter la généralité de la section 31 des CG, le Fournisseur ne peut pas sous-traiter à un tiers l'exécution de l'une de ses obligations, quelle qu'elle soit, en vertu des Conditions de sécurité sans le consentement écrit préalable de CAE.

2) Une fois qu'un tiers a été approuvé par CAE, le Fournisseur doit (i) exiger que ce fournisseur de services externes de systèmes d'information se conforme aux Conditions de sécurité en vigueur et aux lois et règlements applicables; et (ii) surveiller en permanence la conformité des contrôles de sécurité par ce fournisseur de services externes.

3) Le Fournisseur doit effectuer une évaluation organisationnelle avant d'externaliser tout service lié à la sécurité des informations et une copie doit être fournie rapidement à CAE.

f. Logiciels

1) Le Fournisseur convient que le logiciel qui traite, stocke ou héberge les Renseignements confidentiels de CAE (i) a été conçu et développé selon les meilleures pratiques de l'industrie, et (ii) ne contient aucune vulnérabilité non divulguée par écrit à CAE.

2) Le Fournisseur accepte de surveiller activement et périodiquement les vulnérabilités du logiciel qui traite, stocke ou héberge les Renseignements confidentiels de CAE et de remédier rapidement à ces vulnérabilités, en commençant par traiter les menaces les plus prioritaires aussi efficacement que possible.