CLAUSES CONTRACTUELLES RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DÉTENUS PAR LE RÉSEAU DE TRANSPORT MÉTROPOLITAIN (EXO)

Les *Clauses contractuelles relatives à la protection des renseignements personnels détenus par le Réseau de transport métropolitain* (« **Clauses** ») (« **EXO** ») sont conclues entre EXO et **[insérer le nom complet de la personne morale qui fournit les services]** (le « **Fournisseur de services** »). Ces Clauses s'appliquent à l'accès, la collecte, l'utilisation, la communication, la conservation, la destruction et à tout autre type de traitement (collectivement le « **traitement** ») de renseignements personnels par le Fournisseur de services pour le compte d'EXO (« **Renseignements personnels d'EXO** ») afin de fournir les services (« **Services** ») à EXO en vertu d'un contrat (« **Contrat de service** ») conclu entre les parties. L'Appendice 1 fournit des détails sur le traitement de Renseignements personnels d'EXO par le Fournisseur de services en vertu des présentes Clauses.

Les parties conviennent donc de ce qui suit :

1. **Conformité à la Loi sur l'accès**. EXO et le Fournisseur de services doivent se conformer aux exigences de protection des Renseignements personnels prévues dans la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (la « **Loi sur l'accès** »). Le Fournisseur de services doit également se conformer (i) aux politiques, aux directives et aux procédures d'EXO concernant la sécurité, l'utilisation et la communication des Renseignements personnels d'EXO qui peuvent être transférés, communiqués ou autrement mis à disposition du Fournisseur de services de temps en temps; et (ii) à toutes les normes de l'industrie applicables concernant la vie privée, la protection des données, la confidentialité ou la sécurité de l'information.

2. **Limitation de l'utilisation - Propriété**. Toute utilisation des Renseignements personnels d'EXO par le Fournisseur de services doit être limitée à ce qui est nécessaire pour la prestation des Services ou à toutes autres fins expressément autorisées par EXO. Les Renseignements personnels d'EXO sont et restent à tout moment la propriété exclusive d'EXO. Sans limiter la généralité de ce qui précède, le Fournisseur de services s'engage à ne pas tenter d'anonymiser, de dépersonnaliser ou d'agréger les Renseignements personnels d'EXO ou de supprimer ou modifier de toute autre manière les Renseignements personnels d'EXO afin qu'ils ne constituent plus ou n'incluent plus de renseignements permettant d'identifier un individu, sauf dans la mesure où cela est nécessaire pour fournir les Services à EXO ou à d'autres fins expressément autorisées par écrit par EXO et si cela est autorisé, uniquement dans la mesure où il est raisonnable de prévoir, dans les circonstances, que les Renseignements personnels d'EXO ne permettent plus, de façon irréversible, d'identifier directement ou indirectement un individu.

3. **Personnel autorisé**.

3.1. Accès restreint. Le Fournisseur de services limite et n'autorise l'accès aux Renseignements personnels d'EXO qu'aux seules personnes qui en ont besoin pour mener à bien les tâches qui leur sont assignées dans le cadre de la mise en œuvre des Services (« **Personnel autorisé** »), étant entendu que l'accès aux Renseignements personnels d'EXO qui ne sont pas nécessaires à la réalisation d'une tâche assignée dans le cadre de la mise en œuvre des Services est interdit.

3.2. Mesures de protection. Le Fournisseur de services traite les Renseignements personnels d'EXO de manière strictement confidentielle et veille à s'assurer que le Personnel autorisé :

a) soit soumis à des procédures d'authentification d'utilisateur et de connexion pour accéder aux Renseignements personnels d'EXO;
b) soit informé du caractère confidentiel des Renseignements personnels d'EXO;
c) connaît les dispositions des présentes Clauses ainsi que son application à l'exécution des Services;
d) signe un engagement de confidentialité (voir Appendice 3) contenant des clauses de confidentialité qui sont sensiblement similaires à celles énoncées dans les présentes Clauses;
e) prend des mesures raisonnables, telles qu'offrir des formations et appliquer des sanctions appropriées, afin d'assurer le respect par le Personnel autorisé des présentes Clauses; et
f) se conforme aux exigences des présentes Clauses.

4. **Sous-traitants**. EXO autorise le Fournisseur de services à désigner des sous-traitants pour traiter les Renseignements personnels d'EXO pour son compte. La liste de sous-traitants (y compris des tiers et des affiliés du Fournisseur de services) autorisés par EXO est incluse dans l'Appendice 1. Le Fournisseur de services doit obtenir l'approbation d'EXO avant de désigner un nouveau sous-traitant et il doit indiquer à EXO les détails du traitement de Renseignements personnels d'EXO qui sera effectué par le sous-traitant. Le Fournisseur de services doit s'assurer que toute entente avec un sous-traitant est régie par un contrat écrit qui offre aux Renseignements personnels d'EXO un niveau de protection comparable à celui établi dans les présentes Clauses. Le Fournisseur de services est solidairement responsable de toutes les actions et omissions de ses sous-traitants.

5. **Transferts à l'extérieur du Québec**. Le Fournisseur de services ne peut traiter, et doit s'assurer que tout sous-traitant ne traite, les Renseignements personnels d'EXO qu'au sein des frontières du Québec, à moins d'avoir une autorisation écrite d'EXO. Le Fournisseur de services s'engage à coopérer pleinement et rapidement avec EXO dans la réalisation d'une évaluation des risques liés au transfert, ou toute évaluation similaire ou réévaluation périodique qu'EXO considère comme étant requise en vertu de la Loi sur l'accès, en ce qui concerne tout traitement des Renseignements personnels d'EXO à l'extérieur du Québec par le Fournisseur de services ou le sous-traitant. Le Fournisseur de services accepte, et doit faire en sorte que tout sous-traitant accepte, d'apporter toute modification aux présentes Clauses, ou à toute entente similaire entre le Fournisseur de services et son sous-traitant, qu'EXO considère comme nécessaire à la suite d'une telle évaluation ou réévaluation pour permettre à tout traitement des Renseignements personnels d'EXO en dehors du Québec d'être effectué (ou de continuer à être effectué), à tout moment, en conformité avec la Loi sur l'accès.

6. **Demandes des personnes concernées en vertu de la Loi sur l'accès**. Si le Fournisseur de services reçoit une demande d'une personne concernée relativement aux Renseignements personnels d'EXO qui le concernent en vertu de la Loi sur l'accès (ex. demande d'accès ou de rectification), il doit en informer rapidement EXO et accepter de

coopérer pleinement et rapidement avec EXO pour répondre à cette demande conformément à la Loi sur l'accès. Cette coopération peut inclure : (i) fournir à EXO, ou à tout tiers désigné par EXO, toutes les informations pertinentes, y compris des copies des Renseignements personnels d'EXO demandés (ii) corriger ou supprimer ces renseignements et fournir une attestation à l'effet que les Renseignements personnels d'EXO ont été corrigés ou supprimés conformément aux instructions d'EXO; (iii) expliquer comment les Renseignements personnels d'EXO sont traités par le Fournisseur de services; et (iv) expliquer comment les Renseignements personnels d'EXO ont été utilisés pour prendre une décision fondée exclusivement sur un traitement automatisé, y compris les renseignements utilisés pour rendre la décision et les raisons et principaux facteurs et paramètres ayant mené à la décision. Le Fournisseur de services doit se conformer sans délai aux instructions d'EXO concernant la réponse à la demande de la personne concernée par les Renseignements personnels d'EXO en vertu de la Loi sur l'accès.

7. **Avis en cas de demande de communication**. Dans le cas où le Fournisseur de services reçoit une demande gouvernementale ou autre demande réglementaire concernant les Renseignements personnels d'EXO, il accepte d'en informer immédiatement EXO afin de lui permettre d'avoir la possibilité de se défendre contre une telle demande. Le Fournisseur de services doit raisonnablement coopérer avec EXO dans le cadre de cette défense.

8. **Programme de sécurité des données**. Le Fournisseur de services doit maintenir un programme de sécurité complet, consigné par écrit, qui contient des mesures de protection administratives, techniques et physiques qui soient appropriées eu égard (a) à la taille, à l'étendue et au type d'activité du Fournisseur de services; (b) au type et au niveau de sensibilité des renseignements personnels traités par le Fournisseur de services; et (c) au besoin de sécurité et de confidentialité de ces renseignements (« **Programme de sécurité** »). Le Programme de sécurité du Fournisseur de services doit comprendre les mesures détaillées à l'Appendice 2 et être conçu de manière à (a) protéger la confidentialité, l'intégrité et la disponibilité des Renseignements personnels d'EXO en possession ou sous le contrôle du Fournisseur de services ou auxquels le Fournisseur de services a accès; (b) protéger contre toute menace ou tout danger anticipé pour la confidentialité, l'intégrité et la disponibilité des Renseignements personnels d'EXO; (c) protéger contre l'accès, l'utilisation, la communication, l'altération ou la destruction non autorisés ou illégaux des Renseignements personnels d'EXO; (d) protéger contre la perte, la destruction accidentelle ou l'endommagement des Renseignements personnels d'EXO; et (v) protéger les Renseignements personnels d'EXO conformément à la Loi sur l'accès.

9. **Incidents de confidentialité**

9.1 Avis à EXO en cas d'Incident de confidentialité. Le Fournisseur de services doit immédiatement et sans délai informer EXO de toute perte raisonnablement suspectée ou réelle, ou de tout accès non autorisé, utilisation ou communication des Renseignements personnels d'EXO, ou de toute autre violation ou tentative de violation, par toute personne, du Programme de sécurité du Fournisseur de services ou de toute autre atteinte à la protection des Renseignements personnels d'EXO (« **Incident de confidentialité** »). Bien que la notification téléphonique initiale puisse être sous forme de résumé, une notification écrite complète doit être remise à EXO dans les quarante-huit (48) heures. L'avis doit résumer, de manière

raisonnablement détaillée, la nature et la portée de l'Incident de confidentialité (y compris chaque Renseignement personnel d'EXO impliqué, le cas échéant) et les mesures correctives déjà prises ou qui seront prises par le Fournisseur de services. La notification sera complétée en temps utile par les détails raisonnablement demandés par EXO, y compris les rapports d'enquêtes pertinents. Le Fournisseur de services prendra rapidement toutes les mesures correctives nécessaires et recommandables, et coopérera pleinement avec EXO dans tous les efforts raisonnables pour atténuer les effets négatifs de l'Incident de confidentialité et pour empêcher qu'il ne se reproduise.

9.2 Avis d'Incident de confidentialité. Les parties collaboreront pour déterminer si une notification de l'Incident de confidentialité doit être donnée à toute personne et organisme (y compris les personnes concernées et la Commission d'accès à l'information) et, le cas échéant, pour déterminer le contenu de cette notification. EXO est seul responsable de décider quelle partie signalera l'Incident de confidentialité et le Fournisseur de services supportera tous les coûts de la notification.

9.3 Registre des Incidents de confidentialité. Le Fournisseur de services doit conserver un registre des Incidents de confidentialité pendant une période d'au moins cinq (5) ans après la date à laquelle il conclut qu'un Incident de confidentialité s'est produit, afin de pouvoir en fournir une copie à la Commission d'accès à l'information sur demande. Ce registre doit inclure, au minimum (i) une description des Renseignements personnels d'EXO visés par l'Incident de confidentialité; (ii) une brève description des circonstances entourant l'Incident de confidentialité; (iii) la date ou la période où l'Incident de confidentialité a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période; (iv) la date ou la période au cours de laquelle le Fournisseur de services a pris connaissance de l'Incident de confidentialité; (v) le nombre de personnes concernées par l'Incident de confidentialité ou, s'il n'est pas connu, une approximation de ce nombre; (vi) si l'Incident de confidentialité a été signalé ou non (aux personnes concernées et aux organismes de réglementation pertinents) et, le cas échéant, les raisons pour lesquelles l'Incident de confidentialité n'a pas été signalé; et (vii) une brève description des mesures prises par le Fournisseur de services, à la suite de la survenance de l'Incident de confidentialité, afin de diminuer les risques qu'un préjudice soit causé aux personnes concernées.

10. Services spécifiques nécessitant une collaboration supplémentaire

10.1. Évaluations des facteurs relatifs à la vie privée. Si les Services impliquent la collecte, l'utilisation, la conservation, la communication, la destruction ou tout autre type de traitement des Renseignements personnels d'EXO qui nécessite qu'EXO procède à une évaluation des facteurs relatifs à la vie privée (« **EFVP** ») ou à toute autre évaluation similaire ou réévaluation périodique qu'EXO considère comme requise en vertu de la Loi sur l'accès, y compris toute acquisition, tout développement ou toute refonte d'un système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de Renseignements personnels d'EXO, le Fournisseur de services s'engage à coopérer pleinement et rapidement avec EXO dans la conduite d'une telle évaluation ou réévaluation et à mettre en œuvre toutes

les mesures raisonnables que les parties jugent appropriées pour atténuer les risques potentiels à la confidentialité ou la sécurité des renseignements identifiés par EXO, à la suite de l'évaluation ou de la réévaluation, afin de garantir qu'EXO respecte ses obligations en vertu de la Loi sur l'accès (y compris tous les droits applicables des personnes concernées) à tout moment.

11. Responsabilité et indemnisation

11.1. Aucune limitation de responsabilité. Nonobstant toute disposition contraire dans le Contrat de service, aucune limitation de la responsabilité du Fournisseur de services ne s'applique dans le cas de réclamations, demandes, actions ou procédures intentées contre EXO à la suite d'un manquement du Fournisseur de services à une obligation quelconque prévue par les présentes Clauses.

11.2. Indemnisation. Toute clause du Contrat de service relative à l'indemnisation s'applique à toute réclamation, demande, action ou procédure intentée contre EXO à la suite d'un manquement du Fournisseur de services à une obligation quelconque en vertu des présentes Clauses. En l'absence d'une clause du Contrat de service relative à l'indemnisation, le Fournisseur de services doit indemniser EXO et le dégager de toute responsabilité en cas de réclamation, demande, action ou procédure intentée contre EXO à la suite d'un manquement du Fournisseur de services à une obligation quelconque en vertu des présentes Clauses. Par souci de clarté, cette indemnisation doit inclure, sans s'y limiter, tout manquement aux présentes Clauses résultant des actions ou des omissions d'un tiers auquel le Fournisseur de services a transféré les Renseignements personnels d'EXO en vertu de l'article 3 des présentes Clauses.

12. Examen de sécurité et audit

12.1. À la demande d'EXO, le Fournisseur de services fournira à EXO des copies de ses politiques, de ses directives et de ses procédures en matière de protection des renseignements personnels, de respect de la vie privée et de sécurité de l'information, incluant le Programme de sécurité applicable aux Renseignements personnels d'EXO. Dans un délai raisonnable, le Fournisseur de services autorisera et coopérera raisonnablement avec EXO pour effectuer toute autre vérification relative à la confidentialité et à la sécurité des Renseignements personnels d'EXO, incluant, à titre d'exemple, en donnant à EXO l'occasion d'effectuer un audit de confidentialité et de sécurité du Programme de sécurité, des systèmes et des procédures du Fournisseur de services qui sont applicables aux Renseignements personnels d'EXO. Cet audit pourra être effectué par EXO dans les locaux de Fournisseur de services ou de la tierce partie engagée par EXO a contracté, ou par le biais de sondages et d'entrevues, au choix d'EXO.

12.2. Dans l'éventualité où le Fournisseur de services a des examens ou audits de sécurité de ses propres systèmes effectués par le Fournisseur de services ou par un tiers, incluant des évaluations de vulnérabilité et/ou d'intrusion, il avisera EXO de tous résultats qui pourraient avoir un impact défavorable sur les Renseignements personnels d'EXO et informera EXO de ses efforts mis en place pour mitiger ces vulnérabilités.

13. Interprétation, résiliation et destruction sécurisée

13.1. Les présentes Clauses fait partie intégrante du Contrat de service et constitue, avec le Contrat de service, l'entente intégrale entre les parties quant à l'objet de celui-ci, et toute représentation, déclaration ou arrangement antérieurs s'y rapportant est remplacé par les dispositions du Contrat de service. En cas d'incompatibilité entre les dispositions des présentes Clauses et tout autre contrat entre les parties, y compris le Contrat de service, les présentes Clauses a préséance sur le Contrat de service ou tout autre contrat.

13.2. EXO peut résilier de façon immédiate le Contrat de service pour cause, sur avis au Fournisseur de services, si le Fournisseur de services a manqué, de façon importante, à ses obligations en vertu des présentes Clauses et qu'EXO a donné un préavis d'au moins quinze (15) jours de la connaissance de cette violation par EXO (ce préavis devant préciser les détails raisonnables de la violation) et que le Fournisseur de services n'a pas remédié à sa violation pendant cette période.

13.3. Le Fournisseur de services doit retourner ou détruire en toute sécurité tous les Renseignements personnels d'EXO en sa possession ou en possession de tout tiers à qui il les a transférés au terme du Contrat ou sur les instructions d'EXO à la suite de la violation par le Fournisseur de services de toute disposition des présentes Clauses. Une telle destruction doit garantir que les Renseignements personnels d'EXO, où qu'ils se trouvent, sont rendus illisibles et irrécupérables de façon permanente. Sur préavis raisonnable et à la demande d'EXO, le Fournisseur de services doit fournir à EXO une attestation de conformité au présent article par un agent autorisé.

13.4. Les dispositions des présentes Clauses qui sont censées survivre à la résiliation resteront pleinement en vigueur après la résiliation des présentes Clauses.

EN FOI DE QUOI, EXO et le Fournisseur de services ont signé les présentes Clauses, attestées par la signature de leurs dirigeants dûment autorisés en ce nom au jour et à l'année indiqués ci-dessus.

RÉSEAU DE TRANSPORT MÉTROPOLITAIN (EXO)

Par: _____
Nom :
Titre :

NOM DU FOURNISSEUR DE SERVICES

Par: _____
Nom :
Titre :

APPENDICE 1

PRÉCISIONS QUANT AU TRAITEMENT DES RENSEIGNEMENTS PERSONNELS DU RÉSEAU

[Nom du Fournisseur de services]

Renseignements sur le Fournisseur de services (nom, numéro d'enregistrement, adresse et autres coordonnées)	**Traitement envisagé**	**Localisation du Traitement/conservation des Renseignements personnels d'EXO**

[Nom du ou des Sous-traitants]

Renseignements sur le sous-traitant (nom, numéro d'enregistrement, adresse et autres coordonnées)	**Traitement envisagé**	**Localisation du Traitement/conservation des Renseignements personnels d'EXO**

Traitement envisagé

Les Renseignements personnels d'EXO seront sujets aux traitements suivants (veuillez préciser) :

Catégories d'individus

Les Renseignements personnels d'EXO concernent les catégories d'individus suivants (clients, employés, etc.) (veuillez préciser) :

Catégories de Renseignements personnels

Les Renseignements personnels d'EXO concernent les catégories de renseignements suivants (veuillez préciser) :

APPENDICE 2

EXIGENCES MINIMALES DU PROGRAMME DE SÉCURITÉ

Sans limiter la généralité de ce qui précède, le Programme de sécurité du Fournisseur de services doit au minimum comprendre :

(a) **Sensibilisation et formation en matière de sécurité**. Un programme obligatoire de sensibilisation et de formation à la sécurité pour tous les employés (y compris la direction) du Fournisseur de services, qui comprend : (i) une formation sur la façon de mettre en œuvre et de respecter le Programme de sécurité; et (ii) la promotion d'une culture de sécurité de l'Information par des communications périodiques de la haute direction avec les employés.

(b) **Vérification des antécédents et surveillance**. Des politiques, des directives et des procédures visant à évaluer régulièrement les antécédents de tous les membres actuels et futurs de son personnel qui ont accès à des Renseignements personnels d'EXO, y compris les procédures de vérification des antécédents criminels. Ces vérifications seront effectuées sur une base annuelle pour s'assurer que les membres du personnel du Fournisseur de services soient conformes aux normes et exigences applicables.

(c) **Contrôle des accès**. Des politiques, des directives, des procédures et mesures de contrôle afin : (i) de limiter l'accès aux Systèmes d'Information et aux installations dans lesquelles ils sont hébergés aux personnes dûment autorisées ayant réellement besoin d'y accéder; (ii) de s'assurer que le plus faible volume de Renseignements personnels d'EXO est rendu accessible au Personnel autorisé, dans la mesure où cela est nécessaire à l'exercice de leurs fonctions; (iii) de prévenir que les membres du personnel et autres personnes non autorisées ne peuvent obtenir l'accès aux Renseignements personnels d'EXO; (iv) de supprimer les accès en temps opportun en cas de changement des responsabilités ou du statut d'un membre du personnel. Ces politiques, ces directives, ces procédures et ces mesures de contrôle comprennent l'utilisation d'une authentification multifacteurs et la mise en œuvre d'une politique de mots de passe garantissant que les mots de passe sont périodiquement mis à jour et offrent un niveau raisonnable de complexité.

(d) **Sécurité physique et environnementale**. Des mesures de contrôle qui fournissent une assurance raisonnable que l'accès physique aux installations où sont stockés les Renseignements personnels d'EXO, y compris les serveurs physiques, est limité aux personnes dûment autorisées et des contrôles pour détecter, prévenir et contrôler la destruction causée par des conditions environnementales extrêmes. Ces contrôles comprennent : (i) l'enregistrement et la surveillance des tentatives d'accès non autorisées aux installations du Fournisseur de services; (ii) des systèmes de surveillance par caméra aux points d'entrée des installations du Fournisseur de services; (iii) des systèmes qui surveillent et contrôlent la température et l'humidité de l'air à des niveaux appropriés pour le matériel informatique; et (iv) des modules d'alimentation sans interruption et des génératrices de secours qui assurent une alimentation de secours dans le cas de défaillance électrique.

(e) **Procédures en cas d'Incident de confidentialité**. Un plan d'intervention qui comprend des procédures à suivre en cas d'Incident de confidentialité. De telles procédures comprennent : (i) la formation d'une équipe interne de réponse aux Incidents avec un responsable de la réponse; (ii) l'évaluation du risque que pose l'Incident et la détermination des personnes susceptibles d'être touchées; (iii) l'établissement de rapports internes ainsi qu'un processus d'avis en cas de communication non autorisée de Renseignements personnels d'EXO; (iv) la tenue d'un registre de ce qui a été fait et par qui, afin d'aider à l'analyse ultérieure, y compris dans le cas d'une éventuelle action en justice; et (v) la réalisation et la documentation d'une analyse des causes de l'Incident et d'un plan de redressement.

(f) **Planification des mesures d'urgence**. Des politiques, des directives et des procédures d'intervention en cas d'urgence ou d'autre événement (par exemple, incendie, vandalisme, panne de système, pandémie de grippe et catastrophe naturelle) qui pourrait endommager les Renseignements personnels d'EXO ou les systèmes qui contiennent ces renseignements. De telles procédures comprennent : (i) une politique de sauvegarde périodique des systèmes de production et des bases de données contenant des Renseignements personnels d'EXO, selon un calendrier défini; (ii) un plan officiel de reprise après sinistre pour les installations du Fournisseur de services où sont stockés les Renseignements personnels, y compris l'obligation de tester régulièrement le plan de secours et un résumé des tests, au moins annuellement, disponible à EXO sur demande; (iii) un processus officiel visant à gérer les événements non prévus afin de minimiser la perte des ressources essentielles.

(g) **Contrôles de vérification**. Du matériel, des logiciels et/ou des mécanismes qui enregistrent et examinent l'activité dans les Systèmes d'Information qui contiennent ou utilisent de l'Information électronique. Ces mécanismes doivent garantir que l'activité est attribuable à un individu identifiable.

(h) **Intégrité des données**. Des politiques, des directives et des procédures visant à assurer la confidentialité, l'Intégrité et la disponibilité des Renseignements personnels d'EXO et à les protéger contre la communication, la modification inappropriée ou la destruction.

(i) **Sécurité du stockage et de la transmission**. Des mesures de sécurité visant à empêcher l'accès non autorisé aux Renseignements personnels d'EXO qui sont transmis sur un réseau public de communications électroniques ou stockés électroniquement. De telles mesures comprennent (i) limiter l'utilisation de dispositifs de stockage amovibles, tels des lecteurs USB (*Universal Serial Bus*), pour stocker ou transférer les Renseignements personnels d'EXO uniquement dans la mesure où cela est manifestement nécessaire pour atteindre un objectif spécifique et documenté; (ii) l'anonymisation et la pseudonymisation lorsque cela est autorisé expressément par EXO; et (iii) le chiffrement de tous Renseignements personnels d'EXO stockés sur des ordinateurs de bureau, des ordinateurs portables ou d'autres dispositifs de stockage amovibles.

(j) **Segmentation**. Des mesures garantissant la segmentation des Renseignements personnels d'EXO à partir des données d'autrui.

(k) **Responsabilité assignée en matière de sécurité**. Attribuer la responsabilité de l'élaboration, de la mise en œuvre et de la maintenance de son Programme de sécurité, y compris : (i) la désignation d'un responsable de la sécurité ayant la responsabilité globale; et (ii) la définition des rôles et des responsabilités en matière de sécurité pour les personnes exerçant des responsabilités en matière de sécurité.

(l) **Tests**. Des tests réguliers des contrôles, des systèmes et des procédures clés du Programme de sécurité afin de s'assurer qu'ils sont correctement mis en œuvre et qu'ils permettent de contrer efficacement les menaces et les risques identifiés. Ces tests sont effectués au moins une (1) fois par an par des parties indépendantes qualifiées. S'il y a lieu, ces essais comprennent : (i) des évaluations internes des risques; (ii) les certifications ISO 27001 et ISO 27018; et (iii) des rapports d'audit tels que *Service Organization Control* (SOC).

(m) **Surveillance**. Une surveillance du réseau et des systèmes, y compris les journaux d'erreurs sur les serveurs et les événements de sécurité pour tout problème potentiel. Une telle surveillance comprend : (i) examiner les changements touchant les systèmes d'authentification, d'autorisation et de vérification; (ii) examiner l'accès privilégié aux systèmes du Fournisseur de services; et (iii) engager des tiers pour effectuer régulièrement des évaluations de la vulnérabilité des réseaux et des tests de pénétration.

(n) **Gestion du changement et de la configuration**. Tenir à jour les politiques et les procédures de gestion des changements apportés aux systèmes de production, aux applications et aux bases de données du Fournisseur de services. Ces politiques et ces procédures doivent comprendre : (i) un processus de documentation, de mise à l'essai et d'approbation des correctifs et de la maintenance du service; (ii) un processus de mise à jour de la sécurité qui exige que les systèmes soient mis à jour en temps opportun en fonction d'une analyse des risques; et (iii) un processus permettant au Fournisseur de services de faire évaluer par un tiers la sécurité des applications Web.

(o) **Rajustements du programme**. Le Fournisseur de services doit surveiller, évaluer et ajuster, au besoin, le Programme de sécurité à la lumière des éléments suivants : (i) tout changement technologique pertinent et toute menace interne ou externe à l'égard du Fournisseur de services ou des Renseignements personnels d'EXO; (ii) les exigences relatives à la sécurité et la protection des données, y compris les Renseignements personnels, applicables à EXO et/ou au Fournisseur de services; et (iii) les transactions du Fournisseur de services, comme les fusions et acquisitions, alliances et coentreprises, ententes de sous-traitance et modifications des systèmes informatiques.

(p) **Appareils**. Tous les ordinateurs portables et de bureau utilisés par le Fournisseur de services et ses sous-traitants lorsqu'ils accèdent aux Renseignements personnels d'EXO doivent : (i) être équipés d'au moins un disque dur AES 128 bits à cryptage complet; (ii) disposer d'un logiciel de détection et de prévention des virus et des logiciels malveillants à jour et régulièrement mis à jour avec les définitions des virus; et (iii) maintenir un logiciel de détection et de prévention des virus et des logiciels malveillants. Cela comprend, sans toutefois s'y limiter, la mise en œuvre rapide de toute amélioration ou correction applicable en matière de sécurité mise à disposition par le fournisseur de ce logiciel.

APPENDICE 3

MODÈLE D'ENGAGEMENT DE CONFIDENTIALITÉ

ENGAGEMENT À LA CONFIDENTIALITÉ

DES EMPLOYÉS DE _____[*METTRE LE NOM DU FOURNISSEUR*] QUI ONT ACCÈS AUX RENSEIGNEMENTS PERSONNELS DÉTENUS PAR LE RÉSEAU DE TRANSPORT MÉTROPOLITAIN DANS LE CADRE DE L'EXERCICE DE LEURS FONCTIONS POUR LA RÉALISATION D'UN CONTRAT _____[*METTRE L'INTITULÉ DU CONTRAT*] OCTROYÉ PAR L'AUTORITÉ RÉGIONALE DE TRANSPORT MÉTROPOLITAIN

ATTENDU que le Réseau de transport métropolitain est un organisme public assujetti à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1 (la « *Loi sur l'accès* »);

ATTENDU que pour les fins de l'exécution du contrat _____ [*mettre l'intitulé du contrat*] octroyé par le Réseau de transport métropolitain (le « Réseau »), le _____[*mettre la date de l'octroi],* le _____ _____[*nom du fournisseur*] reconnaît qu'elle est appelée à prendre connaissance ou à recevoir communication de renseignements personnels au sens de la *Loi sur l'accès*;

ATTENDU que pour réaliser ledit contrat, _____ [*le nom du fournisseur*] doit accéder et traiter des renseignements personnels appartenant au Réseau;

ATTENDU que _____[*nom du fournisseur*] reconnaît que la *Loi sur l'accès* s'applique aux renseignements personnels qui lui sont confiés dans le cadre de l'exécution du contrat et s'engage à prendre les mesures nécessaires pour qu'elle soit respectée;

ATTENDU que _____[*nom du fournisseur*] doit faire signer, à ses employés, le présent engagement de confidentialité et à transmettre une copie au Réseau avant de débuter l'exécution dudit contrat;

ATTENDU que _____[*nom du fournisseur*] ne pourra déléguer à quiconque en tout ou en partie les obligations qui lui incombent aux termes du présent engagement de confidentialité.

Je, soussigné, _____[nom et prénom en lettres moulées], étant en fonction à [*nom du fournisseur*], déclare ce qui suit et m'engage, en toute connaissance de cause, à respecter les règles suivantes :

1. Je reconnais que dans le cadre de la réalisation du contrat octroyé par le Réseau à _____[*nom du fournisseur*] et dans le cadre de l'exercice

de mes fonctions, je serai appelé à avoir accès à des renseignements personnels appartenant au Réseau.

2. Je reconnais que ces renseignements personnels sont confidentiels et qu'ils ne peuvent être divulgués à des tiers sans le consentement des personnes concernées ou l'autorisation de la loi. En conséquence, je m'engage à ne pas utiliser, conserver, reproduire ou divulguer à des tiers ces renseignements personnels auxquels j'aurai accès sauf lorsque cela est nécessaire à l'exercice de mes fonctions et en conformité avec les autorisations et directives émises par mon employeur.

3. Par ailleurs, je m'engage à ne pas consulter ces renseignements personnels ni à prendre connaissance de ceux-ci à moins que cela ne soit nécessaire à l'exercice de mes fonctions et en conformité avec les autorisations et directives émises par mon employeur.

4. Je m'engage de plus à ne pas divulguer à quiconque, à moins d'être dûment autorisé à le faire, des informations tels que des codes d'accès, des clés de chiffrement, des caractéristiques d'une base de données contenant les renseignements personnels, des modes d'opération, des mesures de sécurité ou autres renseignements permettant à des tiers non autorisés d'avoir accès aux renseignements personnels du Réseau.

5. Je m'engage à porter à la connaissance de mes supérieurs dans les meilleurs délais toute situation permettant de croire qu'en raison d'une défaillance technique, ou d'une tentative d'accès injustifié, les renseignements personnels sont ou pourraient être accessibles à des personnes qui n'ont pas le droit de les consulter.

6. À la fin du contrat, je m'engage à détruire ou à remettre intégralement les renseignements personnels du Réseau en conformité avec les autorisations et les directives émises par mon employeur et par le Réseau.

7. Je reconnais et j'accepte que la violation de l'une ou l'autre des obligations contenues dans le présent engagement de confidentialité pourra donner lieu à l'imposition de sanctions pouvant aller jusqu'au congédiement.

EN FOI DE QUOI, J'AI SIGNÉ :

_____ _____

Signature de l'employé (e) Date

Titre et fonction

_____ _____

Signature du témoin Lieu

Titre et fonction