**UNIVERSITÉ CONCORDIA**

**ADDENDA SUR LE TRAITEMENT DES RENSEIGNEMENTS PERSONNELS APPLICABLE À TOUS LES CONTRATS CONCLUS AVEC L'UNIVERSITÉ CONCORDIA**

Tout fournisseur, consultant, entreprise, personne ou entité (collectivement et individuellement la **« Partie Contractante »**) qui conclut un contrat avec l'Université Concordia **(« Concordia »**) de quelque manière ou sous quelque forme que ce soit, y compris, sans s'y limiter, au moyen d'un bon de commande, d'une entente, d'un contrat, d'un avenant à un contrat existant, d'une lettre d'intention, d'un cahier des charges, d'un devis ou de tout autre instrument (collectivement ou individuellement, selon le cas, le **« Contrat »**) accepte irrévocablement les conditions du présent Addenda sur le Traitement des Renseignements Personnels (l'**« Addenda »**). Nonobstant toute autre disposition contraire, quelle qu'elle soit, y compris, sans s'y limiter, en droit ou dans les conditions générales d'une Partie Contractante, y compris toute clause du type « accord intégral », le présent Addenda prévaut à tout moment sur le Contrat et sur toute autre condition de Concordia ou de la Partie Contractante. Le présent Addenda et ses conditions s'appliquent au Contrat et remplacent toute autre condition et tout bon de commande de la Partie Contractante, qu'ils soient incorporés par référence ou non, qu'ils figurent dans une entente avec Concordia ou non, qu'ils existent actuellement ou qu'ils existent à l'avenir, et qu'ils soient acceptés en ligne par Concordia ou non. Il est entendu que l'Addenda prévaut également sur toutes les conditions présentées sur un écran, par courriel, dans un formulaire ou autrement, que ces conditions aient été acceptées ou non par Concordia, un employé, un ou plusieurs utilisateurs ou un étudiant de Concordia. Le présent Addenda ne peut être modifié que de manière expresse, par écrit, et toute modification doit être signée par un représentant autorisé de Concordia, conformément à la Politique sur l'examen des contrats, le pouvoir de signature et les autorisations requises de Concordia.

**CONSIDÉRANT** que les parties ont conclu un Contrat;

**CONSIDÉRANT** que, pour s'acquitter des obligations qui lui incombent en vertu du Contrat, la Partie Contractante peut être amenée à détenir, héberger, stocker, gérer, posséder ou traiter des Renseignements Personnels (tel que défini ci-dessous) pour le compte de Concordia;

**CONSIDÉRANT** qu'en vertu des articles 3 et 6 de la *Loi sur l'Accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ c A-2.1) (la **« Loi sur l'Accès »**), Concordia est un organisme public régi par la Loi sur l'Accès;

**CONSIDÉRANT** que l'article 67.2 de la Loi sur l'Accès permet à Concordia de communiquer des Renseignements Personnels à toute personne ou à tout organisme sans le consentement des personnes concernées si cette communication est nécessaire à l'exécution d'une entente, sous réserve des conditions suivantes :

(a) l'entente doit être conclue par écrit;
(b) l'entente doit préciser les dispositions de la Loi sur l'Accès qui s'appliquent au renseignement communiqué;
(c) l'entente doit indiquer les mesures que la Partie Contractante doit prendre pour assurer le caractère confidentiel du renseignement, que celui-ci ne doit être utilisé que dans le cadre de l'exécution de l'entente et qu'il ne doit pas être conservé après l'expiration de l'entente;
(d) avant que le renseignement soit communiqué, Concordia doit obtenir un engagement de confidentialité de toute personne à qui le renseignement peut être communiqué à moins que le Responsable du Respect de la Vie Privée de Concordia estime que cela n'est pas nécessaire.

**EN CONTREPARTIE DE CE QUI PRÉCÈDE, LA PARTIE CONTRACTANTE CONVIENT IRRÉVOCABLEMENT DE CE QUI SUIT :**

## 1. DÉFINITIONS

Les termes définis dans le présent Addenda ont la signification énoncée ci-dessous :

1.1. **« Données de Concordia »** signifie tout renseignement confidentiel appartenant à Concordia ou détenu ou géré par Concordia et tout renseignement de Concordia, y compris, sans s'y limiter, tous les renseignements confidentiels de tiers détenus par Concordia, toutes les données sur les étudiants et sur les demandes d'admission, les renseignements sur les étudiants, les résultats d'examen et d'évaluation ainsi que toute donnée et tout renseignement personnel permettant d'identifier des personnes, comme des étudiants, des diplômés, des donateurs, des professeurs ou des employés de Concordia, collectivement considérées comme des **« Renseignements Personnels »** en vertu de la Loi sur l'Accès. Il est entendu, sans limiter la généralité de ce qui précède, que toutes les Données de Concordia, qu'elles soient conservées en

totalité ou en partie localement ou dans un ou plusieurs Centre de Données sont considérées comme des Données de Concordia.

1.2. **« Centre de Données »** signifie tout lieu ou installation utilisé pour héberger la totalité ou une partie des Données.

1.3. **« Partie »** signifie Concordia ou la Partie Contractante et le terme **« Parties »** signifie Concordia et la Partie Contractante.

1.4. **« Responsable du Respect de la Vie Privée »** signifie la personne nommée par Concordia pour être responsable de la protection des Renseignements Personnels aux fins de la Loi sur l'Accès.

1.5. **« Incident de Sécurité »** signifie toute atteinte à la sécurité entraînant, de manière accidentelle ou illégale, le traitement, la destruction, la perte, l'altération, la copie, le stockage, la détérioration, la communication non autorisée ou la consultation de Données de Concordia, quand ces données sont transmises, stockées ou traitées par la Partie Contractante dans le cadre de le présent Addenda.

1.6. **« Mesures de Sécurité »** signifie les mesures de sécurité prises par la Partie Contractante qui doivent minimalement être conformes à celles énoncées à l'**ANNEXE A**.

1.7. **« Sous-traitant »** signifie tout tiers qui a accès aux Données de Concordia et qui est engagé par la Partie Contractante pour l'aider à remplir ses obligations en vertu du Contrat. Les sous-traitants peuvent être des filiales de la Partie Contractante, mais ne peuvent pas être des employés, des contractants ou des consultants de la Partie Contractante.

1.8. **« Utilisateurs »** signifie, selon le cas, toute personne à laquelle Concordia donne accès aux services de la Partie Contractante, y compris tout employé (à temps plein ou à temps partiel), étudiant, consultant, employeur, entrepreneur indépendant ou mandataire de Concordia.

## 2. PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

2.1. La Partie Contractante s'engage à respecter les lois applicables en matière de protection de la vie privée, y compris la Loi sur l'Accès (les **« Lois sur la Protection de la Vie Privée »**).

2.2. Les exigences suivantes concernant les Renseignements Personnels s'appliquent à tout et prévalent sur tout, y compris sur le Contrat, et constituent une considération essentielle pour Concordia sans laquelle elle n'aurait pas conclu le Contrat :

2.2.1. Reconnaissance. La Partie Contractante reconnaît que Concordia a des obligations en vertu de la Loi sur l'Accès lorsqu'elle communique des Renseignements Personnels ou qu'elle confie des Renseignements Personnels à des personnes afin qu'ils soient conservés, utilisés ou communiqués. La Partie Contractante reconnaît que les renseignements transmis ou communiqués par Concordia peuvent comprendre des Renseignements Personnels et que les articles 53, 54, 56, 59, 63.1, 65, 65.1 et 67.2 de la Loi sur l'Accès s'appliquent à tous les Renseignements Personnels. En particulier, lorsqu'elle collecte des Renseignements Personnels pour le compte de Concordia, la Partie Contractante veille à se conformer aux exigences en matière d'information et de transparence de l'article 65 de la Loi sur l'Accès.

2.2.2. Utilisation autorisée. Les Données de Concordia, y compris les Renseignements Personnels, envoyées à la Partie Contractante, détenues par elle ou mises à sa disposition en vertu du Contrat ne doivent être utilisées par la Partie Contractante que pour remplir ses obligations en vertu du Contrat et du présent Addenda. La Partie Contractante ne collecte,

conserve, communique, utilise, traite ou élimine les Données de Concordia qu'en conformité avec le Contrat et le présent Addenda.

2.2.3. Utilisation interdite. Sauf dans les cas autorisés dans le présent Addenda, la Partie Contractante ne peut pas accéder aux Données de Concordia, y compris aux Renseignements Personnels, ni les distribuer, les vendre, les concéder sous licence ou les transférer à ses propres fins ou au profit d'une partie autre que Concordia.

2.2.4. Mesures de Sécurité. La Partie Contractante met en œuvre et maintient des mesures de sécurité techniques et organisationnelles appropriées et raisonnables afin de protéger les Données de Concordia et les Renseignements Personnels contre des Incidents de Sécurité et de préserver la sécurité et la confidentialité des Données de Concordia, y compris les Renseignements Personnels. Ces mesures comprennent minimalement celles énoncées à l'**ANNEXE A**. La Partie Contractante doit prendre des précautions raisonnables pour préserver l'intégrité de tous les Renseignements Personnels qu'elle traite et pour prévenir toute corruption ou perte de Renseignements Personnels, y compris, sans s'y limiter, en mettant en place des mesures efficaces de sauvegarde et de restauration des données conformément aux Lois sur la Protection de la Vie Privée et d'autres lois applicables.

2.2.5. Incidents de Sécurité. Si la Partie Contractante a connaissance d'un Incident de Sécurité touchant des Données de Concordia dont la Partie Contractante ou l'un de ses employés, mandataires ou Sous-traitants, y compris les hébergeurs ou les prestataires de services d'hébergement, a la responsabilité ou la gestion, la Partie Contractante s'engage à prendre immédiatement les mesures prévues dans les Mesures de Sécurité et à notifier Concordia rapidement d'un tel Incident de Sécurité.

2.2.6. Tenue d'archives. La Partie Contractante conservera un enregistrement de tout Incident de Sécurité conformément aux Lois sur la Protection de la Vie Privée.

2.2.7. Notification. La Partie Contractante accepte que Concordia soit seule habilitée à décider s'il convient de signaler l'Incident de Sécurité aux personnes concernées, aux autorités de réglementation, aux organismes d'application de la loi ou à d'autres personnes, comme l'exigent les Lois sur la Protection de la Vie Privée ou d'autres lois ou règlements, ou à la discrétion de Concordia, y compris le contenu et le mode de transmission du signalement.

2.2.8. Coopération. La Partie Contractante coopérera immédiatement et pleinement avec Concordia et avec les assureurs de Concordia, le cas échéant, et fournira toute autre information que Concordia ou les assureurs de Concordia peuvent raisonnablement demander, ce qui comprend la mise à disposition de tous les dossiers, journaux, fichiers, rapports de données et autres documents nécessaires pour se conformer aux Lois sur la Protection de la Vie Privée ou à toute autre exigence raisonnable de Concordia. La Partie Contractante confirme à Concordia qu'elle a également informé ses assureurs si Concordia l'exige. La Partie Contractante restaurera les Données compromises à ses propres frais.

2.2.9. Engagements signés. La Partie Contractante déclare et garantit que tous ses employés, agents, mandataires et Sous-traitants ont signé des engagements de confidentialité au moins aussi contraignants que les engagements de confidentialité du présent Addenda, et dont le Responsable du Respect de la Vie Privée de Concordia peut demander une copie.

2.2.10. Audit et vérification. Pour vérifier le respect des dispositions du présent Addenda, des exigences de sécurité ou des Lois sur la Protection de la Vie Privée par la Partie Contractante, que ce soit à la suite d'un Incident de Sécurité avéré ou parce que des autorités de réglementation l'exigent, Concordia peut demander à la Partie Contractante, moyennant un préavis écrit de 30 jours, qu'un tiers effectue un audit des installations, de l'équipement, des documents et des données électroniques de la Partie Contractante liés au traitement des Données de Concordia en vertu du Contrat et de l'Addenda (l'**« Audit »**), à condition que : (a)

l'audit soit effectué aux frais de Concordia; (b) les parties conviennent mutuellement de l'étendue, du calendrier et de la durée de l'audit; et (c) l'audit n'ait pas d'incidence déraisonnable sur les activités habituelles de la Partie Contractante. Concordia reconnaît que les réponses écrites ou l'audit décrits dans le présent article 2.2 sont soumis aux dispositions relatives à la confidentialité du Contrat et de l'Addenda.

2.2.11. Résiliation. En cas de résiliation du Contrat pour quelque raison que ce soit, ou à la demande de Concordia, la Partie Contractante doit immédiatement remettre à Concordia toutes les Données de Concordia, y compris les Renseignements Personnels (physiques ou numériques) ou, à la discrétion de Concordia, détruire par des moyens sûrs toutes les Données de Concordia, y compris tous les Renseignements Personnels (physiques ou numériques) que la Partie Contractante gère ou possède. Sous réserve de l'article 2.2.12, la Partie Contractante ne doit conserver aucune copie des Données de Concordia, y compris les Renseignements Personnels. À la demande de Concordia, la Partie Contractante doit fournir une déclaration solennelle, ayant la même force et le même effet que si elle était faite sous serment, d'un responsable autorisé de la Partie Contractante, soit (i) que toutes les Données de Concordia, y compris les Renseignements Personnels, ont été remises à Concordia, et qu'aucune copie n'est restée en sa possession, et/ou (ii) que toutes les Données de Concordia, y compris les Renseignements Personnels, ont été détruites.

2.2.12. Obligations légales. Si une loi, un règlement ou un organisme gouvernemental ou réglementaire exige de la Partie Contractante qu'elle conserve des documents ou du matériel qu'elle serait autrement tenue de remettre ou de détruire, elle communiquera par écrit avec Concordia pour préciser les documents ou le matériel qu'elle doit conserver ainsi que les motifs juridiques de la conservation et pour établir un calendrier précis pour la destruction une fois que l'obligation de conservation aura pris fin. La Partie Contractante ne peut utiliser les Données de Concordia conservées que pour le motif de conservation requis ou à des fins d'audit.

## 3. DROIT À LA VIE PRIVÉE

3.1. Demandes d'accès et de correction. Si Concordia n'est pas en mesure de consulter, de supprimer ou de récupérer de manière indépendante les Données de Concordia pertinentes, la Partie Contractante doit, en tenant compte du type de traitement nécessaire, coopérer raisonnablement avec Concordia pour aider celle-ci à répondre à toute demande présentée par une personne au sujet de la manière dont les Données de Concordia sont traitées aux termes du présent Addenda. Si une telle demande est adressée directement à la Partie Contractante, celle-ci en informera rapidement Concordia et ne répondra pas directement à la demande (sauf pour diriger la personne vers Concordia) sans l'autorisation de Concordia, à moins qu'elle y soit contrainte par la loi.

3.2. Coopération générale. Chaque partie coopérera raisonnablement avec l'autre dans le cadre des activités visées par le présent Addenda et pour permettre à chaque Partie de se conformer aux obligations que lui imposent les Lois sur la Protection de la Vie Privée.

## 4. SOUS-TRAITANTS

4.1. Autorisation de sous-traitance. Si la Partie Contractante sous-traite, en tout ou en partie, l'une des obligations qui lui incombent au titre du présent Addenda, alors la Partie Contractante s'engage et convient de n'utiliser que des Sous-traitants dont les Centre de Données sont situés au Québec et qui traitent les Données uniquement au Québec ou dans un État ou une juridiction jugé acceptable par Concordia conformément à la Loi sur l'Accès et tel qu'indiqué à **l'ANNEXE B.**

4.2. Responsabilité. La Partie Contractante est la seule responsable du respect de l'exigence susmentionnée. La Partie Contractante limitera l'accès des Sous-traitants aux seules Données de

Concordia dont ils ont besoin pour aider la Partie Contractante à exécuter le Contrat, et la Partie Contractante demeurera responsable de tout acte ou omission commis par des Sous-traitants qui amèneraient la Partie Contractante à ne pas respecter les obligations qui lui incombent aux termes du présent Addenda. La Partie Contractante conclut ou a conclu avec ses Sous-traitants des ententes écrites qui contiennent des conditions essentiellement identiques à celles énoncées dans le présent Addenda et elle fournira à Concordia une copie de ces ententes si Concordia lui en fait la demande par écrit.

## 5. CENTRES DE DONNÉES

La Partie Contractante accepte, déclare et garantit que les Données (y compris toute copie de sauvegarde) seront hébergées dans des Centres de Données situés au Québec ou dans un État ou une juridiction jugé acceptable par Concordia conformément à la Loi sur l'Accès et tel qu'indiqué à l'**ANNEXE B** (les **« Juridictions Acceptées »**) et que les données seront en tout temps traitées dans des Juridictions Acceptées.

## 6. INDEMNISATION ET LIMITATION DE RESPONSABILITÉ

6.1. La Partie Contractante (la **« Partie Indemnisante »**) doit indemniser et dégager Concordia (la **« Partie Indemnisée »**) de toute responsabilité et prendre en charge la défense de Concordia contre toute réclamation pouvant viser la Partie Indemnisée ou que la Partie Indemnisée pourrait recevoir en rapport avec : (i) le non-respect des obligations énoncées dans le présent Addenda; (ii) toute négligence ou faute de la Partie Indemnisante; (iii) toute brèche de sécurité dont la Partie Indemnisante est responsable et qui entraîne la perte, la transmission, la communication ou la corruption de la totalité ou d'une partie des renseignements de la Partie Indemnisée, ou d'autres effets négatifs pour ces renseignements, lesquels comprennent, sans s'y limiter, les Renseignements confidentiels de Concordia. Aucune limitation de responsabilité ne s'applique aux responsabilités de la Partie Contractante en ce qui concerne ces indemnisations.

Aux fins du présent article, la Partie Indemnisante doit, dans chaque cas, indemniser, défendre et dégager la Partie Indemnisée de toute responsabilité à l'égard de toute réclamation qu'elle reçoit en raison de tout acte, omission, négligence, faute, manquement ou autre commis par la Partie Indemnisante ou commis par ceux dont la Partie Indemnisante est légalement responsable.

6.2. Le présent article 6 (Indemnisation et limitation de responsabilité) remplace et complète les articles du Contrat portant sur la responsabilité et il survivra à l'expiration ou à la résiliation du Contrat ou de l'Addenda, quelle qu'en soit la raison.

6.3. Sous réserve des dispositions du présent Addenda, toute limitation de responsabilité applicable à la Partie Contractante est réciproque et s'applique à la responsabilité de Concordia à l'égard de la Partie Contractante.

## 7. DURÉE ET RÉSILIATION

7.1. Durée. La Partie Contractante est liée par le présent Addenda tant qu'elle détient, stocke, héberge, gère, possède ou conserve des Données de Concordia reçues, consultées, collectées générées ou traitées de toute autre manière pour le compte de Concordia dans le cadre de l'exécution du Contrat ou de l'Addenda. Pour clarifier, nonobstant toute autre disposition du Contrat, la résiliation du Contrat ou du présent Addenda ne libère pas la Partie Contractante de ses obligations et engagements en matière de protection des Renseignements Personnels. Le non-respect des modalités du présent Addenda constitue un manquement autorisant Concordia à résilier le Contrat, sous réserve de tous les recours dont dispose Concordia en vertu du présent Addenda ou de la loi.

7.2. Effet de la résiliation et survie. Si le Contrat est résilié, la Partie Contractante doit se reporter à l'article 7.1 du présent Addenda.

**8. NOTIFICATIONS**

8.1. Notifications. Toutes les notifications et autres communications requises ou autorisées aux termes du présent Addenda peuvent être transmises par courrier électronique ou par courrier de première classe aux représentants désignés sur la première page de l'Addenda.

**9. DIVERS**

9.1. Priorité des ententes. À l'exception des modifications apportées par le présent Addenda, le Contrat reste inchangé et pleinement en vigueur. En cas de conflit entre le présent Addenda et le Contrat, l'Addenda prévaudra dans la mesure de ce conflit.

9.2. Divisibilité. Si une disposition de l'Addenda se trouve invalide, illégale ou inexécutable, la validité, la légalité et la force exécutoire des autres dispositions ne sont en aucun cas affectées ou compromises, et cette disposition ne sera sans effet que dans la mesure où elle est invalide, illégale ou inexécutable.

9.3. Lois applicables. Le présent Addenda est régie par les lois du Québec et les lois du Canada applicables dans la province de Québec, à l'exclusion de toute autre, et les Parties reconnaissent la compétence exclusive des tribunaux de la province de Québec, Canada, district de Montréal.

9.4. Renonciation. Aucun retard ou omission de la part de l'une des Parties dans l'exercice d'un droit aux termes de l'Addenda ne peut être interprété comme une renonciation à ce droit, et les deux Parties se réservent le droit d'exercer ce droit de temps à autre, aussi souvent qu'elles le jugent opportun.

**L'ANNEXE A**

**MESURES DE SÉCURITÉ**

| Code d'identification | Domaine de contrôle | Exigence |
|---|---|---|
| EG-GOV-1 | Cadre de gouvernance | Un cadre documenté de gestion de la sécurité est en place. |
| EG-GOV-2 | Cadre de gouvernance | La Partie Contractante a élaboré et publié une politique de sécurité informatique qu'elle met à jour à intervalles réguliers. |
| EG-GOV-3 | Cadre de gouvernance | La Partie Contractante dispose de diagrammes de l'architecture de la solution comprenant une description complète du flux des Données de Concordia. |
| EG-GOV-4 | Cadre de gouvernance | La Partie Contractante a documenté et mis en œuvre une politique relativement à l'accueil et au départ d'employés. |
| EG-GOV-5 | Cadre de gouvernance | La Partie Contractante dispose d'un processus documenté de gestion des modifications qui prévoit au minimum des étapes d'autorisation, d'analyse d'impact, de mise à l'essai et de validation avant la mise en production des modifications. |
| EG-GOV-6 | Cadre de gouvernance | L'organigramme, l'énoncé de mission et les politiques de l'unité de sécurité informatique de la Partie Contractante sont documentés. |
| EG-GOV-7 | Cadre de gouvernance | La Partie Contractante a mis en œuvre et tient à jour une politique et une procédure pour gérer l'application des correctifs vitaux à tous les systèmes et applications. |
| EG-GOV-8 | Cadre de gouvernance | La Partie Contractante a mis en œuvre et tient à jour une politique et une procédure pour évaluer et atténuer les risques liés à ses activités et à sa chaîne d'approvisionnement. |
| EG-GOV-9 | Cadre de gouvernance | Le cycle de vie de la solution tient compte des meilleures pratiques de sécurité informatique et celles-ci sont documentées. |
| EG-GOV-10 | Cadre de gouvernance | Une politique documentée de sécurité informatique a été mise en œuvre et est mise à jour à intervalles réguliers. |
| EG-GOV-11 | Cadre de gouvernance | La Partie Contractante dispose d'un programme ou d'un processus de gestion des vulnérabilités. |

| | | |
|---|---|---|
| EG-GOV-12 | Cadre de gouvernance | La Partie Contractante a mis en œuvre et tient à jour un processus relatif à la manipulation des supports de données et du matériel de transport de données qui répond tant aux besoins de l'entreprise qu'aux exigences réglementaires et qui comprend une marche à suivre quand ces dispositifs sont en fin de vie ou doivent être réutilisés ou réhabilités. |
| EG-HR-1 | Sécurité des ressources humaines | La Partie Contractante exige de ses nouveaux employés qu'ils signent une entente de non-divulgation et qu'ils prennent connaissance de ses politiques de sécurité informatique. |
| EG-HR-2 | Sécurité des ressources humaines | La Partie Contractante dispose d'un programme de sensibilisation à la sécurité informatique. |
| EG-HR-3 | Sécurité des ressources humaines | Tous les employés et consultants de la Partie Contractante sont tenus de suivre une formation de sensibilisation à la sécurité informatique. Cette formation est donnée à intervalles réguliers et la participation est vérifiée. |
| EG-CONSU-1 | Consultants | Les relations contractuelles de la Partie Contractante avec ses consultants sont gérées et documentées. |
| EG-CONSU-2 | Partie contractante, consultants et sous-traitants | En ce qui concerne les Données de Concordia, la Partie Contractante, ses consultants et sous-traitants auront un accès limité à ce qui est strictement nécessaire pour permettre à la Partie Contractante de s'acquitter de ses obligations en vertu du Contrat et conformément aux termes de l'Addenda. |
| EG-SEC-1 | Sécurité de la solution | La solution de la Partie Contractante ne nécessite pas l'accès aux données de localisation ou aux données GPS de Concordia. |
| EG-SEC-2 | Sécurité de la solution | La Partie Contractante dispose d'un pare-feu d'applications Web. |
| EG-SEC-3 | Sécurité de la solution | Tous les postes de travail de la Partie Contractante sont dotés d'un antivirus et la distribution des signatures est gérée de manière centralisée. |
| EG-SEC-4 | Sécurité de la solution | Si la solution de la Partie Contractante est une application, elle est disponible auprès d'une source fiable (p. ex. App Store, Google Play Store, portail de l'entreprise). |
| EG-SEC-5 | Sécurité de la solution | Les tâches d'administration de la sécurité, d'administration du système et d'utilisation des fonctionnalités de base sont en tout temps distinctes. |
| EG-SEC-6 | Sécurité de la solution | Les environnements de développement, de test et d'exploitation sont strictement séparés. |
| EG-SEC-7 | Sécurité de la solution | Les développeurs de la Partie Contractante sont formés aux techniques de codage sécurisé. |
| EG-SEC-8 | Sécurité de la solution | La solution de la Partie Contractante a été développée en utilisant des techniques de codage sécurisé. |

| | | |
|---|---|---|
| EG-SEC-9 | Sécurité de la solution | Le code de la Partie Contractante a fait l'objet d'une analyse statique ou d'un test statique de sécurité de l'application avant d'être publié. |
| EG-SEC-10 | Sécurité de la solution | Les processus de test des logiciels (dynamiques ou statiques) de la Partie Contractante sont établis et suivis. |
| EG-SEC-11 | Sécurité de la solution | Des tests de pénétration sont effectués à intervalles réguliers. |
| EG-DATH-1 | Hébergement des données | Tous les fournisseurs d'hébergement de la Partie Contractante (Centre de Données) disposent d'un rapport SOC 2 de type 2. |
| EG-NSEC-1 | Sécurité des réseaux | La Partie Contractante utilise un pare-feu moderne à sécurité positive et configuré pour refuser par défaut. |
| EG-NSEC-2 | Sécurité des réseaux | La Partie Contractante dispose d'une politique relative aux demandes de changements au pare-feu dans laquelle les rôles et les responsabilités sont décrits. |
| EG-NSEC-3 | Sécurité des réseaux | La Partie Contractante utilise un système de détection ou de prévention des intrusions qui fonctionne au niveau du réseau et de l'ordinateur. |
| EG-NSEC-4 | Sécurité des réseaux | La Partie Contractante surveille les intrusions 24 heures sur 24, 7 jours sur 7 et 365 jours par an. |
| EG-NSEC-5 | Sécurité des réseaux | Les journaux d'audit de la Partie Contractante sont disponibles relativement à toutes les modifications apportées au réseau, au pare-feu et aux systèmes de détection et de prévention des intrusions. |
| EG-NSEC-6 | Sécurité des réseaux | L'authentification multifactorielle doit être utilisée, y compris pour l'accès privilégié à la solution et aux composants connexes. |
| EG-A&C-1 | Audits et certifications | La Partie Contractante effectue et documente les audits internes dictés par les politiques et procédures. |
| EG-A&C-2 | Audits et certifications | La Partie Contractante effectue et documente les audits externes dictés par les politiques et procédures. |
| EG-A&C-3 | Audits et certifications | Des audits de sécurité des entreprises avec lesquelles la Partie Contractante échange des données sont effectués dans le cadre d'un processus global de gestion des tiers. |
| EG-INC-1 | Gestion des incidents | La Partie Contractante dispose d'un processus officiel de gestion des incidents. |
| EG-INC-2 | Gestion des incidents | La Partie Contractante dispose d'une équipe interne ou externe d'intervention en cas d'incident. |
| EG-INC-3 | Gestion des incidents | La Partie Contractante a la capacité de répondre aux incidents 24 heures sur 24, 7 jours sur 7 et 365 jours par an. |

| | | |
|---|---|---|
| EG-INC-4 | Gestion des incidents | En cas de perte, de destruction, de consultation, de modification ou d'utilisation de renseignements sensibles ou confidentiels ou de Données de Concordia, y compris des Renseignements Personnels (un **« Incident de Sécurité »**), la Partie Contractante doit fournir immédiatement à Concordia les renseignements suivants au sujet de l'incident :<br>- Où et quand l'incident s'est-il produit?<br>- Qui l'a signalé, à qui et quand?<br>- Quels renseignements ou données étaient visés?<br>- Qui a fourni les renseignements ou les données?<br>- Depuis combien de temps les renseignements, les données ou le dispositif électronique sont-ils vulnérables à un accès non autorisé et qui a pu y accéder de cette manière?<br>- Y a-t-il des renseignements ou des données qui ont été extraits ou dont l'intégrité a été compromise? L'intégrité d'un dispositif électronique a-t-elle été compromise? |
| EG-VULN-1 | Gestion des vulnérabilités | Les systèmes et applications de la Partie Contractante font l'objet d'une analyse externe visant à détecter les vulnérabilités à intervalles réguliers. |
| EG-VULN-2 | Gestion des vulnérabilités | Les systèmes et applications de la Partie Contractante ont fait l'objet d'une évaluation de sécurité par un tiers au cours de l'année écoulée. |
| EG-VULN-3 | Gestion des vulnérabilités | Les systèmes et applications de la Partie Contractante sont analysés à l'aide d'un compte utilisateur authentifié afin de détecter et de corriger les vulnérabilités avant le lancement d'une nouvelle version. |
| EG-VULN-4 | Gestion des vulnérabilités | La Partie Contractante surveille les vulnérabilités des applications Web (p. ex. attaques par injection SQL, scripts intersites et falsification de requêtes intersites) et s'en protège. |
| EG-VULN-5 | Gestion des vulnérabilités | La Partie Contractante a fixé un échéancier pour apporter des correctifs en fonction de la gravité des vulnérabilités établie d'après le système d'évaluation CVSS. |
| EG-VULN-6 | Gestion des vulnérabilités | La Partie Contractante, ou un partenaire externe, gère activement le déploiement des correctifs et les processus associés (mises à jour de logiciels, correctifs de sécurité). |
| C-GOV-1 | Cadre de gouvernance | La Partie Contractante a nommé un administrateur de la sécurité des données. |
| C-GOV-2 | Cadre de gouvernance | La Partie Contractante dispose d'une politique documentée en matière de confidentialité des données. |
| C-ACC-1 | Accès et authentification | Le contrôle de l'accès se fonde sur les rôles, les attributs ou les politiques. |

| | | |
|---|---|---|
| C-ACC-2 | Accès et authentification | Le cycle de vie complet de l'accès aux renseignements confidentiels, y compris aux Renseignements Personnels, est encadré et documenté. |
| C-ACC-3 | Accès et authentification | L'accès privilégié fait l'objet d'une gestion et de contrôles différents de ceux de l'accès standard. |
| C-ACC-6 | Accès et authentification | La complexité des mots de passe de Concordia est prise en charge par la solution de la Partie Contractante. |
| C-ACC-9 | Accès et authentification | Tous les mots de passe stockés sont chiffrés. |
| C-ENC-1 | Chiffrement | Toutes les Données de Concordia, y compris les Renseignements Personnels, sont chiffrées qu'elles soient au repos ou en mouvement. La solution de la Partie Contractante doit utiliser un chiffrement SSL à 256 bits ou un protocole plus récent pour la transmission de renseignements entre l'utilisateur et l'application relativement à tout module ou sous-module contenant des renseignements non publics. Le chiffrement doit être maintenu, que les données soient au repos ou en mouvement. |
| C-ENC-2 | Chiffrement | Toutes les copies de sauvegarde de la Partie Contractante doivent être chiffrées selon des normes professionnelles et le chiffrement doit au minimum correspondre au protocole SSL à 256 bits. |
| C-DATH-1 | Hébergement des données | Les Données de Concordia sont stockées au Québec ou dans un des États ou une juridiction autorisée se retrouvant à l'ANNEXE B de l'Addenda. |
| C-PHY-2 | Sécurité physique | L'accès physique est contrôlé et sécurisé au moyen de cartes d'identification, de caméras et de gardes de sécurité. Chaque accès est enregistré de manière à pouvoir être retracé et consulté en tout temps. |
| C-PHY-3 | Sécurité physique | La Partie Contractante applique en permanence une politique de mise en sécurité des documents et de verrouillage des écrans. |

**ANNEXE B**

**TERRITOIRES ACCEPTÉS**

**Au 20 septembre 2023**

Canada
États-Unis - dans la mesure où la Partie Contractante certifie sa participation au cadre de protection des données UE-USA et qu'il est enregistré comme participant au programme.
Israël
Autriche
Jersey
Royaume-Uni
Belgique
Bulgarie
Croatie
Chypre
République tchèque
Danemark
Estonie
Finlande
France
Allemagne
Grèce
Hongrie
Irlande
Italie
Lettonie
Lituanie
Luxembourg
Malte
Pays-Bas
Pologne
Portugal
Roumanie
Slovaquie
Slovénie
Espagne
Suède
Islande
Liechtenstein
Norvège
Andorre
Nouvelle-Zélande
Corée du Sud
Guernsey
Île de Man
îles Féroé
Japon
Suisse