Gordon SERVICE ALIMENTAIRE	**Objet :** Contrat nord-américain de traitement des données **Propriétaire :** Responsable de la protection de la vie privée	**Entrée en vigueur :** 1er avril 2025 **Remplace la politique datée du :** 19 février 2024
	Type : Révision complète ( ) Révision partielle (X) Nouveau document ( )	**Approuvé par :** Responsable de la protection de la vie privée

Contrat nord-américain de traitement des données

Le présent contrat de traitement des données (le «**Contrat**») s'applique à tout fournisseur de marchandises à Service alimentaire Gordon (le «**Fournisseur**») qui a signé une ou plusieurs Ententes avec Gordon Food Service, Inc. et Service alimentaire Gordon Canada ltée (collectivement, «**Service alimentaire Gordon**»). Le Fournisseur et Service alimentaire Gordon sont désignés dans le présent document sous les termes «**Partie**» ou «**Parties**», selon le contexte.

1. Principales définitions

1.1 «**Entreprises affiliées**» désigne toute entité qui contrôle directement ou indirectement Service alimentaire Gordon, qui est contrôlée par Service alimentaire Gordon, ou qui est placée sous un contrôle commun avec Service alimentaire Gordon. «**Contrôle ou contrôler**», pour l'application de cette définition, désigne la propriété ou le contrôle direct ou indirect de plus de 50 % des intérêts avec droit de vote de l'entité concernée.

1.2 «**Entente**» désigne une ou plusieurs ententes entre le Fournisseur et Service alimentaire Gordon en vertu desquelles le Fournisseur peut accéder aux RP couverts, les recueillir ou les traiter.

1.3 «**RP couverts**» désigne les Renseignements personnels fournis au Fournisseur par Service alimentaire Gordon ou recueillis pour le compte de Service alimentaire Gordon, ceux recueillis par le Fournisseur pour le compte de Service alimentaire Gordon ou ceux mis à la disposition du Fournisseur d'une autre manière en vertu des Ententes.

1.4 «**Renseignements personnels**» désigne a) tout renseignement relatif à un consommateur ou à un ménage et b) tout renseignement qui entre dans le champ d'application des «données personnelles», des «renseignements personnels» ou des «données à caractère personnel» (ou tout concept ou toute définition matériellement similaire) en vertu des Lois sur la protection des renseignements personnels.

1.5 «**Format portable**» désigne, dans la mesure où cela est techniquement possible, un format structuré, couramment utilisé, lisible par machine et facilement utilisable qui permet au consommateur de transmettre sans entrave les RP couverts à une autre entité ou à un autre responsable du traitement, comme le prévoient les Lois sur la protection des renseignements personnels.

1.6 «**Lois sur la protection des renseignements personnels**» désigne toutes les lois et tous les règlements sur la protection des renseignements personnels et des données applicables au traitement des RP couverts dans le cadre de l'Entente, y compris, mais sans s'y limiter, celles des États-Unis et du Canada, la *Consumer Privacy Act* de la Californie, la *Privacy Rights Act* de la Californie, la *Consumer Data Protection Act* de la Virginie, la *Privacy Act* du Colorado, la *Loi sur la protection des renseignements personnels et les documents électroniques* («**LPRPDE**»), la *Personal Information Protection Act* de la Colombie-Britannique («**PIPA de la C.-B.**»), la *Personal Information*

Gordon SERVICE ALIMENTAIRE	**Objet :** Contrat nord-américain de traitement des données **Propriétaire :** Responsable de la protection de la vie privée	**Entrée en vigueur :** 1er avril 2025 **Remplace la politique datée du :** 19 février 2024
	Type : Révision complète ( ) Révision partielle (X) Nouveau document ( )	**Approuvé par :** Responsable de la protection de la vie privée

Protection Act de l'Alberta («**PIPA de l'Alberta**») et la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec («**LPRPSP du Québec**»), dans chaque cas quand et si elles sont applicables au traitement des RP couverts par le Fournisseur en vertu du présent contrat.

1.7 Les termes «consommateur», «demande vérifiable du consommateur», «données sensibles», «entreprise», «fins commerciales», «fournisseur de services», «partage», «renseignements personnels sensibles», «responsable du traitement», «sous-traitant», «traitement» et «vente» ont la désignation qui leur est donnée dans les Lois sur la protection des renseignements personnels. En cas de conflit de désignation des termes dans les Lois sur la protection des renseignements personnels, les Parties conviennent que les désignations de chaque loi s'appliquent.

1.8 «Services» désigne les services fournis par le Fournisseur à Service alimentaire Gordon qui sont précisés dans les Ententes.

2. Termes relatifs au traitement de données

2.1 Relation entre les Parties. Les Parties conviennent que Service alimentaire Gordon est la seule Partie qui détermine les objectifs et les moyens de traitement des RP couverts en tant qu'«entreprise» ou «responsable du traitement», et que le Fournisseur traite les RP couverts en tant que «fournisseur de services» ou «sous-traitant» pour le compte de Service alimentaire Gordon.

2.2 Respect des obligations. Le Fournisseur déclare et garantit qu'il, ainsi que ses employés, spécialistes et sous-traitants ultérieurs, a) se conformeront aux Lois sur la protection des renseignements personnels et au présent contrat lors du traitement des RP couverts, et b) fourniront à Service alimentaire Gordon toute aide raisonnablement demandée pour permettre à Service alimentaire Gordon de remplir ses propres obligations en vertu des Lois sur la protection des renseignements personnels. Sur demande raisonnable de Service alimentaire Gordon, le Fournisseur doit mettre à la disposition de Service alimentaire Gordon tous les renseignements en sa possession qui sont raisonnablement nécessaires pour démontrer qu'il respecte le présent paragraphe.

Le Fournisseur s'assurera que les membres de son personnel, lorsqu'ils sont affectés à la prestation de services ou à la fourniture de produits livrables dans le cadre d'un énoncé de travaux, ou lorsqu'ils visitent ou accèdent aux installations de Service alimentaire Gordon i) respectent les politiques, procédures et règles internes de Service alimentaire Gordon en vigueur relatives à la protection de l'environnement, à la santé, à la sécurité et au travail, y compris les exigences de sécurité des données et les exigences et pratiques de sécurité pour les contractants de Service alimentaire Gordon, ii) respectent toutes les conditions régissant l'accès aux systèmes d'information ou de communication de Service alimentaire Gordon, y compris mais sans s'y limiter, les ordinateurs hôtes et personnels, les réseaux d'information ou de communication internes ou externes (y compris les systèmes de messagerie vocale, Internet/Intranet et de courriel), les systèmes d'exploitation, les systèmes de base de données, ou le matériel et les logiciels directement ou indirectement accessibles à partir des systèmes de Service alimentaire Gordon, et le Contrat

de traitement des données de Service alimentaire Gordon (https://gfs.ca/fr-ca/entente-sur-le-traitement-des-donnees), iii) se conforment à toutes les demandes raisonnables du personnel de Service alimentaire Gordon, le cas échéant, concernant la conduite personnelle et professionnelle, et iv) se comportent de manière professionnelle et sérieuse. Service alimentaire Gordon fournira au Fournisseur, à la demande de ce dernier, une copie à jour de ces politiques, procédures et règles internes, sous réserve d'une entente de confidentialité.

2.3 Suppression ou retour de RP couverts. Sur demande écrite de Service alimentaire Gordon ou en cas de résiliation d'une Entente, le Fournisseur cessera de traiter les RP couverts sans retard injustifié. Dans les soixante (60) jours suivant une demande écrite de Service alimentaire Gordon ou la résiliation d'une Entente, le Fournisseur détruira les RP couverts, sauf instruction contraire de Service alimentaire Gordon; à condition qu'avant cette destruction, le Fournisseur renvoie à Service alimentaire Gordon tous les RP couverts en sa possession, ou les mette à sa disposition, pendant une période de soixante (60) jours afin que Service alimentaire Gordon puisse en effectuer un téléchargement complet et sécurisé. Le Fournisseur peut conserver les RP couverts dans la mesure et pendant la période requises par la loi applicable, à condition que le Fournisseur a) informe Service alimentaire Gordon de ces obligations (sauf si cela lui est interdit) et b) garantisse la confidentialité permanente de tous ces RP couverts. Sur demande écrite de Service alimentaire Gordon ou dans les soixante (60) jours suivant la résiliation d'une Entente, le Fournisseur fournira à Service alimentaire Gordon une certification écrite attestant qu'il s'est conformé à ces obligations de suppression.

2.4 Évaluations. Le cas échéant, le Fournisseur doit fournir à Service alimentaire Gordon, sur demande raisonnable de cette dernière, l'aide et les renseignements raisonnablement nécessaires pour permettre à Service alimentaire Gordon d'effectuer des évaluations des facteurs relatifs à la vie privée en vertu des Lois sur la protection des renseignements personnels.

3. Limites d'utilisation des RP couverts

3.1 Portée limitée du traitement. Le Fournisseur traitera les RP couverts uniquement selon les instructions données dans les Ententes, le présent contrat et toute autre instruction écrite fournie par Service alimentaire Gordon qui est compatible avec les conditions de l'Entente, dans chaque cas pour la durée de la fourniture des Services à Service alimentaire Gordon.

3.2. Restrictions en matière de données. Le Fournisseur ne fera pas ce qui suit : a) vendre ou partager les RP couverts, b) recueillir, conserver, utiliser ou divulguer les RP couverts à des fins autres que les fins commerciales précisées dans les Ententes, telles que la fourniture des Services à Service alimentaire Gordon, c) conserver, utiliser ou divulguer les RP couverts en dehors de la relation commerciale directe avec Service alimentaire Gordon, d) combiner les RP couverts avec d'autres Renseignements personnels, y compris pour l'augmentation des données ou le profilage, sauf autorisation expresse en vertu des Lois sur la protection des renseignements personnels pour les

fonctions du Fournisseur (telles que la prévention de la fraude, ou lorsque la loi l'exige), et/ou e) exporter les RP couverts en dehors du pays à partir duquel ils ont été fournis ou recueillis sans l'accord écrit préalable de Service alimentaire Gordon. Le Fournisseur a le droit d'utiliser des Données agrégées (telles que définies ci-dessous) à des fins commerciales internes, moyennant l'accord écrit de Service alimentaire Gordon (un courriel suffit), à condition que le Fournisseur n'utilise ni ne divulgue les Données agrégées à des fins commerciales. «**Données agrégées**» désigne les RP couverts qui sont dépersonnalisés et agrégés conformément à la loi applicable, de sorte que les renseignements ne sont pas liés ou ne peuvent raisonnablement être liés à Service alimentaire Gordon ou à ses clients.

3.3 Droits d'audit. Service alimentaire Gordon ou, au choix de Service alimentaire Gordon, un tiers raisonnablement désigné par Service alimentaire Gordon pour agir au nom de cette dernière et acceptable pour le Fournisseur, a le droit de vérifier la conformité du Fournisseur au présent contrat par des mesures pouvant inclure des examens manuels, des analyses automatisées, des tests de pénétration, des évaluations régulières, des audits ou des tests techniques ou opérationnels. Le Fournisseur doit coopérer pleinement à tout audit entrepris par Service alimentaire Gordon, à condition que cet audit n'interfère pas de manière déraisonnable avec le déroulement normal des activités du Fournisseur. Le Fournisseur doit fournir les résultats de l'audit avec suffisamment de détails pour comprendre les conclusions, les risques associés et les mesures correctives nécessaires. À moins d'indication contraire dans la loi, Service alimentaire Gordon doit avertir le Fournisseur au moins dix (10) jours à l'avance de tout audit et ne doit pas auditer le Fournisseur plus de deux fois par période de douze mois. Service alimentaire Gordon peut cependant procéder à un audit à tout moment en cas d'Incident de sécurité, à la demande d'un organisme de réglementation ou dans le cadre de la défense des droits légaux de Service alimentaire Gordon. Si les résultats démontrent un manquement important au respect du présent contrat par le Fournisseur, ce dernier travaillera de bonne foi avec Service alimentaire Gordon pour remédier à ces problèmes à la satisfaction de Service alimentaire Gordon.

3.4 Mesures correctives relatives à la conformité; droits de résiliation. Le Fournisseur s'engage à informer Service alimentaire Gordon sans retard injustifié s'il détermine qu'il n'est plus en mesure de respecter ses obligations en vertu des Lois sur la protection des renseignements personnels. Après avoir reçu un avis du Fournisseur conformément au présent paragraphe, Service alimentaire Gordon peut demander au Fournisseur de prendre des mesures raisonnables et appropriées pour remédier à l'utilisation non autorisée des RP couverts ou résilier les Ententes.

3.5 Désignation des sous-traitants ultérieurs.

1. Le Fournisseur a le droit d'avoir recours à des sous-traitants ultérieurs dans le cadre de l'exécution de ses Services en vertu du présent contrat (les «**Sous-traitants ultérieurs**»). Avant le début de tout traitement de RP couverts par le Fournisseur en vertu du présent contrat, le Fournisseur doit fournir à Service alimentaire

Gordon la liste actuelle des Sous-traitants ultérieurs traitant les RP couverts pour chaque Service applicable, y compris une description de leurs activités de traitement et leurs pays d'emplacement. Le Fournisseur doit aviser Service alimentaire Gordon par écrit (un courriel suffit) de tout changement concernant l'ajout ou le remplacement de Sous-traitants ultérieurs traitant les RP couverts. De plus, le Fournisseur doit s'assurer que ses Sous-traitants ultérieurs qui traitent les RP couverts pour son compte acceptent par écrit les mêmes restrictions et exigences que celles qui s'appliquent au Fournisseur dans le présent contrat et les Ententes relatives aux RP couverts. Le Fournisseur reste entièrement responsable vis-à-vis de Service alimentaire Gordon des actes et omissions de ses Sous-traitants ultérieurs.

2. **Droit d'opposition.** Service alimentaire Gordon peut s'opposer à la désignation par le Fournisseur d'un nouveau Sous-traitant ultérieur pour des motifs raisonnables liés à la protection des données en avisant par écrit le Fournisseur dans les trente (30) jours civils suivant la réception de l'avis conformément à la disposition 3.5. En cas d'opposition de Service alimentaire Gordon, les Parties discuteront de bonne foi des préoccupations de Service alimentaire Gordon en vue de parvenir à une solution commercialement raisonnable. Si aucune solution ne peut être négociée, le Fournisseur, à sa seule discrétion, ne désignera pas le Sous-traitant ultérieur ou autorisera Service alimentaire Gordon à résilier les Ententes, en remboursant dans ce cas à Service alimentaire Gordon tous les frais non utilisés et payés d'avance.

3.6 Réidentification. Le Fournisseur ne réidentifiera pas, et n'autorisera pas ses Sous-traitants ultérieurs à réidentifier les données dépersonnalisées, anonymisées ou pseudonymisées dérivées des RP couverts qui sont traités par le Fournisseur pour le compte de Service alimentaire Gordon, sauf instruction écrite de Service alimentaire Gordon (un courriel suffit).

4. Demandes des consommateurs

4.1 Traitement des demandes des consommateurs. Le Fournisseur mettra en œuvre et maintiendra des procédures et des processus adéquats pour répondre aux demandes de Service alimentaire Gordon concernant l'accès, la correction ou la suppression de RP couverts détenus par le Fournisseur. Dans les dix (10) jours civils suivant une demande écrite de Service alimentaire Gordon (un courriel suffit), le Fournisseur doit, le cas échéant : a) effacer ou détruire, ou faire effacer ou détruire, des éléments précis des RP couverts de manière sécurisée, y compris toute copie de ces RP couverts conservée par les Sous-traitants ultérieurs du Fournisseur; b) fournir les renseignements demandés par Service alimentaire Gordon concernant le traitement des RP couverts par le Fournisseur; c) fournir les éléments précis des RP couverts que le Fournisseur et/ou l'un de ses Sous-traitants ultérieurs ont recueillis ou obtenus d'une autre manière au sujet du consommateur pour le compte de Service alimentaire Gordon dans un Format portable; d) modifier des éléments précis des RP couverts, ou demander à ses Sous-traitants ultérieurs de le faire; ou e) limiter le traitement des RP couverts définis dans les Lois sur la protection des renseignements

personnels en tant que «renseignements personnels sensibles» ou «données sensibles», conformément aux instructions de Service alimentaire Gordon.

4.2 Renvoi de demandes directes. Le Fournisseur doit renvoyer à Service alimentaire Gordon les demandes de consommateurs applicables soumises directement au Fournisseur concernant les RP couverts et ne pas répondre à ces demandes autrement qu'en informant le demandeur que la demande est renvoyée à Service alimentaire Gordon.

5. Contrôles de sécurité

5.1 Obligation de confidentialité. Le Fournisseur, ainsi que ses employés, ses spécialistes et ses Sous-traitants ultérieurs sont soumis à une obligation de confidentialité en ce qui concerne les RP couverts.

5.2 Mesures de sécurité. Le Fournisseur doit mettre en œuvre et maintenir des mesures, procédures et pratiques de sécurité techniques et organisationnelles raisonnables, de même qu'adaptées à la nature des RP couverts, afin de protéger ces RP couverts contre tout accès non autorisé ou toute destruction, utilisation, modification ou divulgation non autorisées (les «**Mesures de sécurité**»). Ces Mesures de sécurité doivent respecter ou dépasser les normes industrielles applicables (p. ex. NIST Cybersecurity Framework) et toute obligation énoncée dans les Ententes ou dans la loi applicable. Le Fournisseur doit se conformer aux exigences de l'**Annexe sur la sécurité** jointe au présent document.

5.3 Incident de sécurité.

a) Avis. Le Fournisseur informera Service alimentaire Gordon dans les vingt-quatre (24) heures de l'accès, de la destruction, de l'utilisation, de la modification ou de la divulgation non autorisés soupçonnés par le Fournisseur (chacun étant un «**Incident de sécurité**») de tout RP couvert. Le Fournisseur enverra un avis par courriel à Service alimentaire Gordon avec accusé de réception à **privacy@gfs.com** ainsi qu'une copie à **legal@gfs.com** et à la personne-ressource principale du Fournisseur chez Service alimentaire Gordon. Le Fournisseur doit fournir à Service alimentaire Gordon le nom et les coordonnées d'un de ses employés qui servira de personne-ressource principale de Service alimentaire Gordon en matière de sécurité et qui sera disponible pour aider Service alimentaire Gordon à s'acquitter de ses obligations liées à un Incident de sécurité, vingt-quatre (24) heures par jour, sept (7) jours par semaine. L'avis écrit fourni conformément au présent alinéa comprendra un bref résumé des faits disponibles, de l'état d'avancement de l'enquête du Fournisseur et, s'il est connu et applicable, du nombre potentiel de personnes dont les données ont été divulguées.

b) Gestion et prise de mesures correctives. Le Fournisseur assurera sa collaboration et fournira à Service alimentaire Gordon toute information raisonnablement demandée par Service alimentaire Gordon concernant cet Incident de sécurité, y compris en fournissant à Service alimentaire Gordon ou à son enquêteur judiciaire désigné raisonnablement acceptable par le Fournisseur un accès physique aux installations et opérations affectées, en

facilitant les entretiens et en mettant à disposition les dossiers, registres et autres documents pertinents raisonnablement requis par Service alimentaire Gordon. Le Fournisseur doit immédiatement régler tout Incident de sécurité à ses frais, conformément aux lois applicables. Le Fournisseur doit rembourser à Service alimentaire Gordon les coûts réels encourus par Service alimentaire Gordon pour répondre à un Incident de sécurité et atténuer les dommages causés par celui-ci, y compris tous les coûts d'avis et de mesures correctives. Sauf si la loi l'exige, le Fournisseur n'informera aucun tiers d'un Incident de sécurité sans l'accord écrit de Service alimentaire Gordon. De plus, le Fournisseur accepte que Service alimentaire Gordon ait le droit exclusif de déterminer la pertinence et le contenu de l'avis de l'Incident de sécurité, ainsi que la nature et l'étendue des mesures correctives.

5.4 Contrôle. Sur demande et sur une base annuelle, le Fournisseur fournira à Service alimentaire Gordon les résultats de tout audit effectué (p. ex. SOC1, SOC2, ISO27001, etc.) par le Fournisseur ou pour son compte qui évalue l'efficacité du programme de sécurité de l'information du Fournisseur en ce qui concerne la sécurité et la confidentialité des RP couverts (le «**Rapport sur les contrôles**»). Le Fournisseur doit veiller à ce que chaque Sous-traitant ultérieur mette à la disposition de Service alimentaire Gordon un Rapport sur les contrôles sur une base annuelle ou à la suite d'un Incident de sécurité.

6. Enquêtes

6.1 Avis d'une enquête réglementaire. Le Fournisseur doit informer Service alimentaire Gordon de toute enquête ou correspondance réglementaire concernant les RP couverts (une «**Enquête**») dans les trois (3) jours civils suivant la réception de l'avis d'Enquête. Le Fournisseur doit fournir à Service alimentaire Gordon toutes les copies de la correspondance et des documents relatifs à l'Enquête sans retard injustifié.

6.2 Réponse à l'Enquête. Le Fournisseur ne doit divulguer aucun renseignement confidentiel de Service alimentaire Gordon ou d'une partie affiliée à l'autorité compétente sans le consentement écrit préalable de Service alimentaire Gordon. Le Fournisseur doit prendre toutes les autres mesures nécessaires pour répondre à l'Enquête ou y remédier de manière adéquate et dans les plus brefs délais.

7. Divers

7.1 Divisibilité. Si une disposition du présent contrat est jugée nulle par un tribunal, cette disposition sera considérée comme séparable des autres dispositions du présent contrat, et le reste du Contrat prendra effet, comme si les Parties n'avaient pas inclus la disposition séparée.

7.2 Saisie ou confiscation. Si des RP couverts peuvent faire l'objet d'une saisie ou d'une confiscation, d'une procédure d'insolvabilité (y compris une vente) ou de concordat, de tout autre événement, ou d'une autre mesure prise par un tiers, le Fournisseur doit en informer Service alimentaire Gordon avec un préavis raisonnable. De plus,

le Fournisseur doit informer le tiers que la souveraineté et la propriété des RP couverts reviennent à Service alimentaire Gordon.

7.3 Applicabilité. Toutes les déclarations, garanties et indemnités doivent demeurer en vigueur après la résiliation ou l'expiration du présent contrat. Tous les droits et privilèges d'une Partie, dans la mesure où ils sont équitablement attribuables à des conditions ou événements survenant ou existant au moment de la résiliation ou de l'expiration du présent contrat ou avant, demeurent en vigueur après la résiliation et peuvent être appliqués par cette Partie.

7.4 Généralités. Sauf mention expresse dans le présent document, les conditions des Ententes demeurent inchangées et pleinement en vigueur. En cas de conflit entre les conditions des Ententes et celles du présent contrat, les conditions du présent contrat prévalent, à moins que les Ententes ne contiennent un renvoi particulier à la disposition du Contrat destiné à être modifié. Les en-têtes sont utilisés pour des raisons de commodité et n'affectent pas l'interprétation des conditions du présent contrat.

Gordon SERVICE ALIMENTAIRE	**Objet :** Contrat nord-américain de traitement des données **Propriétaire :** Responsable de la protection de la vie privée	**Entrée en vigueur :** 1er avril 2025 **Remplace la politique datée du :** 19 février 2024
	Type : Révision complète ( ) Révision partielle (X) Nouveau document ( )	**Approuvé par :** Responsable de la protection de la vie privée

ANNEXE SUR LA SÉCURITÉ

1. Politiques et procédures. Le Fournisseur doit maintenir et assurer la conformité avec ses politiques et procédures écrites de gestion de la sécurité (les «**Politiques du Fournisseur**») afin de prévenir, détecter, limiter et corriger les violations des mesures prises pour protéger la confidentialité, de même que l'intégrité ou la disponibilité des systèmes d'information du Fournisseur qui servent à accéder aux renseignements confidentiels de Service alimentaire Gordon, à les stocker, à les traiter ou à les transférer (les «**Systèmes du Fournisseur**»). Les Politiques du Fournisseur doivent au minimum : i) dans la mesure où le Fournisseur a accès aux RP couverts, traiter à tout moment les RP couverts comme des renseignements hautement sensibles; ii) inclure un programme officiel de gestion des risques qui comprend des évaluations périodiques des risques; et iii) fournir un cadre adéquat de contrôles qui protègent les Systèmes du Fournisseur, y compris mais sans s'y limiter, tout matériel ou logiciel soutenant Service alimentaire Gordon et les renseignements confidentiels de Service alimentaire Gordon.

2. Évaluations de sécurité. Le Fournisseur doit effectuer et documenter chaque année une évaluation de la sécurité technique de ses Politiques et Systèmes afin de s'assurer qu'il continue à respecter les obligations énoncées dans la présente annexe et celles imposées par la loi. Ces évaluations doivent garantir que les renseignements confidentiels de Service alimentaire Gordon sont stockés de manière confidentielle et sécurisée dans les Systèmes du Fournisseur et évaluer la maintenance et la structure des Systèmes du Fournisseur.

3. Certifications. Sur demande écrite de Service alimentaire Gordon, le Fournisseur doit fournir à Service alimentaire Gordon les résultats de tout audit réalisé par le Fournisseur ou pour son compte qui évalue l'efficacité du programme de sécurité de l'information du Fournisseur en ce qui concerne la sécurité et la confidentialité des RP couverts partagés dans le cadre de l'Entente (le «**Rapport sur les contrôles**»). Le Fournisseur doit veiller à ce que chaque Sous-traitant ultérieur mette à la disposition de Service alimentaire Gordon un Rapport sur les contrôles sur une base annuelle ou à la suite d'un Incident de sécurité.

4. Sécurité physique. Le Fournisseur doit maintenir des contrôles de sécurité physique appropriés (y compris des contrôles des installations et de l'environnement) afin d'empêcher l'accès physique non autorisé aux Systèmes du Fournisseur.

5. Limites d'accès. Le Fournisseur doit mettre en œuvre des contrôles d'accès appropriés limitant l'accès aux RP couverts aux employés, spécialistes et Sous-traitants ultérieurs qui ont besoin de connaître ces renseignements pour s'acquitter des obligations qui leur incombent en vertu des Ententes.

6. Registres de contrôle d'accès des visiteurs. Le Fournisseur doit tenir des registres de contrôle d'accès des visiteurs (le «**Registre des visiteurs**») et veiller à ce que ces visiteurs soient accompagnés lorsqu'ils se trouvent dans toute installation permettant un accès physique ou virtuel aux Systèmes du Fournisseur. Il doit également conserver le Registre des visiteurs dans un endroit sécurisé pendant au moins trois (3) mois.

7. Contrôles du périmètre. Le Fournisseur doit maintenir des contrôles raisonnables du périmètre du réseau, tels que des pare-feux, à toutes les connexions du périmètre aux Systèmes du Fournisseur.

8. Gestion et tests de la vulnérabilité. Le Fournisseur doit utiliser des processus raisonnables de gestion de la vulnérabilité pour atténuer les risques liés à la sécurité des données, y compris mais sans s'y limiter, des mesures d'atténuation pour résoudre les problèmes identifiés par le Fournisseur, Service alimentaire Gordon, ou comme l'exige la loi. Le Fournisseur doit autoriser Service alimentaire Gordon et ses tiers approuvés à effectuer des tests de vulnérabilité dans le but d'identifier les failles de sécurité accessibles au public dans la fonctionnalité Web du Fournisseur utilisée par Service alimentaire Gordon et ses clients, ainsi que les clients et les contractants indépendants, sous réserve que Service alimentaire Gordon fournisse un préavis raisonnable et que le Fournisseur obtienne tous les consentements nécessaires de la part de son fournisseur de plateforme d'hébergement.

9. Renforcement de la sécurité des systèmes. Les paramètres de configuration du Fournisseur pour ses systèmes comprennent des procédures visant à désactiver tous les services inutiles sur les appareils et les serveurs et doivent être appliqués à tous les Systèmes du Fournisseur qui accèdent aux renseignements confidentiels de Service alimentaire Gordon, les transmettent ou les stockent.

10. Gestion des correctifs. Le Fournisseur doit établir et respecter des politiques de correctifs de systèmes qui garantissent que tous ses systèmes sont maintenus à un niveau de correctif stable et à jour.

11. Détection de virus. Le Fournisseur doit installer un logiciel de détection de codes malveillants commercialement raisonnable, comprenant des détecteurs de virus et de logiciels malveillants, sur tous les systèmes vulnérables aux logiciels malveillants qui servent à accéder aux renseignements confidentiels de Service alimentaire Gordon, à les traiter ou à les stocker. Le Fournisseur doit également maintenir à jour les signatures de virus.

12. Registres. Le Fournisseur doit tenir des registres qui identifient de manière unique les utilisateurs individuels et leur accès aux systèmes associés et qui identifient les activités tentées ou exécutées par ces utilisateurs. Tous les systèmes créant des registres doivent être synchronisés avec une source horaire centrale. Le Fournisseur doit déterminer et examiner toute activité suspecte ou malveillante identifiée dans ce registre, ainsi qu'y répondre. Le Fournisseur doit conserver une piste de vérification du registre de sécurité pour son système. Le Fournisseur doit conserver ces registres pendant toute la durée de l'Entente ou pendant un (1) an, selon la durée la plus longue, ou selon les exigences de la loi.

13. Vérifications des antécédents. Le Fournisseur doit exiger que tous les membres du personnel ayant accès aux renseignements confidentiels de Service alimentaire Gordon via les Systèmes du Fournisseur fassent l'objet d'une vérification des antécédents. Le Fournisseur doit en plus veiller à ce que les membres de son personnel chargés du traitement des renseignements confidentiels de Service alimentaire Gordon soient informés de la nature confidentielle des RP couverts, aient reçu une formation appropriée sur leurs responsabilités et aient signé des

ententes de confidentialité écrites. Le Fournisseur doit veiller à ce que ces obligations de confidentialité demeurent en vigueur après la fin du travail des membres du personnel.

14. Processus de contrôle des changements. Le Fournisseur doit maintenir des processus raisonnables de contrôle des changements afin d'approuver et de suivre les changements au sein de son environnement informatique.

15. Protection des supports de stockage. Le Fournisseur doit s'assurer que les supports de stockage contenant des renseignements confidentiels de Service alimentaire Gordon sont correctement nettoyés de tous les renseignements confidentiels de Service alimentaire Gordon ou sont détruits avant d'être éliminés ou réutilisés pour un traitement ne relevant pas du Fournisseur. Tous les supports sur lesquels les renseignements confidentiels de Service alimentaire Gordon sont stockés doivent être protégés contre toute modification ou tout accès non autorisé. Le Fournisseur doit maintenir des processus et des mécanismes raisonnables et appropriés pour assurer la responsabilité et le suivi de la réception, du retrait et du transfert des supports de stockage utilisés pour les systèmes d'information du Fournisseur ou sur lesquels les renseignements confidentiels de Service alimentaire Gordon sont stockés.

16. Comptes système. Le Fournisseur doit maintenir des politiques appropriées en matière de demande, d'approbation, d'audit et d'administration des comptes et des privilèges d'accès pour ses systèmes d'information et les renseignements confidentiels de Service alimentaire Gordon. Les membres du personnel du Fournisseur qui accèdent aux systèmes qui stockent, transmettent ou traitent les renseignements confidentiels de Service alimentaire Gordon se verront attribuer des comptes système individuels afin de garantir la responsabilité de l'accès accordé.

17. Mots de passe. Le Fournisseur doit mettre en œuvre des paramètres de mot de passe appropriés pour les systèmes qui accèdent aux renseignements confidentiels de Service alimentaire Gordon, qui les transmettent ou qui les stockent (les «**Systèmes connexes**»). Le Fournisseur doit mettre en œuvre une authentification à deux facteurs efficace et des mots de passe complexes pour tous les accès au réseau et aux Systèmes connexes. Le Fournisseur doit respecter les pratiques de l'industrie en matière de mots de passe. Les mots de passe par défaut du fabricant utilisés dans les produits du Fournisseur doivent être modifiés lors de leur installation.

18. Continuité des activités. Le Fournisseur doit s'assurer d'avoir des procédures et des processus adéquats permettant à une entreprise de maintenir ses activités en cas de catastrophe (les «**Plans de continuité des activités**») afin de garantir sa conformité avec les conditions du présent contrat et de réviser et tester les plans au moins une fois par an.

19. Destruction des données. Tous les renseignements confidentiels de Service alimentaire Gordon doivent être détruits de manière sécurisée dès qu'ils ne sont plus nécessaires, selon des processus commercialement raisonnables. La stratégie du Fournisseur en matière de destruction des données doit être documentée et inclure des registres pour tous les renseignements confidentiels de Service alimentaire Gordon détruits, qui doivent être disponibles pour examen par Service alimentaire Gordon.

Gordon SERVICE ALIMENTAIRE	**Objet :** Contrat nord-américain de traitement des données **Propriétaire :** Responsable de la protection de la vie privée	**Entrée en vigueur :** 1er avril 2025 **Remplace la politique datée du :** 19 février 2024
	Type : Révision complète ( ) Révision partielle (X) Nouveau document ( )	**Approuvé par :** Responsable de la protection de la vie privée

20. Conformité aux normes de sécurité sur les données de l'industrie des cartes de paiement (PCI DSS). En ce qui concerne les Services, le Fournisseur doit, dans la mesure du possible, maintenir le niveau requis de conformité et de certification PCI DSS et fournir la documentation correspondante à la demande de Service alimentaire Gordon. Le Fournisseur est responsable de la sécurité des données des titulaires de cartes qu'il trouve, utilise et/ou conserve conformément au présent contrat ou afin de fournir les Services. Le Fournisseur est tenu de mettre en œuvre et de maintenir des mesures de sécurité raisonnables. Ces mesures de sécurité doivent être appropriées compte tenu du caractère sensible des renseignements et doivent protéger les renseignements contre tout accès, toute utilisation ou toute divulgation non autorisés.