CONTRAT D'APPROVISIONNEMENT DE GRÉ À GRÉ

DÉSIGNATION DES PARTIES

ENTRE : **LE MINISTRE DE LA SANTÉ ET DES SERVICES SOCIAUX**, pour et au nom du gouvernement du Québec, représenté par monsieur Reno Bernier, sous-ministre associé à la Direction générale des technologies de l'information (DGTI), dûment autorisé en vertu du Règlement 2 sur la signature de certains actes, documents ou écrits du ministère de la Santé et des Services sociaux (c. M-19.2, r.3), dont les bureaux d'affaires sont situés au 930, chemin Sainte-Foy, Québec (Québec) G1S 2L4;

ci-après appelé « le ministre ».

ET : **AKINOX SOLUTIONS INC.**, personne morale légalement constituée dont le numéro d'entreprise du Québec (NEQ) est 1166640020, ayant son siège au 2467, rue Bellevue, Lévis (Québec), G6W 2T8, représentée par monsieur Alexander Dahl, président, dûment autorisé tel qu'il le déclare;

ci-après appelée « le fournisseur ».

LES PARTIES CONVIENNENT CE QUI SUIT :

1. Le fournisseur consent à fournir les biens et services ci-après décrits. Le présent contrat ainsi que les documents afférents constituent l'entente entre les parties à toutes fins que de droit. En cas d'incompatibilité, les stipulations du présent contrat auront préséance.

2. OBJET DU CONTRAT

   Le 11 mars 2020, l'Organisation mondiale de la santé a déclaré une pandémie de la COVID 19. Le 13 mars 2020, le gouvernement du Québec a déclaré l'état d'urgence sanitaire en vertu de l'article 118 de la Loi sur la santé publique. En vertu de l'alinéa 7 de l'article 123 de la Loi sur la santé publique, le ministre peut faire les dépenses et conclure les contrats qu'il juge nécessaires. Par le décret numéro 177 2020 du 13 mars 2020 et les décrets et arrêtés subséquents, le gouvernement et le ministre de la Santé et des Services sociaux ont pris différentes mesures pour protéger la santé de la population québécoise.

   Le ministre retient les services du fournisseur pour la réalisation du mandat suivant:

   La livraison et l'adaptation d'une solution de preuve vaccinale et d'un passeport vaccinal pour les résidents Québécois.

   Dans le cadre de la mise en place des mesures de sécurité, en lien avec la pandémie du virus COVID-19, le Ministère de la santé et des services sociaux doit effectuer des travaux et actions afin de rendre disponible à la population une preuve vaccinale. La solution retenue s'opérationnalise par le biais d'un passeport vaccinal. Ce dernier, permettant la lecture des codes QR vérifiables. Ce passeport vaccinal sera disponible gratuitement et publiquement à l'aide d'une application mobile. Il est également possible de télécharger cette preuve vaccinale en format PDF ou imprimée, en format papier, à partir d'un ordinateur ou d'un appareil mobile.

   Par solution, nous entendons (i) tous concepts, inventions, systèmes, procédés, techniques, méthodologie, savoir-faire, données, outils, maquettes, technologies (y compris les logiciels en codes exécutables et en codes sources), documentation ou tout autre information, données et matériels, et toute expression des précédents, développés par, propriétés de, habilités par le fournisseur avant la livraison/fourniture de la Solution désignée dans le Contrat et (ii) toute amélioration, progrès ou dérivés développés par le fournisseur afin de fournir la Solution mentionnée dans le Contrat.

Pour davantage d'informations, veuillez-vous référer à l'annexe 2 « Description des besoins : Devis » et l'annexe 3 « Description des besoins : Test d'intrusion »

3. MONTANT DU CONTRAT

Le mode de rémunération du présent contrat est mixte, par conséquent, les montants se déclines comme suit :

Le ministre s'engage à verser au fournisseur:

le montant forfaitaire de :

Trois millions sept cent trente mille dollars 3 730 000,00 $

et

le montant à la demande maximale de :

Cinq millions quatre cent mille dollars 5 400 000,00 $

Type de rémunération	Description	Prix unitaire ($)	Total ($)	Pourcentage (%)
Forfaitaire	Licence et support niveau 3 (VaxiCode, VaxiCode Verif, engin de règles d'affaires, API, BI, usage illimité)	[redacted]	[redacted]	[redacted]
	Licence et support niveau 3 pour serveur TSP-VACC (portail, concours, notifications et intégration de la billetterie)	[redacted]		
	Frais d'hébergement – Hors Azure (courriels, sms, etc. – usage de base du forfait annuel)	[redacted]		
	Hébergement (Microsoft Azure Cloud, période de 11 mois)	[redacted]		
Montant maximal pour service à la demande	Travaux de base : services, personnalisation et intégrations (Usage domestique seulement)	[redacted]	[redacted]	[redacted]
	Travaux de base : services, personnalisation, intégrations (Usage hors Québec, voyages, liens Fédéral et autres juridictions)	[redacted]		
	Contingence pour travaux à la demande (Banque d'heures, hébergement, support, licences apparentées,	[redacted]		

	travaux non prévus demandant une expertise externe, etc.)			
Total ($)			9 130 000,00 $	100 %

Pour l'exécution complète et entière des obligations prévues au présent contrat, sans autres frais, coûts ou dépens que ce soit et conformément aux modalités prévues à la clause 4 du présent contrat.

Advenant où le fournisseur serait dans l'obligation de sous-contracter une partie des travaux non définis dans la portée du présent contrat, en raison de demandes additionnelles du Ministre, les fonds nécessaires à son exécution seront assurés par la contingence pour travaux à la demande.

Les frais de déplacement, de recherche, de communication et toutes autres dépenses relatifs aux présentes sont inclus dans le prix ou le taux soumis et, par le fait même, dans le montant maximal du contrat.

4. MODALITÉS DE PAIEMENT

	DESCRIPTION	**FRÉQUENCE**
1)	Licence et support niveau 3 (VaxiCode, VaxiCode Verif, engin de règles d'affaires, API, BI, usage illimité)	À la signature
2)	Licence et support niveau 3 pour serveur TSP-VACC (portail, concours, notifications et intégration de la billetterie)	À la signature
3)	Frais d'hébergement – Hors Azure (courriels, sms, etc. – usage de base du forfait annuel)	À la signature
4)	Hébergement (période de 11 mois)	À la signature
5)	Travaux de base : services, personnalisation et intégrations (Usage domestique seulement)	À l'utilisation
6)	Travaux de base : services, personnalisation, intégrations (Usage hors Québec, voyages, liens Fédéral et autres juridictions)	À l'utilisation
7)	Contingence pour travaux à la demande (Banque d'heures, hébergement, support, licences apparentées, travaux non prévus demandant une expertise externe, test d'intrusion, etc.)	À l'utilisation

Le coût des licences, de support, SMS/courriels ainsi que l'hébergement sont payables à la signature du contrat. Les travaux de base ainsi que la contingence pour travaux à la demande sont payables à l'utilisation, et ce, conditionnellement à l'acceptation des travaux.

Le fournisseur devra présenter au ministre, à la date de début de contrat, une facture contenant de façon générale l'information suivante : le montant officiel des licences, du support, des sms-courriels et d'hébergement. Il devra également y inclure les dates visées, la description des activités réalisées ainsi que le numéro du contrat.

Le fournisseur devra également présenter au ministre, à la suite de l'acceptation des travaux et en fonction de l'utilisation du budget de services à la demande, une facture contenant de façon générale l'information suivante : les dates et les heures travaillées, la description des activités réalisées ou services demandés, le nom de la ressource, le taux horaire ainsi que le numéro de contrat.

La facturation devra être acheminée à l'adresse suivante :

Direction des services administratifs — informatique
Direction générale du financement, de l'allocation des ressources et du budget
Ministère de la Santé et des Services sociaux
1075, chemin Sainte-Foy, 16e étage
Québec (Québec) G1S 2M1
Téléphone : 418 266-6923
Courriel : [redacted]

Après vérification, le ministre verse les sommes dues au fournisseur dans les 30 jours qui suivent la date de réception de la facture, accompagnée de tous les documents requis.

Le ministre règle normalement les demandes de paiement conformément aux dispositions prévues au Règlement sur le paiement d'intérêts aux fournisseurs du gouvernement (RLRQ, chapitre C-65.1, r.8).

Le ministre se réserve le droit de procéder à toute vérification des demandes de paiement déjà acquittées.

5. DURÉE DU CONTRAT

Les services faisant l'objet du présent contrat, à l'exclusion de l'hébergement Azure, débuteront le 1er septembre 2021 et devront être terminés pour le 31 août 2022.

Les services d'hébergements Azure faisant l'objet du présent contrat, débuteront le 1er octobre 2021 et devront être terminés pour le 31 août 2022.

6. LIEU DE RÉALISATION DES TRAVAUX

Pour la réalisation de son mandat, le fournisseur effectue le mandat dans ses locaux.

7. DOCUMENTS CONTRACTUELS

Les documents ci-annexés font partie intégrante du présent contrat comme s'ils y étaient au long récités. Le fournisseur reconnaît en avoir reçu une copie, les avoir lus et consent aux normes et aux conditions qui y sont énoncées.

Le présent contrat constitue la seule entente intervenue entre les parties et toute autre entente non reproduite au présent contrat est réputée nulle et sans effet.

8. REPRÉSENTANTS DES PARTIES

Le ministre, aux fins de l'application du présent contrat, y compris pour toute approbation qui y est requise, désigne monsieur Reno Bernier, sous-ministre associé, pour le représenter. Si un remplacement était rendu nécessaire, le ministre en aviserait le fournisseur de services dans les meilleurs délais.

De même, le fournisseur désigne monsieur Alexander Dahl, président, pour le représenter. Si un remplacement était rendu nécessaire, le fournisseur en aviserait le ministre dans les meilleurs délais.

Dans le cas où il y a plusieurs représentants, chacun pourra agir séparément et l'autorisation de l'un d'eux constituera une autorisation valide.

9. RESPONSABILITÉ DU MINISTRE

Sauf en cas de faute intentionnelle ou de faute lourde de la part du ministre, ce dernier n'assumera aucune responsabilité à l'égard de tous les dommages matériels subis par le fournisseur, ses employés, agents, représentants ou sous-contractants

10. OBLIGATIONS DU FOURNISSEUR

Le fournisseur s'engage envers le ministre à :

a) exécuter les travaux ou rendre l'ensemble des services décrits au présent contrat, ce qui inclut les travaux ou services qui, bien que non spécifiquement énumérés dans ce document, sont requis suivant la nature du présent contrat;

b) collaborer entièrement avec le ministre dans l'exécution du contrat et tenir compte de toutes les instructions et recommandations du ministre relativement à la façon de préparer et d'exécuter le travail confié.

11. AUTORISATION DE CONTRACTER

Lorsque le contrat comporte une dépense, incluant la dépense découlant de toute option prévue au contrat, qui est égale ou supérieure au montant déterminé par le gouvernement au regard de l'obligation de détenir une autorisation de contracter, le fournisseur doit, à la date de la conclusion du contrat, être autorisé à contracter par l'Autorité des marchés publics.

Dans le cas d'un consortium qui n'est pas juridiquement organisé, seules les entreprises le composant doivent être individuellement autorisées à la date de la conclusion du contrat. Par contre, s'il s'agit d'un consortium juridiquement organisé en société en nom collectif, en société en commandite ou en société par actions, celui-ci doit, en tant que fournisseur, être autorisé à contracter à cette date de même que chacune des entreprises le formant.

Toute entreprise qui souhaite être partie à un sous-contrat rattaché directement ou indirectement au présent contrat et dont le montant est égal ou supérieur au seuil déterminé par le gouvernement au regard de l'obligation de détenir une autorisation de contracter doit également être autorisée à contracter par l'Autorité des marchés publics.

12. MAINTIEN DE L'AUTORISATION DE CONTRACTER

Le fournisseur doit, pendant toute la durée du contrat, maintenir son autorisation de contracter accordée par l'Autorité des marchés publics.

Dans le cas d'un consortium qui n'est pas juridiquement organisé, seules les entreprises le composant doivent individuellement maintenir leur autorisation de contracter pendant toute la durée du contrat.

Par contre, s'il s'agit d'un consortium juridiquement organisé en société en nom collectif, en société en commandite ou en société par actions, celui-ci doit, en tant que fournisseur, maintenir son autorisation de contracter pendant toute la durée du contrat, de même que chacune des entreprises le formant.

Dans l'éventualité où le fournisseur, le consortium juridiquement organisé ou une entreprise composant un consortium voyait son autorisation de contracter révoquée, expirée ou non renouvelée en cours d'exécution du contrat, le fournisseur, le consortium ou l'entreprise composant le consortium sera réputé en défaut d'exécuter le contrat au terme d'un délai de 60 jours suivant, selon le cas, la date d'expiration de l'autorisation ou la date de notification de la décision de l'Autorité des marchés publics.

Toutefois, le fournisseur, le consortium juridiquement organisé ou une entreprise composant tout consortium n'est pas réputé en défaut d'exécution lorsqu'il s'agit d'honorer les garanties au contrat ou du seul fait qu'il n'a pas fait sa demande de renouvellement dans le délai requis d'au moins 90 jours avant le terme de la durée de l'autorisation. Par conséquent, il pourra, malgré la date d'expiration de son autorisation, continuer le contrat en cours d'exécution jusqu'à la décision de l'Autorité des marchés publics relative au renouvellement de l'autorisation.

13. DÉFAUT D'EXÉCUTION DU CONTRAT

Le fournisseur inscrit au registre des entreprises non admissibles (RENA) est, sous réserve d'une permission du Conseil du trésor, réputé en défaut d'exécuter ce contrat au terme d'un délai de 60 jours suivant la date de son inadmissibilité.

Le ministre peut, dans les 30 jours suivant la notification de l'inadmissibilité et pour un motif d'intérêt public, demander au Conseil du trésor de permettre la poursuite de l'exécution du contrat. Le Conseil du trésor pourra notamment assortir sa permission de conditions dont celle demandant que le fournisseur soit soumis, à ses propres frais, à des mesures de surveillance et d'accompagnement. Par contre, la permission du Conseil du trésor n'est pas requise lorsqu'il s'agit de se prévaloir d'une garantie découlant du contrat.

Un fournisseur qui ne peut poursuivre l'exécution d'un contrat public en application du premier alinéa de l'article 21.3.1 de la Loi sur les contrats des organismes publics (RLRQ, chapitre C-65.1) est réputé en défaut d'exécuter ce contrat.

14. SOUS-CONTRAT

Lorsque la réalisation du présent contrat implique la participation de sous-contractants, sa réalisation et les obligations qui en découlent demeurent alors sous la responsabilité du fournisseur avec lequel le ministre a signé le contrat.

Le fournisseur doit, avant de conclure tout sous-contrat requis pour l'exécution du contrat, s'assurer que chacun de ses sous-contractants n'est pas inscrit au registre des entreprises non admissibles aux contrats publics (RENA) ou, s'il y est inscrit, que sa période d'inadmissibilité aux contrats publics est terminée. De plus, si le montant d'un sous-contrat est égal ou supérieur au seuil déterminé par le gouvernement, le fournisseur de services doit s'assurer que le sous-contractant est autorisé à contracter par l'Autorité des marchés publics.

15. PROTECTION DES RENSEIGNEMENTS PERSONNELS ET CONFIDENTIELS

Le fournisseur, tel que stipulé au paragraphe 9 de l'article 14.2 des conditions générales décrites en annexe 1 du présent contrat, s'engage à :

A. ne conserver, à l'expiration du contrat, aucun document contenant un renseignement personnel ou confidentiel, quel qu'en soit le support, en les retournant au ministre dans les 60 jours suivant la fin du contrat et remettre au ministre une confirmation que lui et les membres de son personnel ont retourné tous ces documents.

ou

B. procéder, à ses frais, à la destruction des renseignements personnels et confidentiels en se conformant à la fiche d'information sur la destruction des documents contenant des renseignements personnels de la Commission d'accès à l'information du Québec ainsi qu'aux directives que lui remettra le représentant du ministre et transmettre à celui-ci, dans les 60 jours suivant la fin du contrat, l'Attestation de destruction des renseignements personnels et confidentiels jointe à l'annexe 7, signée par une personne autorisée qu'il aura désignée à cette fin.

ou

C. confier la destruction des renseignements personnels et confidentiels à une entreprise de récupération, laquelle s'engage contractuellement à se conformer à la fiche d'information sur la destruction des documents contenant des renseignements personnels de la Commission d'accès à l'information du Québec ainsi qu'aux directives du ministre. Le fournisseur devra alors, dans les 60 jours suivant la fin du contrat de récupération, remettre au ministre l'Attestation de destruction des renseignements personnels et confidentiels jointe à l'annexe 7, signée par le responsable autorisé de cette entreprise.

Veuillez choisir une lettre (A, B ou C) : ___A____

16. ÉVALUATION ET ACCEPTATION DES TRAVAUX

Malgré toute autorisation ou approbation donnée à des fins de rémunération aux différentes étapes d'exécution du contrat, le ministre se réserve le droit, lors de la réception définitive des travaux ou de l'acceptation des services, de refuser, en tout ou en partie, les travaux ou les services qui n'auraient pas été exécutés conformément aux exigences du présent contrat.

Le ministre fait connaître, par avis écrit, son refus d'une partie ou de l'ensemble des travaux exécutés par le fournisseur dans les trente (30) jours de la réception définitive des travaux ou de l'acceptation des services.

Le ministre ne pourra refuser les travaux exécutés ou les services rendus par le fournisseur que pour une bonne et valable raison relative à la qualité du travail compte tenu de l'objet de ce contrat donné au fournisseur et des attentes qui peuvent raisonnablement en découler.

Le ministre se réserve le droit de faire reprendre les travaux ou les services rendus refusés par un tiers ou par le fournisseur aux frais de ce dernier.

17. REMISE DES DOCUMENTS ET DU MATÉRIEL

À l'expiration du présent contrat, le fournisseur devra remettre au ministre tous les documents, matériaux, outils et équipements que ce dernier lui aura fournis relativement à l'exécution du présent contrat, ceux-ci étant et demeurant la propriété entière et exclusive du ministre.

Ces documents, matériaux, outils et équipements devront être remis dans les mêmes conditions qu'ils étaient lors de leur réception par le fournisseur, sauf pour l'usure normale résultant de l'exécution du présent contrat.

Le fournisseur s'engage à indemniser le ministre pour toutes pertes ou tous dommages causés à ces biens lors de l'exécution du contrat. Le montant des dommages correspondra à la valeur de remplacement du bien ou, en cas de dommages mineurs, au coût des réparations. Ce montant sera déterminé par le ministre et pourra, le cas échéant, être retenu sur le solde dû au fournisseur.

18. MODIFICATION DU CONTRAT

Toute modification au contenu du présent contrat devra faire l'objet d'une entente écrite entre les parties. Cette entente ne peut changer la nature du contrat et elle en fera partie intégrante.

19. COMMUNICATIONS

Les communications et avis devant être transmis en vertu du présent contrat, pour être valides et lier les parties, doivent être donnés par écrit et être transmis par un moyen permettant de prouver la réception à un moment précis, aux coordonnées suivantes :

Pour le ministre :

Monsieur Luc Tremblay
Directeur des mandats stratégiques
Direction générale adjointe des licences et
des systèmes d'information (DGALSI)
Ministère de la Santé et des Services sociaux
930, ch. Sainte-Foy, 4e étage
Québec (Québec) G1S 2L4
Téléphone : 418-446-8041
Courriel : [redacted]

Pour le fournisseur :

Monsieur Alexander Dahl
Président
AKINOX Solutions Inc.
2467, rue Bellevue
Lévis (Québec) G6W 2T8
Téléphone : 418-476-7970
Courriel : [redacted]

Tout changement d'adresse de l'une des parties doit faire l'objet d'un avis à l'autre partie.

20. CLAUSE FINALE

Tout engagement financier du gouvernement du Québec n'est valide que s'il existe, sur un crédit, un solde disponible suffisant pour imputer la dépense découlant de cet engagement conformément aux dispositions de l'article 21 de la Loi sur l'administration financière (RLRQ, chapitre A-6.001).

EN FOI DE QUOI, les parties ont signé le présent contrat à la date indiquée ci-dessous :

LE MINISTRE,

[redacted] _____

Reno Bernier, sous-ministre associé

LE FOURNISSEUR,

[redacted] _____

Alexander Dahl, *président*

IMPORTANT : Le numéro de contrat doit être indiqué sur toutes les factures

ANNEXE 1 – CONDITIONS GÉNÉRALES
« Contrat de services de gré à gré »

1. LOIS ET RÈGLEMENTS APPLICABLES ET TRIBUNAL COMPÉTENT

Le fournisseur s'engage à respecter, dans l'exécution du présent contrat, les lois et règlements en vigueur au Québec applicables à l'exécution du présent contrat et en cas de contestation, les tribunaux du Québec seront seuls compétents.

2. POLITIQUE GOUVERNEMENTALE RELATIVE À L'EMPLOI ET À LA QUALITÉ DE LA LANGUE FRANÇAISE DANS L'ADMINISTRATION

Le fournisseur ayant un établissement au Québec et ayant 50 employés ou plus au Québec depuis au moins 6 mois doit se conformer aux critères d'application du point 22 de la Politique gouvernementale relative à l'emploi et à la qualité de la langue française dans l'administration pendant la durée du contrat.

3. ATTESTATION DE REVENU QUÉBEC

Tout fournisseur ayant un établissement au Québec doit, pour se voir octroyer un contrat de 25 000 $ ou plus, transmettre au ministre une attestation délivrée par l'Agence du revenu du Québec, nommée « Attestation de Revenu Québec ». Cette attestation du fournisseur est valide jusqu'à la fin de la période de trois mois qui suit le mois au cours duquel elle a été délivrée.

De plus, l'attestation du fournisseur ne doit pas avoir été délivrée après la date et l'heure limites fixées pour la réception des soumissions.

Cette attestation indique que, à sa date de délivrance, le fournisseur a produit les déclarations et les rapports qu'il devrait produire en vertu des lois fiscales et qu'il n'a pas de compte payable en souffrance à l'endroit du ministre du Revenu du Québec, notamment lorsque son recouvrement a été légalement suspendu ou lorsque des dispositions ont été convenues avec lui pour en assurer le paiement et qu'il n'est pas en défaut à cet égard.

Un fournisseur ne peut transmettre une attestation de Revenu Québec qui contient des renseignements faux ou inexacts, produire pour lui-même l'attestation d'un tiers ou faussement déclarer qu'il ne détient pas l'attestation requise.

Il est interdit d'aider une personne, par un acte ou une omission, à contrevenir aux dispositions du paragraphe précédent ou, par un encouragement, un conseil, un consentement, une autorisation ou un ordre, de l'amener à y contrevenir.

La violation des dispositions des deux paragraphes précédents constitue une infraction suivant le Règlement sur les contrats de services des organismes publics (chapitre C-65.1, r. 4) et rend son auteur passible d'une amende de 5 000 $ à 30 000 $ dans le cas d'une personne physique et de 15 000 $ à 100 000 $ dans les autres cas. En cas de récidive dans les cinq ans, le montant des amendes minimales et maximales prévues est doublé.

4. DÉCLARATION CONCERNANT LES ACTIVITÉS DE LOBBYISME EXERCÉES AUPRÈS DE L'ORGANISME PUBLIC RELATIVEMENT À L'ATTRIBUTION D'UN CONTRAT DE GRÉ À GRÉ

Avant la signature du contrat de gré à gré, tout fournisseur doit produire le formulaire « Déclaration concernant les activités de lobbyisme exercées auprès de l'organisme public relativement à l'attribution d'un contrat de gré à gré » joint à l'annexe 4 et dûment signé pour se voir octroyer le contrat. Dans ce formulaire, le contractant déclare notamment qu'au sens de la Loi sur la transparence et l'éthique en matière de lobbyisme (RLRQ, chapitre T-11.011) et des avis émis par le Commissaire au lobbyisme :

• soit que personne n'a exercé pour son compte, que ce soit à titre de lobbyiste d'entreprises ou de lobbyiste-conseil ou de lobbyiste d'organisation, des activités de lobbyisme, préalablement à la déclaration;

• ou que des activités de lobbyisme ont été exercées pour son compte et qu'elles l'ont été en conformité avec cette loi, avec ces avis ainsi qu'avec le Code de déontologie des lobbyistes (RLRQ, chapitre T-11.011, r.2).

De plus, le contractant reconnaît que, si l'organisme public a des motifs raisonnables de croire que des communications d'influence non conformes à la Loi sur la transparence et l'éthique en matière de lobbyisme et au Code de déontologie des lobbyistes ont eu lieu pour obtenir le contrat, une copie de la déclaration pourra être transmise au Commissaire au lobbyisme par l'organisme public.

Ce formulaire doit être celui du ministre ou contenir les mêmes dispositions. Le défaut de produire cette déclaration pourra entraîner la non-conclusion du contrat.

5. RESPONSABILITÉ DU FOURNISSEUR

Le fournisseur sera responsable de tous les dommages causés par lui, ses employés, agents, représentants ou sous-contractants dans le cours ou à l'occasion de l'exécution du présent contrat, y compris le dommage résultant d'un manquement à un engagement pris en vertu du présent contrat.

Le fournisseur s'engage à indemniser, protéger et prendre fait et cause pour le ministre contre tout recours, toute réclamation, toute demande, toute poursuite et toute autre procédure pris par toute personne en raison de dommages ainsi causés.

Malgré les deux premiers alinéas, la responsabilité du fournisseur aux termes de ce contrat est toutefois limitée à cinq fois la valeur du contrat jusqu'à concurrence de 3 000 000 $.

Cette limite financière de responsabilité ne s'applique pas au préjudice corporel ou moral ni au préjudice matériel causé par une faute intentionnelle ou une faute lourde.

6. REGISTRE DES ENTREPRISES NON ADMISSIBLES AUX CONTRATS PUBLICS (RENA)

Le fournisseur ne doit pas être inscrit au registre des entreprises non admissibles aux contrats publics (RENA) ou, s'il y est inscrit, sa période d'inadmissibilité aux contrats publics doit être terminée.

Par contre, le Conseil du trésor peut, lors de circonstances exceptionnelles, permettre à un organisme public ou à un organisme visé à l'article 7 de conclure un contrat avec une entreprise inadmissible aux contrats publics ou permettre à une entreprise de conclure un sous-contrat rattaché directement à un contrat public avec un sous-contractant inadmissible aux contrats publics. Le Conseil du trésor peut assortir cette permission de conditions, notamment celle que l'entreprise ou le sous-contractant inadmissible soit soumis, à ses frais, à des mesures de surveillance et d'accompagnement.

En outre, lorsqu'un organisme public ou un organisme visé à l'article 7 constate qu'il y a urgence et que la sécurité des personnes ou des biens est en cause, le dirigeant de cet organisme peut permettre de conclure un contrat avec une entreprise inadmissible aux contrats publics ou permettre à une entreprise de conclure un sous-contrat rattaché directement à un contrat public avec un sous-contractant inadmissible aux contrats publics. Le dirigeant de l'organisme doit toutefois en aviser par écrit le président du Conseil du trésor dans les 15 jours.

Les dispositions des deux paragraphes précédents s'appliquent également, avec les adaptations nécessaires, lorsqu'il s'agit de permettre la conclusion d'un contrat public ou d'un sous-contrat rattaché directement à un contrat public avec une entreprise qui ne détient pas une autorisation de contracter alors qu'une telle autorisation est requise.

7. RÉSILIATION

7.1 Le ministre se réserve le droit de résilier ce contrat pour l'un des motifs suivants :

a) le fournisseur fait défaut de remplir l'un ou l'autre des termes, conditions ou obligations qui lui incombent en vertu du présent contrat;

b) le fournisseur cesse ses opérations de quelque façon que ce soit, y compris en raison de la faillite, liquidation ou cession de ses biens;

c) le fournisseur lui a présenté des renseignements faux ou trompeurs ou lui a fait de fausses représentations;

d) le fournisseur est déclaré coupable d'une infraction à la Loi sur la concurrence (L.R.C. (1985), c. C-34) édictée par le gouvernement fédéral relativement à un appel d'offres public ou à un contrat conclu avec une administration publique au Canada, sans toutefois avoir encore été inscrit au registre des entreprises non admissibles aux contrats publics (RENA).

Pour ce faire, le ministre adresse un avis écrit de résiliation au fournisseur énonçant le motif de résiliation. S'il s'agit d'un motif de résiliation prévu au paragraphe a), le fournisseur devra remédier au défaut énoncé dans le délai prescrit à cet avis, à défaut de quoi ce contrat sera automatiquement résilié, la résiliation prenant effet de plein droit à l'expiration de ce délai. S'il s'agit d'un motif de résiliation prévu au paragraphe b), c) ou d), la résiliation prendra effet de plein droit à compter de la date de la réception de l'avis par le fournisseur.

Le fournisseur aura alors droit aux frais, déboursés et sommes représentant la valeur réelle des services rendus jusqu'à la date de la résiliation du contrat, conformément au présent contrat, sans autre compensation ni indemnité que ce soit (en considérant l'avance reçue, s'il y a lieu), et ce, à la condition qu'il remette au ministre tous les travaux déjà effectués au moment de la résiliation.

Le fournisseur sera par ailleurs responsable de tous les dommages subis par le ministre du fait de la résiliation du contrat.

En cas de poursuite du contrat par un tiers, le fournisseur devra notamment assumer toute augmentation du coût du contrat pour le ministre.

7.2 Le ministre se réserve également le droit de résilier ce contrat sans qu'il soit nécessaire pour lui de motiver la résiliation.

Pour ce faire, le ministre doit adresser un avis écrit de résiliation au fournisseur. La résiliation prendra effet de plein droit à la date de la réception de cet avis par le fournisseur.

Le fournisseur aura alors droit aux frais, déboursés et sommes représentant la valeur réelle des services rendus jusqu'à la date de résiliation du contrat, conformément au présent contrat, sans autre compensation ou indemnité que ce soit et, notamment, sans compensation ni indemnité pour la perte de tous profits escomptés.

8. CESSION DE CONTRAT

Les droits et obligations contenus au présent contrat ne peuvent, sous peine de nullité, être cédés, en tout ou en partie, sans l'autorisation du ministre.

9. PROPRIÉTÉ MATÉRIELLE ET DROITS D'UTILISATION

9.1 Propriété matérielle

La documentation produite par le MSSS et transmise au fournisseur sur les processus, rapports statistiques et diagrammes sont et demeurent la propriété du ministre. La documentation produite par le fournisseur à la demande du ministre devient la propriété du ministre (documents de gestion, rapport de projet, etc.).

Le fournisseur reconnaît ne pas être propriétaire des données (saisies par les utilisateurs dans la Solution) et, ce faisant, il doit permettre au ministre ou, selon le cas, aux établissements et organismes du RSSS, d'y accéder selon les modalités prévues au Devis.

Nonobstant toute disposition contraire, aucune disposition du présent contrat ne modifie les droits du fournisseur quant à la propriété intellectuelle de la Solution, et le fournisseur n'accorde à l'autre partie le droit à la propriété intellectuelle de la Solution.

9.2 Droits d'utilisation

Licence

Le fournisseur détient la propriété intellectuelle de la solution et il en demeure le seul à pouvoir modifier son code informatique. Cependant, les clés cryptographiques servant à signer les preuves de vaccination demeurent la propriété entière et exclusive du ministre.

Cette licence est accordée sans limites territoriales et pour une durée limitée à la durée du présent contrat.

Toute considération pour la licence de droits d'utilisation consentie en vertu du présent contrat est incluse dans la rémunération prévue.

Garanties

Le fournisseur garantit au ministre qu'il détient tous les droits lui permettant de réaliser le présent contrat et, notamment, d'accorder la licence de droits d'auteur prévue au présent article et se porte garant envers le ministre contre tout recours, réclamation, demande, poursuite et toute autre procédure, pris par toute personne relativement à l'objet de ces garanties.

Le fournisseur s'engage à prendre fait et cause et à indemniser le ministre de tout recours, réclamation, demande, poursuites et toute autre procédure, pris par toute personne relativement à l'objet de ces garanties.

9.3 Restrictions d'utilisation

Le ministre, le réseau de la santé et des services sociaux et les établissements du Réseau de la santé et des services sociaux ne doivent pas (i) concéder de sous licence, sous-licencier, vendre, revendre, transférer, céder, distribuer ou autrement exploiter commercialement ou mettre à la disposition de tout tiers la Solution ou son contenu de quelque manière que ce soit; (ii) copier, reproduire, modifier ou créer des œuvres dérivées basées sur la Solution ou son contenu; (iii) «cadrer» ou «refléter» tout contenu sur tout autre serveur ou appareil sans fil ou Internet (iv) « reverse engineer » la Solution; (v) créer un produit ou une Solution concurrentiel, (vi) construire un produit en utilisant des idées, des caractéristiques ou des fonctions similaires de la Solution ou (vii) «spider » la Solution ou autrement automatiser la collecte de données de la Solution par tout autre moyen que par le biais des utilisateurs, à l'insu du fournisseur.

10. APPLICATION DE LA TPS ET DE LA TVQ

Ceci est pour certifier que les services retenus en vertu du présent contrat sont requis et payés par le ministère de la Santé et des Services sociaux avec les deniers publics pour son utilisation propre et sont assujettis aux taxes de vente applicables (taxe de vente du Québec (TVQ) et taxe sur les produits et services (TPS) ou, le cas échéant, taxe de vente harmonisée (TVH)) et, par conséquent, ces taxes doivent être facturées.

11. REMBOURSEMENT DE LA DETTE FISCALE

L'article 31.1.1 de la Loi sur l'administration fiscale (RLRQ, chapitre A-6.002) et l'article 53 de la Loi facilitant le paiement des pensions alimentaires (RLRQ, P-2.2) s'appliquent lorsque le fournisseur est redevable d'un montant exigible en vertu d'une loi fiscale ou alimentaire. Ainsi, le ministre pourra transmettre tout ou partie du montant payable en vertu du présent contrat au ministre du Revenu, à sa demande, afin que ce montant soit affecté au paiement de cette dette.

12. CONFLITS D'INTÉRÊTS

Le fournisseur doit éviter toute situation qui mettrait en conflit soit son intérêt propre, soit d'autres intérêts, notamment, mais sans limiter la généralité de ce qui précède, l'intérêt d'une de ses ressources, d'une de ses filiales ou d'une personne liée; dans le cas d'un consortium, l'intérêt d'une des constituantes versus l'intérêt du ministre. Si une telle situation se présente ou est susceptible de se présenter, le fournisseur doit immédiatement en informer le ministre qui pourra, à sa seule discrétion, émettre une directive indiquant au fournisseur comment remédier à ce conflit d'intérêts ou résilier le contrat.

Le présent article ne s'applique pas à un conflit pouvant survenir sur l'interprétation ou l'application du contrat.

13. CONFIDENTIALITÉ

Le fournisseur s'engage à ce que ni lui ni aucun de ses employés ne divulge, sans y être dûment autorisé par le ministre, les données, analyses ou résultats inclus dans les rapports réalisés en vertu du contrat ou, généralement, quoi que ce soit dont il aurait eu connaissance dans l'exécution du contrat.

Le fournisseur s'engage à prendre les mesures nécessaires pour que chacun de ses employés affectés à l'exécution du contrat certifie que tout renseignement obtenu par suite de son affectation à l'exécution du contrat ne sera pas divulgué ou porté à la connaissance de qui que ce soit et qu'il n'utilisera pas ces renseignements pour son avantage personnel.

14. PROTECTION DES RENSEIGNEMENTS PERSONNELS ET CONFIDENTIELS

14.1 Définitions

« Renseignement personnel » : tout renseignement qui concerne une personne physique et qui permet de l'identifier.

« Renseignement confidentiel » : tout renseignement dont l'accès est assorti d'une ou de plusieurs restrictions prévues par la Loi sur l'accès, notamment un renseignement ayant des incidences sur les relations intergouvernementales, sur les négociations entre organismes publics, sur l'économie, sur l'administration de la justice et la sécurité publique, sur les décisions administratives ou politiques ou sur la vérification.

14.2 Le fournisseur s'engage envers le ministre à respecter chacune des dispositions applicables aux renseignements personnels et confidentiels ci-dessous énumérées; que ces renseignements lui soient communiqués dans le cadre de la réalisation de ce contrat ou soient générés à l'occasion de sa réalisation.

1) Informer son personnel des obligations stipulées aux présentes dispositions et diffuser à cet égard toute l'information pertinente.

2) Rendre accessibles les renseignements personnels, au sein des membres de son personnel, uniquement à ceux qui ont qualité pour les recevoir, lorsqu'ils sont nécessaires à l'exercice de leurs fonctions et sont utilisés aux fins pour lesquelles ils ont été recueillis ou que la loi autorise leur utilisation.

3) Signer, préalablement à l'accès à des renseignements personnels et confidentiels, les engagements au respect de la confidentialité de ces renseignements selon l'annexe 5 du présent document et les transmettre aussitôt au ministre, sous peine de se voir refuser l'accès aux locaux, à l'équipement du ministre ou aux données à être transmises par celui-ci, le cas échéant.

4) Ne pas communiquer les renseignements personnels à qui que ce soit sans le consentement de la personne concernée, sauf dans le cadre d'un sous-contrat et selon les modalités prévues au paragraphe 14).

5) Soumettre à l'approbation du ministre le formulaire de consentement à la communication de renseignements personnels de la personne concernée.

6) Utiliser les renseignements personnels uniquement pour la réalisation du contrat.

7) Recueillir un renseignement personnel au nom du ministre, dans les seuls cas où cela est nécessaire à la réalisation du contrat, et informer préalablement toute personne visée par cette cueillette de l'usage auquel ce renseignement est destiné, ainsi que des autres éléments mentionnés à l'article 65 de la Loi sur l'accès.

8) Prendre toutes les mesures de sécurité propres à assurer la confidentialité des renseignements personnels et confidentiels à toutes les étapes de la réalisation du contrat et, le cas échéant, les mesures identifiées à l'annexe 5 – Engagement de confidentialité, jointe au présent document.

9) **Le fournisseur devra, au moment de la signature du contrat, faire un choix parmi les trois options suivantes :**

   - ne conserver, à l'expiration du contrat, aucun document contenant un renseignement personnel ou confidentiel, quel qu'en soit le support, en les retournant au ministre dans les 60 jours suivant la fin du contrat et remettre au ministre une confirmation que lui et les membres de son personnel ont retourné tous ces documents;

   - procéder, à ses frais, à la destruction des renseignements personnels et confidentiels en se conformant à la fiche d'information sur la destruction des documents contenant des renseignements personnels de la Commission d'accès à l'information du Québec ainsi qu'aux directives que lui remettra le ministre et transmettre à celui-ci, dans les 60 jours suivant la fin du contrat, l'Attestation de destruction des renseignements personnels et confidentiels jointe à l'annexe 7, signée par une personne autorisée qu'il aura désignée à cette fin;

   - confier la destruction des renseignements personnels et confidentiels à une entreprise de récupération, laquelle s'engage contractuellement à se conformer à la fiche d'information sur la destruction des documents contenant des renseignements personnels de la Commission d'accès à l'information du Québec ainsi qu'aux directives du ministre. Le fournisseur devra alors, dans les 60 jours suivant la fin du contrat de récupération, remettre au ministre l'Attestation de destruction des renseignements personnels et confidentiels jointe à l'annexe 7, signée par le responsable autorisé de cette entreprise.

10) Informer, dans les plus brefs délais, le ministre de tout manquement aux obligations prévues aux présentes dispositions ou de tout événement pouvant

risquer de porter atteinte à la sécurité ou à la confidentialité des renseignements personnels ou confidentiels.

11) Fournir, à la demande du ministre, toute l'information pertinente au sujet de la protection des renseignements personnels et confidentiels et donner accès, à toute personne désignée par le ministre, à la documentation, aux systèmes, aux données et aux lieux physiques relatifs au contrat afin de s'assurer du respect des présentes dispositions.

12) Se conformer aux objectifs et aux exigences de sécurité de l'information définis par le ministre.

13) Obtenir l'autorisation écrite du ministre avant de communiquer ou de transférer quelque donnée que ce soit, même à des fins techniques, hors du Québec.

14) Lorsque la réalisation du présent contrat est confiée, en tout ou en partie, à un sous-contractant et qu'elle comporte la communication de renseignements personnels et confidentiels par le fournisseur au sous-contractant ou la cueillette de renseignements personnels et confidentiels par le sous-contractant :

- soumettre à l'approbation du ministre la liste des renseignements personnels et confidentiels communiqués au sous-contractant;
- conclure un contrat avec le sous-contractant stipulant les mêmes obligations que celles prévues aux présentes dispositions;
- exiger du sous-contractant qu'il s'engage à ne conserver, à l'expiration du sous-contrat, aucun document contenant un renseignement personnel ou confidentiel, quel qu'en soit le support, et à remettre au fournisseur, dans les 60 jours suivant la fin de ce contrat, un tel document.

15) Transmettre de façon sécuritaire les renseignements personnels ou confidentiels lorsque ceux-ci sont communiqués par courriel ou Internet. Ces renseignements doivent nécessairement faire l'objet d'un chiffrement ou être protégés par un dispositif de sécurité éprouvé. Si les renseignements personnels ou confidentiels sont acheminés par télécopieur, l'émetteur du document doit s'assurer que le récepteur est habilité à le recevoir et qu'il prendra toutes les mesures nécessaires à la protection de ces renseignements. Toutefois, les parties peuvent convenir entre elles de tout autre moyen, telle la remise en mains propres, la messagerie ou la poste recommandée en indiquant toujours sur l'enveloppe la mention « personnel et confidentiel ».

14.3 La fin du contrat ne dégage aucunement le fournisseur et le sous-contractant de leurs obligations et engagements relatifs à la protection des renseignements personnels et confidentiels. Les principales dispositions applicables se retrouvent notamment, mais non limitativement, aux articles 1, 9, 18 à 41.3, 53 à 60.1, 62, 64 à 67.2, 83, 89, 158 à 164.

La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels peut être consultée à l'adresse suivante : www.publicationsduquebec.gouv.qc.ca.

ANNEXE 2 – DESCRIPTION DES BESOINS : DEVIS

1. Exigences technologiques

1.1 La solution

Dans la présente annexe, le terme « la solution » sera utilisée pour identifier la solution complète à supporter, soit :

- Le portail web d'émission de la preuve vaccinale
- L'application mobile VaxiCode
- L'application mobile VaxiCode Verif

1.2 Navigateurs et systèmes d'exploitation

Le FOURNISSEUR doit assurer la disponibilité des applications mobiles pour les systèmes d'exploitation IOS et Android.

Dans le cas où des mises à jour de ces systèmes d'exploitation par le MANUFACTURIER engendre des ajustements à effectuer sur les applications, ceux-ci devront faire l'objet d'une analyse préliminaire à la réalisation des travaux.

Seules les navigateurs web et leurs versions supportés et recommandés (*Evergreen*) par le MANUFACTURIER sont supportées par la solution :

Les postes de travail fixes ou portables :
- Google Chrome
- Edge
- Firefox
- Safari Desktop

Les appareil mobiles, téléphones intelligents et tablettes IOS et Android :
- Google Chrome
- Safari IOS

Le FOURNISSEUR s'engage à documenter et fournir les versions des systèmes d'exploitation et des navigateurs web minimum nécessaires pour accéder à la solution. Les versions minimums requises sont sujet à changement.

1.3 Accessibilité

Les portails web accessibles par les citoyens doivent respecter les normes d'accessibilité web du Conseil du Trésor du Québec Québec en vigueur à la signature du contrat et documentées dans Modernisation des standards sur l'accessibilité du Web 2.0 (SGQRI-008).

Référence :
https://www.tresor.gouv.qc.ca/ressources-informationnelles/architecture-dentreprise-gouvernementale/standards-et-normes/standards-sur-laccessibilite-du-web/

1.4 Adaptation visuelle

La solution est une solution commerciale détenue par le FOURNISSEUR. Son visuel global est donc défini par le FOURNISSEUR. La solution possède toutefois une structure permettant la personnalisation de la facture visuelle afin d'intégrer le plus adéquatement possible les standards visuels du gouvernement du Québec.

Le visuel de l'application intègre également des éléments de la marque de commerce du FOURNISSEUR et celui-ci se réserve le droit de le faire évoluer.

1.5 Hébergement et exploitation

1.5.1 Interdépendances

La solution est hébergée par le FOURNISSEUR dans son environnement infonuagique. Elle nécessite des interdépendances de systèmes en lien avec la solution. Leur bon fonctionnement pourrait avoir une incidence sur celui de la solution. Le FOURNISSEUR n'est toutefois pas responsable du bon fonctionnement des systèmes tiers. Parmi les interdépendances, notons les suivantes (liste non exhaustive) :

- La solution est hébergée hors du RITM et fournit une plateforme de communication de courriels (ex. SENDGRID).
- La solution est hébergée hors du RITM et fournit une plateforme de communication de texto (ex. TWILIO).
- La solution de fédération d'identité et d'authentification (ex. Okta)

1.5.2 Inclusions à l'hébergement

Le FOURNISSEUR prend en charge tous les éléments liés à l'hébergement de la solution, l'ORGANISME PUBLIC désirant une solution de type « clé en main ».

Par « clé en main », il est entendu que le FOURNISSEUR assume l'ensemble des dépenses liées à la mise en place et au maintien de la solution. Ceci inclut, sans s'y limiter:

- Un hébergement par le FOURNISSEUR, dans ses installations physiques, en colocation ou par une tierce partie sous sa responsabilité.
- Les mises à jour et l'entretien de la solution sont de la responsabilité du FOURNISSEUR.
- Les dispositions pour atteindre les niveaux de disponibilité sont de la responsabilité du FOURNISSEUR.

Les infrastructures et tous logiciels ou composantes requis pour le fonctionnement sécuritaire de la solution conformément aux exigences décrites dans le présent appel d'offres sont fournies et hébergées par le FOURNISSEUR, incluant notamment:

- L'infrastructure
- Les environnements
- Les serveurs
- Les logiciels tiers (exemple : licences SGBD, système d'exploitation, etc.)
- Les bases de données
- La sauvegarde et récupération des données
- La redondance et relève géographique
- Le lien internet reliant l'infrastructure du FOURNISSEUR à l'Internet
- L'ensemble des droits et licences sans limites de nombre d'utilisateurs et serveurs pour répondre aux besoins exprimés

Ce qui est EXCLU :

- Le lien entre Internet et chacun des sites de l'ORGANISME PUBLIC
- Travaux supplémentaires comme par exemple, mais sans s'y limiter :
  - Des mécanismes API pour intégration sécuritaires avec des solutions existantes
  - L'appel à des API tierces, par exemple pour des validations de pièces d'identité

- Des envois massifs de courriels / SMS au-delà des envois automatiques des processus habituels

Conséquemment l'hébergement doit répondre aux exigences suivantes :

- Les données doivent être chiffrées à l'aide de protocoles reconnus sécuritaires lors d'échanges et lorsqu'elles sont conservées sur support de sauvegarde
- La maintenance et l'entretien des serveurs ne doivent pas interférer à la disponibilité et la performance de la solution, hors des périodes convenues
- Le FOURNISSEUR doit signaler à l'ORGANISME PUBLIC les brèches de sécurité soupçonnées ou confirmées

1.5.3 Transfert de connaissance et documentation

Le FOURNISSEUR doit réaliser un transfert d'expertise pour permettre aux équipes du RSSS de piloter la solution selon les meilleures pratiques de l'industrie. Le FOURNISSEUR offre du soutien aux équipes tout au long du contrat.

Le FOURNISSEUR doit rendre disponible la description de l'architecture technologique de sécurité soutenant sa solution. Ces documents doivent être maintenus à jour advenant des modifications pendant toute la durée du contrat.

Le FOURNISSEUR doit rendre disponible et maintenir la mise à jour des documents suivants, advenant des modifications, pendant toute la durée du contrat :

- Architecture technologique de sécurité
- Systèmes d'exploitation et navigateurs web minimums supportés par la solution

1.5.4 Charge

La solution doit être capable de soutenir les usages concurrents raisonnables du RSSS :

- Les utilisateurs (licence populationnelle)
    - Nous entendons par utilisateurs :
        - Les employés directs de l'ORGANISME PUBLIC ayant accès au portail de gestion
        - Les citoyens demandant leurs preuves vaccinales sur le portail de libre-service
- Les interfaces
- Toutes autres connexions « machines » nécessaires au fonctionnement de la solution

Le FOURNISSEUR est tenu responsable si des problèmes de performance de son ressort affectent sa solution. Il sera par conséquent, de la responsabilité du Fournisseur de défrayer les coûts pour une mise à jour des serveurs (coût du matériel ou équipement nécessaire ainsi que le coût de main-d'œuvre) pour répondre à ses nouvelles spécifications. Le FOURNISSEUR ne sera pas tenu responsable si le problème résulte d'une dépendance externe, par exemple un problème avec un système du MSSS lié par interface comme le SI-PMI.

1.5.5 Niveaux de service

Les niveaux de service suivants doivent être respectés par le portail web d'émission de la preuve vaccinale :

- Environnement de production :

    - Taux de disponibilité : 99,5 %, excluant les arrêts planifiés sur un service 24/7, soit une indisponibilité par année de 1,83 jours

équivalent à 3,60 heures/mois ou 50,4 minutes/semaine ou 7,2 minutes/jour et ce globalement pour la province.
- Perte de données maximale admissible (*Recovery Point Objective – RPO*) ; délai durant lequel les mises à jour des données par les utilisateurs avant la panne majeure sont perdues : 4 heures.
- Délai de reprise attendu (*Recovery Time Objective – RTO*) ; délai maximum nécessaire pour rendre disponibles les services à l'utilisateur après la décision d'activer la relève à la suite d'une panne majeure : 4 heures.
- Le taux de rétention exigé est de : 16 derniers jours, 1 mensuel et 1 annuel par année pour la durée du contrat incluant les renouvellements, le cas échéant.

- Environnements de préproduction :

  - Niveau de disponibilité : 90 %, ceci est l'équivalent d'un potentiel de non-disponibilité de 36,5 jours par année, sur les heures normales d'affaires.

Les heures normales d'affaires sont de 9 heures à 17 heures, excluant les fins de semaine et les jours fériés.

1.5.6 Arrêts planifiés

Afin d'exécuter des travaux d'entretien, d'amélioration et de rehaussement, le FOURNISSEUR peut effectuer des arrêts planifiés, en tenant compte du fait que les arrêts planifiés :

- S'effectuent sur approbation préalable de l'ORGANISME PUBLIC.
- Peuvent s'effectuer hors des heures normales d'affaires, selon un horaire à convenir avec l'ORGANISME PUBLIC.
- Un calendrier annuel doit être soumis pour approbation à l'ORGANISME PUBLIC, étant entendu que des arrêts peuvent s'ajouter en cours d'année, au besoin.

1.6 Performances

1.6.1 Surveillance

La solution doit disposer d'outils de surveillance des performances et le FOURNISSEUR doit être en mesure de produire des rapports à la demande de l'ORGANISME PUBLIC portant sur la qualité de service et la gestion de la capacité.

Le FOURNISSEUR dispose d'un mécanisme de notification et d'escalade des alertes sur le dépassement des seuils acceptables des différents indicateurs de service et de performance. Les seuils seront définis conjointement entre l'ORGANISME PUBLIC et le FOURNISSEUR lors du déploiement de la solution.

1.7 Données

L'accès et l'exploitation des données doivent être permis et soutenus par le FOURNISSEUR à tous les paliers d'agrégation. Les données au sens large ne peuvent être exploitées en partie ou en totalité par toute autre entité que celles prévues au contrat, sans l'approbation écrite de l'ORGANISME PUBLIC. L'accès aux données de production par des tiers du fournisseur est prohibé.

À la demande, le FOURNISSEUR doit fournir le modèle de base de données, toutes les métadonnées et la documentation adéquate pour permettre à l'ORGANISME PUBLIC d'exploiter les données, le cas échéant. Ces documents doivent être maintenus à jour advenant des modifications pendant toute la durée du contrat et seront fournis à l'intérieur d'un délai de cinq (5) jours ouvrables suivant la demande par l'ORGANISME PUBLIC.

Le FOURNISSEUR doit isoler et maintenir le cloisonnement physique ou logique des données de celles de ses autres clients.

La solution permet l'interrogation de façon autonome de l'ensemble des données à partir d'une méthodologie convenue entre le FOURNISSEUR et l'ORGANISME PUBLIC. Le FOURNISSEUR doit fournir un accès à toutes les tables de la ou des bases de données de production.

Le FOURNISSEUR doit mettre en place un processus par lequel l'ORGANISME PUBLIC peut extraire lui-même toutes les données nécessaires, et ce en n'affectant pas les performances de la production (ex. : réplique de la base de données de production, etc.). L'ensemble des données de production doit être accessible, sauf les données des dernières 24 heures au maximum.

Les données doivent être chiffrées au repos et en mouvement avec des protocoles de sécurité reconnus comme sûrs à des niveaux de sécurité acceptable (ex. : PFS).

En aucun cas le FOURNISSEUR ne peut disposer des données à d'autres fins que celles prévues au présent contrat.

1.7.1 Suppression de données

Le FOURNISSEUR doit démontrer la garantie de la destruction complète de toute donnée, et ce, dans tous catalogues et unités de stockage, suivant des standards reconnus (ex. : NIST 800-88 Rev. 1).

1.7.2 Portabilité des données

En cas de sortie ou de fin de contrat, le FOURNISSEUR et l'ORGANISME PUBLIC devront prévoir la possibilité d'exporter les données pertinentes (incluant les données de journalisation) vers une ou des solutions (ex. : une solution d'archivage et une solution d'exploitation) à la convenance de l'ORGANISME PUBLIC selon les standards du marché en cours à ce moment.

À la fin du contrat et sur demande, le FOURNISSEUR doit assurer l'élimination et la suppression complète et sécuritaire des données de tous les supports de stockage, en veillant à ce que les données ne soient pas récupérables par aucun moyen, selon les standards reconnus et dans un délai raisonnable suivant la réception de la demande.

1.8 Évolution de la solution

1.8.1 Rehaussement des infrastructures

Tout au long du contrat, le FOURNISSEUR doit procéder au rehaussement de ses infrastructures pour répondre au niveau de service demandé. Si la solution ne supporte pas une mise à jour requise dans le cadre des activités de l'ORGANISME PUBLIC, une mise à jour de la solution apportant les correctifs nécessaires doit être disponible dans un délai maximum de huit (8) semaines débutant à partir de la date de la demande de l'ORGANISME PUBLIC.

Le FOURNISSEUR s'engage à faire évoluer sa solution afin qu'il demeure compatible avec les systèmes d'exploitation supportés par le manufacturier pour la durée du contrat incluant les renouvellements, le cas échéant.

1.8.2 Mise à jour de la solution

La solution doit être dans sa version la plus à jour (version stable), et doit être maintenue à jour en tout temps.

Les mises à jour de la solution doivent être faites tout au long du contrat. L'ensemble des mises à jour, qu'elles soient mineures ou majeures (changement de version), sont incluses dans le prix soumis.

Le FOURNISSEUR prend en charge le déploiement des mises à jour de sa solution.

Le FOURNISSEUR doit s'engager à effectuer la mise à jour à jour de la solution proposée ou des composantes utilisées par celle-ci (ex. : SGBD, librairies externes, etc.).

Le FOURNISSEUR doit confirmer, tester et certifier que l'application des correctifs (ex. : rustine sur le système d'exploitation, sur le SGBDR, librairies externes, etc.) proposés n'impacte pas les niveaux de services et que la solution est toujours pleinement fonctionnelle avant de procéder à l'application de correctifs. Les changements pouvant affecter la sécurité des données doivent enclencher un processus de validation de sécurité afin d'identifier l'exposition à de nouveaux risques.

Le processus de déploiement d'une mise à jour doit être convenu avec l'ORGANISME PUBLIC.

Un mécanisme de traçabilité des changements doit être en place.

L'ensemble de la solution doit être et demeurer compatible, tout au long du contrat, avec les logiciels utilisés sur les postes de travail du RSSS incluant les mises à jour (autant mineures [rustine de sécurité] que majeures [Windows 10]). Si la solution ne supporte pas une mise à jour requise dans le cadre des activités du RSSS, une mise à jour de la solution apportant les correctifs nécessaires doit être disponible dans un délai maximum de huit (8) semaines débutant à partir de la date de la demande de l'ORGANISME PUBLIC.

1.8.3 Processus de rehaussement des versions

Le FOURNISSEUR doit décrire le processus de rehaussement des versions qu'il entend mettre en œuvre.

Ce processus doit, entre autres, respecter les cibles suivantes :

A. Minimiser le temps de non-disponibilité du système, le cas échéant
B. Être exécuté en dehors des heures normales d'affaires ou selon un calendrier sujet à l'approbation du CDO
C. Dois comprendre en tout temps un plan de retour arrière en cas d'anomalie

Le FOURNISSEUR doit publier un registre des changements avec chaque version déployée et mettre à jour toute la documentation pertinente en conformité avec les changements induits (aide en ligne, guides d'utilisation, guides de formation, etc.).

1.8.4 Solution commerciale

La solution est une solution commerciale détenue par le FOURNISSEUR. Le FOURNISSEUR se réserve le droit de la faire évoluer. Toutes évolutions ou améliorations seront rendues disponibles dans un délai raisonnable pendant la validité du contrat.

Le processus de déploiement d'une mise à jour doit être convenu avec l'ORGANISME PUBLIC.

1.9 Certification

Une certification de la solution, effectuée par un organisme auditeur indépendant, doit également être réalisée à la demande de l'ORGANISME PUBLIC. Le fournisseur doit prévoir débourser un maximum de 25 000 $ pour obtenir cette certification. Les informations pour l'obtention de cette certification sont disponibles à l'adresse suivante :

http://ti.msss.gouv.qc.ca/Familles-de-services/Bureau-de-certification-et-dhomologation/Documents.aspx

Les efforts investis par le FOURNISSEUR dans le processus de certification et pour les corrections nécessaires à l'obtention de cette dernière sont à ses frais. Le FOURNISSEUR doit s'assurer que la certification est maintenue tout au long du contrat pour toutes les nouvelles versions déployées de la solution.

La certification doit avoir la même portée que le présent contrat. Elle doit impliquer la portion logicielle, plateforme et infrastructure.

2. Sécurité

2.1 Classification, analyse de préjudices et analyse de risques

Un processus de classification (cote DIC), d'analyse de préjudices et d'analyse de risques concernant la sécurité des actifs de ce contrat est en cours au sein de l'ORGANISME PUBLIC. Exceptionnellement, ce processus n'a pu être complété avant l'élaboration du présent contrat. Ce processus interne se terminera d'ici le 1er octobre 2021.

Pour donner suite à la complétion de ce processus interne, une série d'exigences techniques et administratives basées sur des normes de sécurité devront être appliquées par le FOURNISSEUR afin de sécuriser adéquatement l'environnement selon les meilleures pratiques de l'industrie. Un plan de résorption de la situation devra être acheminé à l'ORGANISME PUBLIC par le FOURNISSEUR 30 jours suivant la réception des exigences détaillées et complètes. L'ensemble des mesures de correction reliées aux exigences de sécurité devront être appliquées dans l'année suivant la signature du présent contrat selon un ordre de priorités définies par l'ORGANISME PUBLIC.

Le FOURNISSEUR doit rendre disponible son infrastructure à tout audit commandité par le MSSS.

Le FOURNISSEUR doit déposer au MSSS une architecture technologique de sécurité, et la maintenir à jour pour la durée du contrat.

Le FOURNISSEUR devra respecter les nouvelles exigences de sécurité qui pourraient subvenir pendant le contrat.

2.2 Protection des clés de chiffrement

Les clés publiques et privées, générées par l'ORGANISME PUBLIC et utilisées dans le cadre du déploiement de la preuve vaccinale pour la signature des codes QR, demeurent la propriété de l'ORGANISME PUBLIC et sous sa gouverne.

La protection des clés confiées au FOURNISSEUR doit se faire sous les conditions de sécurité de l'ORGANISME PUBLIC, se déclinant ainsi :

- La sécurité des clés doit être maintenue tout au long de son cycle de vie;
- Toute utilisation de clés privées doit être effectuée dans un module cryptographique conforme minimalement à la norme FIPS 140-2 Level 2 tel qu'un module cryptographique physique (HSM) (l'accès, le chiffrement, le déchiffrement, la signature, etc.).
- Les clés privées ne doivent jamais être stockées au format texte brut, ni échangées sous un quelconque prétexte, sans autorisation de l'ORGANISME PUBLIC.
- L'ORGANISME PUBLIC peut à tout moment exiger de consulter les journaux des accès, le FOURNISSEUR doit pouvoir fournir les journaux selon les modalités fixées par l'ORGANISME PUBLIC.

- Le FOURNISSEUR doit procéder à une sauvegarde de sécurité des clés sous sa garde, en respectant les conditions susmentionnées.

- La clé publique ne doit jamais perdre son intégrité, le FOURNISSEUR doit mettre en place des mécanismes lui permettant de garantir son intégrité tout au long de son cycle de vie. Le cas échéant, elle doit en outre la déposer dans un endroit unique accessible aux partenaires identifiés par l'ORGANISME PUBLIC, après y être autorisé.

- L'accès aux clés cryptographiques doit être restreint au plus petit nombre d'opérateurs possible, en général ceux qui sont chargés de la gestion de ces clés.

- Les clés cryptographiques doivent être stockées dans aussi peu d'emplacements que possible. Une liste spécifiant les lieux d'entreposage doit être dressée.

La solution du FOURNISSEUR :

- Ne doit pas autoriser ni accepter la substitution de clés de la part de sources non autorisées ou de processus inattendus.

- Doit distribuer les clés privées de manière sécurisée, c'est-à-dire que les clés sont uniquement distribuées aux individus chargés de leur gestion et qu'elles ne sont jamais distribuées en texte clair.

Le FOURNISSEUR doit avoir une documentation détaillée et communiquée des processus et des procédures de gestion des clés cryptographiques de la solution. Ces processus et procédures doivent intégrer ce qui suit :

- La génération de clés cryptographiques robustes,
- La sécurisation la distribution des clés cryptographiques,
- La sécurisation du stockage des clés cryptographiques,
- Les changements de clé cryptographique pour les clés ayant atteint la fin de leur cryptopériode (sur une base annuelle),
- La prévention de la substitution non autorisée des clés cryptographiques.

Les opérateurs chargés de la gestion de clés cryptographiques comprennent et acceptent leurs responsabilités et que celles-ci soient acceptées formellement en tant que telles.

En cas de conflit d'interprétation des mesures susmentionnées, celles-ci doivent être interprétées en se référant aux exigences de la norme PCI-DSS v.3.2.1.

2.3 Déclaration des incidents de sécurité

Le FOURNISSEUR doit déposer un processus documenté de gestion des incidents de sécurité. L'ORGANISME PUBLIC doit être informé immédiatement des incidents de sécurité et ces incidents doivent être pris en charge sans délais.

L'ORGANISME PUBLIC reconnaît les niveaux de sévérité suivants pour les incidents de sécurité :

Niveaux de sévérité	**Caractéristiques**
Mineur	• Affecte un secteur d'activité d'une des parties prenantes.
Modéré	• Affecte plusieurs secteurs d'une des parties prenantes.
Important	• Affecte plusieurs des parties prenantes.

	• Affecte de manière significative la qualité de services indispensables à la population. • Possède un potentiel fort de nuire à la réputation de l'ORGANISME PUBLIC. • Affecte le respect des droits fondamentaux des personnes à la protection de leurs renseignements personnels et de leur vie privée, sans porter atteinte à la santé, à la vie ou au bien-être de ces personnes.
Critique	• Un ou plusieurs services indispensables à la population ne peuvent être rendus. • Mets en danger la santé, la vie ou le bien-être de personnes. • Affecte le respect des droits fondamentaux des personnes à la protection de leurs renseignements personnels et de leur vie privée et, de ce fait, mets en danger la santé, la vie ou le bien-être de ces personnes. • Affecte la réputation d'une des parties prenantes, avec ou sans médiatisation.

L'ORGANISME PUBLIC reconnaît la classification suivante pour la déclaration des incidents de sécurité. Le FOURNISSEUR doit utiliser cette classification.

1. Atteinte à la sécurité physique : Incident caractérisé par un accès non autorisé à un périmètre physique contrôlé (ex. : centres de traitement) et résultant en des accès non autorisés à de l'information ou une perturbation de la disponibilité des infrastructures technologiques.

2. Code malicieux : Incident caractérisé par l'installation ou l'exécution réussie (infection) d'un code malicieux sur un système, une application ou un environnement. Les codes malicieux mis avec succès en quarantaine, notamment par un antivirus, ne doivent pas être rapportés.

3. Comportement inapproprié : Incident caractérisé par une négligence, une erreur, une omission ou le non-respect des règles de sécurité.

4. Cyberattaque : Incident caractérisé par un accès non autorisé et mal intentionné visant principalement à compromettre la confidentialité, l'intégrité ou la disponibilité de l'information ou des infrastructures technologiques.

5. 5. Dysfonctionnement technologique : Incident ayant pour cause des configurations déficientes de sécurité ou des pannes de l'infrastructure technologique ou application ayant des impacts sur la sécurité de l'information.

6. Vol ou perte d'information : Incident caractérisé par la perte ou le vol d'information sur papier ou support électronique (ex . : clé USB, ordinateur portatif).

La prise en charge des incidents de sécurité doit :

1. Identifier, signaler et enregistrer les incidents de sécurité;

2. Évaluer le niveau de sévérité et classifier les incidents de sécurité selon les échelles reconnues par l'ORGANISME PUBLIC.

3. Mettre en place une équipe d'intervention opérationnelle apte à prendre en charge et traiter les incidents de sécurité.

4. Mettre en place une procédure d'escalade administrative et opérationnelle qui tient compte du niveau de sévérité et de la classification des incidents de sécurité.

5. Mettre en place une démarche d'amélioration continue assurant notamment la prévention, la détection et la réaction.

6. Transmettre un bilan des incidents de sécurité ou rendre compte d'incidents de sécurité spécifiques sur demande de l'ORGANISME PUBLIC.

L'ORGANISME PUBLIC doit être informé immédiatement des incidents de sécurité.

3. Services d'entretien

3.1 Besoins

Le fournisseur doit inclure les services d'entretien de la solution pour toute la durée du contrat.

Le centre de support du FOURNISSEUR doit être capable de fournir des numéros de billets (incidents, requêtes, etc.) lors de l'ouverture d'appels ou de la réception de courriels. Le personnel du centre de support doit parler couramment le français.

Dans les quinze (15) jours suivant la signature du contrat, le FOURNISSEUR doit fournir le processus de prise en charge des demandes et sa façon d'assurer la disponibilité de ses ressources spécialisées afin d'assurer une résolution efficace des problèmes. Il doit également fournir son modèle de soutien.

3.2 Exigences en matière de soutien

Services de soutien :

Désigne un service de soutien technique permettant de répondre aux questions des utilisateurs et de résoudre les problèmes rencontrés lors de l'opération et de l'exploitation de la solution.

L'ORGANISME PUBLIC, les établissements du RSSS et le CSII (Centre de services informatiques intégrés) assument respectivement le soutien de premier et second niveau. Ils procèdent au tri des demandes d'assistance et à la résolution des incidents mineurs. Le CSII doit escalader les demandes d'assistance non résolues au troisième niveau, qui est administré par l'ORGANISME PUBLIC. Dans l'impossibilité de répondre, l'ORGANISME PUBLIC escalade à son tour la demande vers le FOURNISSEUR qui agit à titre de quatrième et dernier niveau.

Les services de soutien incluent un service de soutien technique pour la solution complète[1].

Tous les coûts relatifs à l'offre de services en matière de soutien doivent être inclus dans les coûts des services d'entretien.

Résolution des problèmes :

La résolution des problèmes implique nécessairement le retour à un « fonctionnement et à des performances normales ». Le FOURNISSEUR atteste qu'il s'engage à :

- Intervenir rapidement sur place afin de régler le problème et sa cause s'il ne peut le faire en utilisant un outil de prise de contrôle à distance;

- Prendre en charge les problèmes rencontrés et mettre en œuvre toutes les ressources humaines et matérielles nécessaires pour obtenir le rétablissement complet des services dans les meilleurs délais;

[1] Excluent le support des appareils mobiles physiques.

- Maintenir l'intégrité de la configuration de la solution durant l'intervention visant la résolution du problème;

- Faire en sorte que les correctifs apportés n'entrainent pas de diminution de service ou de nouveaux problèmes.

Le FOURNISSEUR doit prévoir des méthodes d'intervention en cas de problème ou de panne permettant de continuer à fonctionner tout en corrigeant la situation rapidement.

Couverture du soutien

Le FOURNISSEUR s'engage à fournir un support téléphonique ainsi qu'un système de billets d'assistance sur les heures normales d'affaires (HNA), soit de 9h00 à 17h00, excluant les fins de semaine et jours fériés, en français, selon les modalités suivantes :

- La couverture durant les HNA : le FOURNISSEUR offre un soutien pour traiter les requêtes de toutes priorités et pour l'ensemble de la solution.

- La couverture en dehors des HNA : incluant les jours de fin de semaine et les jours fériés, le FOURNISSEUR offre un service de support par billets d'assistance pour prendre en note les requêtes de toutes priorités. Les requêtes déposées seront alors réputées l'être au prochain jour ouvrable. La réponse aux requêtes soumises sera ensuite traitée dès la prochaine HNA en respectant les délais de réponse et de résolution établis ci-après.

Niveau de priorité des requêtes

Un niveau de priorité est assigné à chacune des requêtes de soutien reçues par le FOURNISSEUR. L'assignation du niveau de priorité se fait conjointement par le FOURNISSEUR et l'ORGANISME PUBLIC en tenant compte de la sévérité et de l'impact sur les opérations. Si l'ORGANISME PUBLIC se trouve en désaccord avec la priorité assignée, il doit en référer immédiatement au FOURNISSEUR selon la procédure d'escalade. Les niveaux de priorité sont définis comme suit :

Priorité de niveau 1

Problème rapporté sur l'environnement de production faisant en sorte que la solution dans son ensemble, ou qu'une ou des fonctions critiques de la solution, sont (a) non opérationnelles ou (b) opèrent d'une manière qui peut compromettre l'intégrité des données de production ou (c) opèrent d'une manière qui peut compromettre la sécurité des citoyens.

Priorité de niveau 2

Problème rapporté sur l'environnement de production faisant en sorte qu'une ou des fonctions non critiques du système sont (a) non opérationnelles et (b) opèrent d'une manière qui peut compromettre l'intégrité des données de production ou causer de sérieux inconvénients à l'ORGANISME PUBLIC.

Priorité de niveau 3

Problème rapporté sur l'environnement de production faisant en sorte qu'une ou des fonctions de la solution sont (a) non opérationnelles ou opèrent d'une manière non conforme aux spécifications ou à la documentation et (b) pour lequel il existe une procédure de contournement manuel, acceptable pour l'établissement, pendant le temps de résolution.

Priorité de niveau 4

Problème rapporté sur un environnement autre que production, demande d'information ou demande de changement.

Temps de réponse et temps de résolution

Suite à l'ouverture d'une requête par l'ORGANISME PUBLIC, le FOURNISSEUR s'engage à offrir le service de soutien dans un temps inférieur ou égal à :

Pour les utilisateurs du portail de la preuve vaccinale :

	Temps de réponse		Temps de résolution	
Priorité	**Du lundi au vendredi selon les HNA**	**En dehors de ces heures**	**Du lundi au vendredi, selon les HNA**	**En dehors de ces heures**
1	**1 heure**	**N/A**	**16 heures**	**N/A**
2	**4 heures**	**N/A**	**32 heures**	**N/A**
3	**8 heures**	**N/A**	**14 jours**	**N/A**
4	**16 heures**	**N/A**	**30 jours**	**N/A**

Pour les utilisateurs des applications mobiles :

	Temps de réponse		Temps de résolution	
Priorité	**Du lundi au vendredi selon les HNA**	**En dehors de ces heures**	**Du lundi au vendredi, selon les HNA**	**En dehors de ces heures**
1	**1 heure**	**N/A**	**16 heures**	**N/A**
2	**4 heures**	**N/A**	**32 heures**	**N/A**
3	**8 heures**	**N/A**	**14 jours**	**N/A**
4	**16 heures**	**N/A**	**30 jours**	**N/A**

Définition du temps de réponse

Désigne le temps entre l'ouverture de la requête par l'ORGANISME PUBLIC et le retour par un expert logiciel qualifié du FOURNISSEUR. Pour les requêtes qui sont soumises en dehors des HNA, le calcul du temps de réponse débute à la prochaine HNA suivant l'ouverture de la requête.

Définition du temps de résolution

Signifie le temps entre le moment utilisé pour débuter le calcul du temps de réponse et celui où le problème est résolu selon une des avenues suivantes :

- Un correctif est installé dans l'environnement de production et l'ORGANISME PUBLIC certifie que le problème est résolu;
- Le FOURNISSEUR livre une procédure de contournement durable à long terme acceptable pour l'ORGANISME PUBLIC;
- L'ORGANISME PUBLIC reçoit une réponse satisfaisante à sa demande d'information;
- Le FOURNISSEUR confirme que la requête est une demande de changement.

Procédure d'escalade

Le FOURNISSEUR doit fournir une procédure d'escalade. Cette procédure est disponible pour l'ORGANISME PUBLIC. Si le FOURNISSEUR est dans l'incapacité d'établir la cause du problème et/ou de déterminer la période nécessaire pour le régler, il doit immédiatement en informer l'ORGANISME PUBLIC qui peut alors avoir recours à la procédure d'escalade.

Ce livrable doit être approuvé par l'ORGANISME PUBLIC selon les modalités d'approbation des biens livrables.

Exigences sur l'offre de services en matière de soutien

Le soutien est accessible aux employés de l'ORGANISME PUBLIC ayant été désignés par ce dernier pour agir comme interlocuteurs en ce qui a trait à l'installation ou à l'utilisation de la solution. Il n'y a pas de limite quant au nombre de requêtes pouvant être effectués par ces ressources pour obtenir le soutien technique.

Dans l'éventualité où le FOURNISSEUR aurait à se déplacer pour résoudre un problème, aucuns frais supplémentaires (de séjour, de repas ou de déplacement) ne peut être chargés. Si le problème est causé par l'environnement de l'ORGANISME PUBLIC (ex. : ordinateur, connexion réseaux, etc.), l'ORGANISME PUBLIC sera responsable de rembourser les frais supplémentaires pour le déplacement.

Le FOURNISSEUR doit inclure un processus de prise en charge des requêtes et les mécanismes permettant d'assurer la disponibilité de ses ressources spécialisées pendant la période de couverture du soutien afin d'assurer une résolution efficace des problèmes.

3.3 Services de maintenance

Le FOURNISSEUR doit inclure les services de maintenance de la solution pour la durée du contrat, incluant les renouvellements le cas échéant. La maintenance inclut tout rehaussement ainsi que toute amélioration à la solution dont notamment, la correction des erreurs empêchant le logiciel de fonctionner selon les spécifications (problème), ainsi que des mises à jour de la solution, incluant les fonctionnalités génériques que le FOURNISSEUR peut ajouter de temps à autre au logiciel.

Une procédure formelle de maintenance corrective (correction des erreurs dans le progiciel) doit être établie, documentée et suivie. Elle doit prévoir les moyens de revenir à la situation antérieure en cas de problème.

Le FOURNISSEUR doit rendre disponibles les nouvelles versions de sa solution en temps opportun. Il doit livrer des versions qui s'adaptent aux modifications des logiciels tiers (systèmes sources) afin de maintenir la compatibilité. Il doit rendre disponibles les correctifs (rustines) dans un délai acceptable (huit (8) semaines maximum pour se conformer à la sécurité et pour l'adaptation aux changements dans le système d'exploitation). La distribution des correctifs doit être automatisée autant que possible.

La solution doit inclure l'ensemble des outils et des processus nécessaires à la maintenance, à la gestion des versions et à la gradation des composantes afin de mettre en place un processus de contrôle des versions.

Tous les coûts relatifs à l'offre de services en matière de maintenance doivent être inclus dans les coûts des services d'entretien.

ANNEXE 3 – DESCRIPTION DES BESOINS : TEST D'INTRUSION

1. Volet test d'intrusion

1.1. Recommandation critères sélection d'une compagnie

La compagnie mandatée pour effectuer un test d'intrusion (pentest) doit être en mesure d'effectuer un test de méthode manuel. Un balayage de vulnérabilité tel que des scanners est considéré comme une addition et non comme étant un facteur déterminant.

Une compagnie offrant ce service spécialisé reconnu et établie dans le milieu est fortement suggérée.

1.2. Critère test effectué

L'organisme chargé d'effectuer le test d'intrusion doit être en mesure de valider les vulnérabilités du 'top 10' de l'Open Web Application Security Project (OWASP) version 2021 ou plus récente. Il est un atout si la compagnie peut effectuer au-delà de ce 'top 10'.

Si possible, la compagnie doit être capable de procéder à de la lecture de code afin d'y détecter des possibles risques et vulnérabilités.

Dans le cas d'un test d'application mobile, la compagnie doit être apte à effectuer ce genre de test.

1.3. Rapport

Si un pentest récent a déjà été fait, une copie du rapport doit être acheminée au MSSS et au Centre Opérationnel Cyberdéfense (COCD). Le rapport doit représenter une version de l'application qui reflète la version de production.

Le rapport doit soulever les risques, les faiblesses, les impacts, la difficulté d'exploitation et des recommandations de mitigations. Des preuves de concepts dans le rapport sont considérées comme un atout.

1.4. Récurrence des tests

Un mandat de test d'intrusion doit être planifié lors de chaque changement majeur ou ajout de fonctionnalité qui pourrait mettre en risque l'application.

Un test annuel est suggéré, mais non exigé. Cependant, un test annuel permet de s'assurer d'un contrôle de désuétude des versions utilisées par l'application ou de valider à une vulnérabilité qui serait présente mais mitigée par une rustine.

ANNEXE 4 - DÉCLARATION CONCERNANT LES ACTIVITES DE LOBBYISME EXERCEES AUPRES DE L'ORGANISME PUBLIC RELATIVEMENT A L'ATTRIBUTION DU CONTRAT DE GRÉ A GRÉ

N° : **21-0275-COVID**

TITRE DU PROJET : LE DEVELOPPEMENT D'UNE PREUVE VACCINALE ET DU PASSEPORT VACCINAL DES CITOYENS QUEBECOIS.

JE, SOUSSIGNE(E), **ALEXANDER DAHL**, **PRESIDENT**,

(NOM ET TITRE DE LA PERSONNE AUTORISEE PAR LE CONTRACTANT)

PRESENTE AU MINISTERE DE LA SANTE ET DES SERVICES SOCIAUX, ATTESTE QUE LES DECLARATIONS CI-APRES SONT VRAIES ET COMPLETES A TOUS LES EGARDS, AU NOM DE :

AKINOX SOLUTIONS INC.,

(NOM DU CONTRACTANT)

(CI-APRES APPELE LE « CONTRACTANT »).

JE DECLARE CE QUI SUIT :

1. J'AI LU ET JE COMPRENDS LE CONTENU DE LA PRESENTE DECLARATION.

2. JE SUIS AUTORISE(E) PAR LE CONTRACTANT A SIGNER LA PRESENTE DECLARATION.

3. LE CONTRACTANT DECLARE (INDIQUER L'UNE OU L'AUTRE DES DECLARATIONS SUIVANTES) :

   A. QUE PERSONNE N'A EXERCE POUR SON COMPTE, QUE CE SOIT A TITRE DE LOBBYISTE D'ENTREPRISE OU DE LOBBYISTE-CONSEIL OU DE LOBBYISTE D'ORGANISATION, DES ACTIVITES DE LOBBYISME, AU SENS DE LA LOI SUR LA TRANSPARENCE ET L'ETHIQUE EN MATIERE DE LOBBYISME (RLRQ, CHAPITRE T-11.011) ET DES AVIS EMIS PAR LE COMMISSAIRE AU LOBBYISME*, PREALABLEMENT A CETTE DECLARATION RELATIVEMENT A LA PRESENTE ATTRIBUTION DU CONTRAT;

   B. QUE DES ACTIVITES DE LOBBYISME, AU SENS DE LA LOI SUR LA TRANSPARENCE ET L'ETHIQUE EN MATIERE DE LOBBYISME ET DES AVIS EMIS PAR LE COMMISSAIRE AU LOBBYISME*, ONT ETE EXERCEES POUR SON COMPTE ET QU'ELLES L'ONT ETE EN CONFORMITE AVEC CETTE LOI, AVEC CES AVIS AINSI QU'AVEC LE CODE DE DEONTOLOGIE DES LOBBYISTES*, PREALABLEMENT A CETTE DECLARATION RELATIVEMENT A LA PRESENTE ATTRIBUTION DU CONTRAT (RLRQ, CHAPITRE T-11.011, R.2).

   VEUILLEZ CHOISIR UNE **LETTRE (A OU B)** : ___**A**___.

4. JE RECONNAIS QUE, SI L'ORGANISME PUBLIC A DES MOTIFS RAISONNABLES DE CROIRE QUE DES COMMUNICATIONS D'INFLUENCE NON CONFORMES À LA LOI SUR LA TRANSPARENCE ET L'ÉTHIQUE EN MATIÈRE DE LOBBYISME ET AU CODE DE DÉONTOLOGIE DES LOBBYISTES* ONT EU LIEU POUR OBTENIR LE CONTRAT, UNE COPIE DE LA PRÉSENTE DÉCLARATION POURRA ÊTRE TRANSMISE AU COMMISSAIRE AU LOBBYISME PAR L'ORGANISME PUBLIC.

ET J'AI SIGNE, ____ [redacted]

(SIGNATURE ET DATE)

* LA LOI, LE CODE ET LES AVIS EMIS PAR LE COMMISSAIRE AU LOBBYISME SONT DISPONIBLES A CETTE ADRESSE : WWW.COMMISSAIRELOBBY.QC.CA.

ANNEXE 5 – ENGAGEMENT DE CONFIDENTIALITÉ

TITRE DU CONTRAT : LE DEVELOPPEMENT D'UNE PREUVE VACCINALE ET DU PASSEPORT VACCINAL DES CITOYENS QUEBECOIS.

Je, soussigné(e), Alexander Dahl, exerçant mes fonctions au sein de AKINOX Solutions Inc., déclare formellement ce qui suit :

1. Je suis un(e) employé(e) de cette entreprise et, à ce titre, j'ai été affecté(e) à l'exécution du mandat faisant l'objet du contrat de services entre le ministre de la Santé et des Services sociaux et mon employeur en date du 2021-09-01;

2. Je m'engage, sans limite de temps, à garder le secret le plus entier, à ne pas communiquer ou permettre que soit communiqué à quiconque quelque renseignement ou document, quel qu'en soit le support, qui me sera communiqué ou dont je prendrai connaissance dans l'exercice ou à l'occasion de l'exécution de mes fonctions, à moins d'avoir été dûment autorisé à le faire par le ministre de la Santé et des Services sociaux ou par l'un de ses représentants autorisés. À cet effet;

   2.1 Je comprends que les clés privées et publiques, générées par le MSSS soient utilisées dans le cadre du déploiement de la preuve vaccinale, notamment dans la signature des codes QR, demeurent la propriété du MSSS et sous sa gouverne.

   2.2 Je comprends que la protection des clés confiées à AKINOX doit se faire sous les conditions de sécurité du MSSS, se déclinant ainsi :

      a. La sécurité des clés doit être maintenue tout au long de son cycle de vie;

      b. Toute utilisation de clés privées doit être effectuée dans un module cryptographique conforme minimalement à la norme FIPS 140-2 Level 2 tel qu'un module cryptographique physique (HSM) (l'accès, le chiffrement, le déchiffrement, la signature, etc.);

      c. Les clés privées ne doivent jamais être stockées au format texte brut ni échangées sous un quelconque prétexte, sans autorisation du MSSS;

      d. Le MSSS peut à tout moment exiger de consulter les journaux des accès, AKINOX doit pouvoir fournir les journaux selon les modalités fixées par le MSSS;

      e. AKINOX doit procéder à une sauvegarde de sécurité des clés sous sa garde, en respectant les conditions susmentionnées;

      f. La clé publique ne doit jamais perdre son intégrité, AKINOX doit mettre en place des mécanismes lui permettant de garantir son intégrité tout au long de son cycle de vie. Le cas échéant, elle doit en outre la déposer dans un endroit unique accessible aux partenaires identifiés par le MSSS, après y être autorisé;

      g. L'accès aux clés cryptographiques doit être restreint au plus petit nombre d'opérateurs possible, en général ceux qui sont chargés de la gestion de ces clés;

      h. Les clés cryptographiques doivent être stockées dans aussi peu d'emplacements que possible. Une liste spécifiant les lieux d'entreposage doit être dressée;

2.3 Je comprends que la solution :

a. Ne dois pas autoriser ni accepter la substitution de clés de la part de sources non autorisées ou de processus inattendus;

b. Dois distribuer les clés privées de manière sécurisée, c'est-à-dire que les clés sont uniquement distribuées aux individus chargés de leur gestion et qu'elles ne sont jamais distribuées en texte clair.

2.4 Je comprends qu'AKINOX doit avoir une documentation détaillée et communiquée des processus et des procédures de gestion des clés cryptographiques de la solution. Ces processus et procédures doivent intégrer ce qui suit :

a. La génération de clés cryptographiques robustes;

b. La sécurisation la distribution des clés cryptographiques;

c. La sécurisation du stockage des clés cryptographiques;

d. Les changements de clé cryptographique pour les clés ayant atteint la fin de leur cryptopériode (sur une base annuelle);

e. La prévention de la substitution non autorisée des clés cryptographiques.

2.5 Je m'engage à ce que les opérateurs chargés de la gestion de clés cryptographiques comprennent et acceptent leurs responsabilités et que celles-ci soient acceptées formellement en tant que telles.

2.6 En cas de conflit d'interprétation des mesures susmentionnées, celles-ci doivent être interprétées en se référant aux exigences de la norme PCI-DSS v.3.2.1.

2.7 Le fournisseur, AKINOX, s'engage à rendre disponible son infrastructure à tout audit commandité par le MSSS.

2.8 Le fournisseur, AKINOX, s'engage à déposer au MSSS une architecture de sécurité, et la maintenir à jour pour la durée du contrat.

2.9 Le fournisseur, AKINOX, s'engage à respecter de nouvelles exigences de sécurité qui pourraient subvenir pendant le contrat.

3. Je m'engage également, sans limite de temps, à ne pas faire usage d'un tel renseignement ou document à une fin autre que celle s'inscrivant dans le cadre des rapports contractuels entretenus avec le ministère de la Santé et des Services sociaux.

4. J'ai été informé(e) que le défaut par le (la) soussigné(e) de respecter tout ou partie du présent engagement de confidentialité m'expose à des recours légaux, des réclamations, des poursuites et toute autre procédure en raison du préjudice causé pour quiconque est concerné par le contrat précité;

5. Je confirme avoir lu les termes du présent engagement et en avoir saisi toute la portée.

[redacted]

(Signature du déclarant ou de la déclarante)

Commission d'accès à l'information du Québec

ANNEXE 6 – FICHE D'INFORMATION SUR LA DESTRUCTION DES DOCUMENTS CONTENANT DES RENSEIGNEMENTS PERSONNELS

Tout organisme ou toute entreprise privée qui recueillent, détiennent, utilisent ou communiquent des renseignements personnels doivent mettre en place des mesures de sécurité propres à préserver le caractère confidentiel de ces données. Cette obligation découle à la fois de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et de la *Loi sur la protection des renseignements personnels dans le secteur privé*. À la suite d'incidents majeurs qui lui ont été signalés, la Commission d'accès à l'information a réfléchi sur les moyens à prendre pour assurer la protection du caractère confidentiel des renseignements personnels au moment de leur destruction.

Au sein de l'organisme ou de l'entreprise, il est important que chaque employé, à son poste de travail, se sente responsable d'assurer la protection des renseignements personnels qu'il traite. C'est ainsi qu'il ne doit pas jeter au rebut les documents, cartes de mémoire flash, clés USB, disques durs d'ordinateur, CD, DVD, etc. qui en contiennent, sans s'être assuré au préalable que leur contenu ne peut être reconstitué.

La Commission suggère aux organismes et entreprises de désigner une personne qui sera responsable de mettre en place et de surveiller l'application d'une politique sur la destruction de documents contenant des renseignements personnels.

Le déchiquetage de documents sur support papier, le formatage de médias numériques réutilisables et la destruction physique de médias numériques non réutilisables demeurent les meilleures méthodes de destruction des documents confidentiels. Si les spécifications techniques de la déchiqueteuse de l'entreprise ne répondent pas au volume des documents sur support papier à détruire, il faut les entreposer dans un endroit fermé à clef avant de les confier à une entreprise spécialisée de récupération de papier.

La Commission voit mal comment la destruction des documents contenant des renseignements personnels puisse s'effectuer sur la foi d'une simple entente verbale. Aussi, un contrat en bonne et due forme concernant la destruction des documents devrait-il contenir au moins des clauses spécifiant :

- le procédé utilisé pour la destruction des documents;
- la nécessité d'un accord préalable entre les parties avant de confier la destruction des documents confidentiels à un sous-contractant;
- les pénalités aux dépens de l'entreprise de récupération si elle ne respecte pas ses engagements.

En outre, dans ce même contrat, la Commission est d'avis que l'entreprise de récupération devrait :

- reconnaître que les renseignements personnels contenus dans les documents sont de nature confidentielle;
- faire signer un engagement à la confidentialité à toute personne qui aura à manipuler ces documents;
- s'engager à ce que les documents soient entreposés dans des locaux sécuritaires et qu'ils soient toujours sous bonne garde jusqu'à leur destruction;
- veiller à limiter de façon très stricte l'accès aux lieux où les documents sont entreposés ou transformés;
- s'engager à ne pas céder les documents en sa possession à des tiers à des fins autres que la transformation du papier préalablement et obligatoirement déchiqueté;
- assurer à son client le droit d'avoir accès en tout temps à ses installations, toute la durée du contrat;
- voir à la destruction totale des documents qui ne font pas l'objet d'une transformation;
- faire rapport à son client lors de la destruction des documents reçus.

ANNEXE **7 –** ATTESTATION DE DESTRUCTION DES RENSEIGNEMENTS PERSONNELS ET CONFIDENTIELS

Je, soussigné(e), _____
(Prénom et nom de l'employé(e))

exerçant mes fonctions au sein de _____

dont le bureau principal est situé à l'adresse _____

_____,

déclare solennellement que je suis dûment autorisé(e) à certifier que les renseignements personnels et confidentiels communiqués par le ministre ou toute autre personne dans le cadre du projet octroyé à

_____
(Nom du fournisseur de services)

et qui prend fin le _____, ont été détruits selon les méthodes suivantes :
(Date)

Cochez les cases appropriées :

☐	par déchiquetage : renseignements sur support papier
☐	par destruction logique et effacement physique en utilisant un logiciel de réécriture : renseignements sur support informatique
☐	par un autre mode de destruction : préciser le support et le mode de destruction _____ _____ _____ _____ _____

EN FOI DE QUOI, J'AI SIGNÉ À _____, CE _____ JOUR DU MOIS DE _____DE L'AN _____.

_____
(Signature de l'employé(e))

À remplir seulement après la destruction des renseignements. Cependant, vous devez cocher une des cases de l'article 13 du contrat, au moment de sa signature.