Ministère
de la Cybersécurité
et du Numérique
Québec

Direction générale du secrétariat général

PAR COURRIEL

Québec, le 22 juin 2022

[redacted]

Réf. : 2022-06

Objet : **Votre demande en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels,* (RLRQ, chapitre A-2.1)**

Monsieur,

Par la présente, nous donnons suite à votre demande d'accès, le 3 juin 2022, visant à obtenir :

1. Une copie de tous les contrats et mandats offerts à des firmes externes depuis 2 ans et qui visent à réaliser des tests d'intrusion sur les systèmes informatiques du gouvernement.

2. Tout rapport ou document nature semblable, produit à l'interne ou par une firme externe, depuis 2 ans, réalisé à la suite de tests d'intrusion sur les systèmes informatiques du gouvernement.

En réponse au point 1 de votre demande, considérant la création du MCN le 1er janvier 2022, nous vous transmettons le seul document repéré par la Direction générale du Centre gouvernemental de cyberdéfense depuis cette date. Nous avons élagué, sur deux (2) des pages communiquées, des renseignements personnels en application des articles 53, 54 et 57 de la Loi sur l'accès.

Nous avons également élagué, sur une (1) des pages comuniquées, un renseignement de nature confidentielle en application des articles 23 et 24 de la Loi sur l'accès. En effet, il s'agit d'un renseignement dont la divulgation risquerait de nuire de façon substantielle à la compétitivité de cette entreprise.

….2

900, place D'Youville, 9e étage
Québec (Québec) G1R 3P7
Téléphone : 418 644-1030
acces@mcn.gouv.qc ca

Concernant le point 2 de votre demande, nous vous informons que les documents repérés par la Direction générale du Centre gouvernemental de cyberdéfense ne vous sont pas accessible en application des articles 14, 29 et 37 de la Loi sur l'accès. En effet, ces documents contiennent des recommandations et des informations qui, une fois divulguées, pourrait avoir pour effet de réduire l'efficacité d'un dispositif de sécurité destiné à la protection d'un bien, en l'occurrence, des systèmes et infrastructures informatiques.

Conformément à l'article 51 de la Loi sur l'accès, nous vous informons que vous avez trente (30) jours à compter de ce jour pour exercer un recours en révision de cette décision auprès de la Commission d'accès à l'information. Vous trouverez en pièce jointe l'avis vous informant de ce recours.

Je vous prie d'agréer, Monsieur, nos salutations distinguées.

La responsable de l'accès aux documents
et de la protection des renseignements personnels,

Renée Giguère

p. j. Articles de la loi et avis de recours en révision

AVIS DE RECOURS

À la suite d'une décision rendue en vertu de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnel (RLRQ, chapitre A-2.1)

Révision par la Commission d'accès à l'information

a) Pouvoir

L'article 135 de la Loi prévoit qu'une personne dont la demande écrite a été refusée en tout ou en partie par le responsable de l'accès aux documents ou de la protection des renseignements personnels peut demander à la Commission d'accès à l'information de réviser cette décision.

La demande de révision doit être faite par écrit. Elle peut exposer brièvement les raisons pour lesquelles la décision devrait être révisée (art. 137).

L'adresse de la Commission d'accès à l'information est la suivante :

Québec	Bureau 2.36 525, boulevard René—Lévesque Est Québec (Québec) G1R 5S9	Tél. : 418 528-7741 Sans frais 1 888 528-7741	Télécopieur : 418 529-3102
Montréal	Bureau 900 2045, rue Stanley Montréal (Québec) H3A 2V4	Tél. : 514 873-4196 Sans frais 1 888 528-7741	Télécopieur : 514 844-6170
Courriel	cai.communications@cai.gouv.qc.ca		

b) Motifs

Les motifs relatifs à la révision peuvent porter sur la décision, sur le délai de traitement de la demande, sur le mode d'accès à un document ou à un renseignement, sur les frais exigibles ou sur l'application de l'article 9 (notes personnelles inscrites sur un document, esquisses, ébauches, brouillons, notes préparatoires ou autres documents de même nature qui ne sont pas considérés comme des documents d'un organisme public).

c) Délais

Les demandes de révision doivent être adressées à la Commission d'accès à l'information dans les 30 jours suivant la date de la décision ou de l'expiration du délai accordé au responsable pour répondre à une demande (art. 135).

La Loi prévoit spécifiquement que la Commission d'accès à l'information peut, pour un motif raisonnable, relever le requérant du défaut de respecter le délai de 30 jours (art. 135).

Extraits de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels
(RLRQ, c. A-2.1)

CHAPITRE II
ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS

SECTION II
RESTRICTIONS AU DROIT D'ACCÈS

14. Un organisme public ne peut refuser l'accès à un document pour le seul motif que ce document comporte certains renseignements qu'il doit ou peut refuser de communiquer en vertu de la présente loi.

Si une demande porte sur un document comportant de tels renseignements, l'organisme public peut en refuser l'accès si ces renseignements en forment la substance. Dans les autres cas, l'organisme public doit donner accès au document demandé après en avoir extrait uniquement les renseignements auxquels l'accès n'est pas autorisé.
1982, c. 30, a. 14.

23. Un organisme public ne peut communiquer le secret industriel d'un tiers ou un renseignement industriel, financier, commercial, scientifique, technique ou syndical de nature confidentielle fourni par un tiers et habituellement traité par un tiers de façon confidentielle, sans son consentement.
1982, c. 30, a. 23.

24. Un organisme public ne peut communiquer un renseignement fourni par un tiers lorsque sa divulgation risquerait vraisemblablement d'entraver une négociation en vue de la conclusion d'un contrat, de causer une perte à ce tiers, de procurer un avantage appréciable à une autre personne ou de nuire de façon substantielle à la compétitivité de ce tiers, sans son consentement.
1982, c. 30, a. 24.

29. Un organisme public doit refuser de confirmer l'existence ou de donner communication d'un renseignement portant sur une méthode ou une arme susceptible d'être utilisée pour commettre un crime ou une infraction à une loi.

Il doit aussi refuser de confirmer l'existence ou de donner communication d'un renseignement dont la divulgation aurait pour effet de réduire l'efficacité d'un programme, d'un plan d'action ou d'un dispositif de sécurité destiné à la protection d'un bien ou d'une personne.
1982, c. 30, a. 29; 2006, c. 22, a. 16.

37. Un organisme public peut refuser de communiquer un avis ou une recommandation faits depuis moins de dix ans, par un de ses membres, un membre de son personnel, un membre d'un autre organisme public ou un membre du personnel de cet autre organisme, dans l'exercice de leurs fonctions.

Il peut également refuser de communiquer un avis ou une recommandation qui lui ont été faits, à sa demande, depuis moins de dix ans, par un consultant ou par un conseiller sur une matière de sa compétence.
1982, c. 30, a. 37.

CHAPITRE III
PROTECTION DES RENSEIGNEMENTS PERSONNELS

SECTION I
CARACTÈRE CONFIDENTIEL DES RENSEIGNEMENTS PERSONNELS

53. Les renseignements personnels sont confidentiels sauf dans les cas suivants:

1° la personne concernée par ces renseignements consent à leur divulgation; si cette personne est mineure, le consentement peut également être donné par le titulaire de l'autorité parentale;

2° ils portent sur un renseignement obtenu par un organisme public dans l'exercice d'une fonction juridictionnelle; ils demeurent cependant confidentiels si l'organisme les a obtenus alors qu'il siégeait à huis-clos ou s'ils sont visés par une ordonnance de non-divulgation, de non-publication ou de non-diffusion.
1982, c. 30, a. 53; 1985, c. 30, a. 3; 1989, c. 54, a. 150; 1990, c. 57, a. 11; 2006, c. 22, a. 29.

54. Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier.
1982, c. 30, a. 54; 2006, c. 22, a. 110.

57. Les renseignements personnels suivants ont un caractère public:

1° le nom, le titre, la fonction, la classification, le traitement, l'adresse et le numéro de téléphone du lieu de travail d'un membre d'un organisme public, de son conseil d'administration ou de son personnel de direction et, dans le cas d'un ministère, d'un sous-ministre, de ses adjoints et de son personnel d'encadrement;

2° le nom, le titre, la fonction, l'adresse et le numéro de téléphone du lieu de travail et la classification, y compris l'échelle de traitement rattachée à cette classification, d'un membre du personnel d'un organisme public;

3° un renseignement concernant une personne en sa qualité de partie à un contrat de services conclu avec un organisme public, ainsi que les conditions de ce contrat;

4° le nom et l'adresse d'une personne qui bénéficie d'un avantage économique conféré par un organisme public en vertu d'un pouvoir discrétionnaire et tout renseignement sur la nature de cet avantage;

5° le nom et l'adresse de l'établissement du titulaire d'un permis délivré par un organisme public et dont la détention est requise en vertu de la loi pour exercer une activité ou une profession ou pour exploiter un commerce.

Toutefois, les renseignements personnels prévus au premier alinéa n'ont pas un caractère public si leur divulgation est de nature à nuire ou à entraver le travail d'un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime. De même, les renseignements personnels visés aux paragraphes 3° et 4° du premier alinéa n'ont pas un caractère public dans la mesure où la communication de cette information révélerait un renseignement dont la communication doit ou peut être refusée en vertu de la section II du chapitre II.

En outre, les renseignements personnels prévus au paragraphe 2° ne peuvent avoir pour effet de révéler le traitement d'un membre du personnel d'un organisme public.
1982, c. 30, a. 57; 1985, c. 30, a. 4; 1990, c. 57, a. 12; 1999, c. 40, a. 3; 2006, c. 22, a. 31.

Ministère
de la Cybersécurité
et du Numérique
Québec

CONTRAT DE SERVICES PROFESSIONNELS

GRÉ À GRÉ

RÉALISATIONI DE TESTS D'INTRUSION

NUMÉRO DU CONTRAT : ~~94600717~~ 96400717

ENTRE

LE MINISTRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE, pour et au nom du gouvernement du Québec, M. Dave Roussy**,** directeur général du centre gouvernemental de cyberdéfense dûment autorisé par application de la Loi édictant la Loi sur le ministère de la Cybersécurité et du Numérique et modifiant d'autres dispositions (2021, chapitre 33), dont les bureaux sont situés au 880, chemin Sainte-Foy, 10e étage, Québec (Québec) G1S 2L2

ci-après appelé « le ministre »,

ET

OKIOK DATA LTÉE, personne morale légalement constituée dont le numéro d'entreprise du Québec (NEQ) est 1177161727, ayant son siège social au 655, promenade du Centropolis, porte 230, Laval, (Québec) H7T 0A3, agissant par M. Michel De Marinis, vice-président ventes et marketing, dûment autorisé ainsi qu'il le déclare,

ci-après appelé « prestataire de services ».

1. INTERPRÉTATION

1.1 Documents contractuels

Le contrat est constitué des documents suivants :

1) le cas échéant, le contrat, les demandes d'exécution ainsi que les avenants;
2) la description des besoins élaborée par le ministre présentée à l'annexe 6;

En cas de conflit entre les termes de l'un ou l'autre de ces documents, les termes du document qui figure en premier dans la liste prévalent sur ceux des documents qui le suivent.

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.

1.2 Lois applicables et tribunal compétent

Le contrat est régi par le droit applicable au Québec et, en cas de contestation, les tribunaux du Québec sont seuls compétents. Tout recours doit être intenté dans le cadre du présent contrat dans le district judiciaire de Québec.

2. REPRÉSENTANT DES PARTIES

Le ministre aux fins de l'application du présent contrat, y compris pour toute approbation qui y est requise, désigne Francis Provencher, directeur de la prévention, de la détection et de la gestion des incidents, pour le représenter. Si un remplacement était rendu nécessaire, le ministre en avise le prestataire de services dans les meilleurs délais.

De même, le prestataire de services désigne Anderson Ortega, Directeur – Développement commercial pour le représenter. Si un remplacement était rendu nécessaire, le prestataire de services en avise le ministre dans les meilleurs délais.

3. OBJET DU CONTRAT

Le ministre retient les services du prestataire de services dans le cadre de « Réalisation de tests d'intrusion », conformément au présent contrat.

Le prestataire de services est tenu de réaliser les travaux requis par le ministre, conformément aux exigences énoncées dans la description présentée à l'annexe 6 du présent contrat.

Malgré ce qui précède, le prestataire de services accepte que le ministre retire un ou des biens livrables sans pénalité.

4. DURÉE DU CONTRAT

Le présent contrat à exécution sur demande débute le 16 mai 2022 pour se terminer le 15 décembre 2022.

Le premier des événements suivants met fin au contrat :

- la date de fin du contrat;
- l'atteinte du montant maximal du contrat.

5. MONTANT DU CONTRAT

Le prestataire de services est rémunéré au taux horaire de [redacted]

Le montant maximal du contrat est fixé à 93 960 $.

Le montant maximal du contrat comprend les honoraires, les autres frais administratifs du prestataire de services et les frais de transport et de séjour encourus dans l'exécution du contrat.

6. MODALITÉS DE PAIEMENT

Le paiement s'effectue mensuellement, sur présentation de facture, selon les modalités de paiement qui suivent. Les factures doivent contenir de façon générale les informations suivantes : la date, le numéro de contrat, le numéro de la demande d'exécution (DE), la description des travaux et des biens livrables réalisés, le nom de la ou des ressources, le nombre d'heures de services rendus; le taux horaire.

Après vérification, le ministre verse les sommes dues au prestataire de services 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.

7. AUTORISATION DE CONTRACTER

En cours d'exécution du présent contrat, dans l'éventualité où le montant de la dépense est inférieur au montant déterminé par le gouvernement au regard de l'obligation de détenir une autorisation de contracter, ce dernier peut obliger le prestataire de services et, dans le cas d'un consortium, les entreprises le composant ainsi que les entreprises parties à un sous-contrat rattaché directement ou indirectement à ce contrat, à obtenir une autorisation de contracter de l'Autorité des marchés publics dans les délais et selon les modalités particulières qu'il a déterminés.

8. PROTECTION DES RENSEIGNEMENTS PERSONNELS

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

Le prestataire de services s'engage envers le ministre à respecter chacune des dispositions applicables aux renseignements personnels 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. Ainsi, le prestataire de services doit :

1) Informer son personnel des règles prévues à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (Loi sur l'accès) (RLRQ, chapitre A-2.1) et notamment, mais non limitativement, de celles prévues aux articles 53 à 60.1, 62, 64 à 67.2, 83, 89 et 158 à 164 ainsi que 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) Faire signer aux membres de son personnel, préalablement à l'accès à des renseignements personnels, des engagements au respect de la confidentialité de ces renseignements selon l'annexe 1 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, sans le consentement de la personne concernée, à qui que ce soit, 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, notamment celles prévues aux politiques, directives et autres règles de sécurité applicables à l'information gouvernementale et identifiées par le ministre ou l'organisme public, à toutes les étapes de la réalisation du contrat et, le cas échéant, les mesures identifiées à l'annexe 1 – Engagement de confidentialité, jointe au présent document.

9) Le prestataire de services doit, 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, quel que 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

   □ 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 jointe à l'annexe 2 ainsi qu'aux directives que lui remet le ministre et transmet à celui-ci, dans les 60 jours suivant la fin du contrat, l'Attestation de destruction des renseignements personnels jointe à l'annexe 3, signée par une personne autorisée qu'il a désignée à cette fin.

   OU

   □ Confier la destruction des renseignements personnels et confidentiels à une entreprise spécialisée dans la récupération de ce type de renseignements, 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 jointe à l'annexe 2, ainsi qu'aux directives que lui remet le ministre. Le prestataire de services doit alors, dans les 60 jours suivant la fin du contrat de récupération, remettre au ministre l'Attestation de destruction des renseignements personnels jointe à l'annexe 3, signée par le responsable autorisé de cette entreprise.

10) Informer, dans les plus brefs délais, le ministre de toute violation ou tentative de violation par toute personne des obligations prévues aux présentes dispositions ou de tout événement pouvant risquer de porter atteinte à la sécurité ou à la confidentialité des renseignements personnels.

11) Fournir, à la demande du ministre, toute l'information pertinente au sujet de la protection des renseignements personnels et lui 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 par le prestataire de services au sous-contractant ou la cueillette de renseignements personnels par le sous-contractant :

   - soumettre à l'approbation du ministre la liste des renseignements personnels 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, quel qu'en soit le support, et à remettre au prestataire de services, dans les 60 jours suivant la fin de ce contrat, un tel document.

15) Transmettre de façon sécuritaire les renseignements personnels 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 sont acheminés par télécopieur, l'émetteur du document doit s'assurer que le récepteur est habilité à le recevoir et qu'il prend 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 ».

La fin du contrat ne dégage aucunement le prestataire de services et le sous-contractant de leurs obligations et engagement 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 : http://www.legisquebec.gouv.qc.ca/fr.

9. RÈGLES DE SÉCURITÉ DESTINÉS AUX RESSOURCES DU PRESTATAIRES DE SERVICES

Le prestataire de services s'assure que les ressources qui sont affectées à l'exécution du contrat ont pris connaissance et ont signé le document « Règles de sécurité du MCN », annexe 5 du présent contrat. L'annexe signée est remise au représentant désigné du ministre avant l'affectation de la ressource au contrat.

10. DÉCLARATION CONCERNANT LES ACTIVITÉS DE LOBBYISME EXERCÉES AUPRÈS DE L'ORGANISME PUBLIC RELATIVEMENT À L'ATTRIBUTION DU CONTRAT DE GRÉ À GRÉ

À la signature du contrat, le prestataire de services doit produire le formulaire dûment signé « Déclaration concernant les activités de lobbyisme exercées auprès de l'organisme public relativement à l'attribution d'un contrat de gré à gré » (annexe 4).

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

11. SOUS-CONTRAT

Un sous-contrat n'est pas permis dans le cadre de l'exécution de ce contrat.

12. RESPONSABILITÉ DU MINISTRE

Sauf en cas de faute intentionnelle ou de faute lourde de la part du ministre, ce dernier n'assume aucune responsabilité à l'égard de tout dommage matériel subi par le prestataire de services, ses employés, agents, représentants ou sous-contractants.

13. RESPONSABILITÉ DU PRESTATAIRE DE SERVICES

Le prestataire de services est responsable de tout dommage causé 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 prestataire de services s'engage à indemniser, protéger et prendre fait et cause pour le ministre contre tous recours, réclamations, demandes, poursuites et autres procédures pris par toute personne en raison de dommages ainsi causés.

14. RÉSILIATION

14.1 Résiliation avec motif

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

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

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

3) le prestataire de services lui a présenté des renseignements faux ou trompeurs ou lui a fait de fausses représentations;

4) le prestataire de services est déclaré coupable d'une infraction à la Loi fédérale sur la concurrence 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 prestataire de services énonçant le motif de résiliation. S'il s'agit d'un motif de résiliation prévu au paragraphe 1), le prestataire de services doit remédier au défaut énoncé dans le délai prescrit à cet avis, à défaut de quoi ce contrat est 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 2), 3) ou 4), la résiliation prend effet de plein droit à compter de la date de la réception de l'avis par le prestataire de services.

Le prestataire de services a 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, et ce, à la condition qu'il remette au ministre tous les travaux déjà effectués au moment de la résiliation. Si le prestataire de services avait obtenu une avance monétaire, il doit la restituer dans son entier.

Le prestataire de services est 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 prestataire de services doit notamment assumer toute augmentation du coût du contrat pour le ministre.

14.2 Résiliation sans motif

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 prestataire de services. La résiliation prend effet de plein droit à la date de la réception de cet avis par le prestataire de services.

Le prestataire de services a 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.

15. PROPRIÉTÉ MATÉRIELLE ET DROITS D'AUTEUR

15.1 Propriété matérielle

Les travaux réalisés par le prestataire de services en vertu du contrat, y compris tous les accessoires, qui sont remis au ministre, deviennent sa propriété entière et exclusive et il peut en disposer à son gré.

15.2 Droits d'auteur

1) Licence des droits d'auteur sur les travaux réalisés par le prestataire de services en faveur du ministre

Le prestataire de services accorde au ministre une licence exclusive, transférable, permettant l'octroi de sous-licences et irrévocable, qui lui permet de reproduire, adapter, publier, communiquer au public par quelque moyen que ce soit, traduire, exécuter ou représenter en public tous les travaux réalisés par le prestataire de services en vertu du contrat, pour toute fin jugée utile par le ministre.

Cette licence est accordée avec limites territoriales et sans limites de temps.

Toute considération pour la licence de droits d'auteur consentie en vertu du contrat est incluse dans le montant du contrat.

2) Renonciation aux droits moraux

Le prestataire de services s'engage à obtenir de l'auteur des travaux réalisés, en faveur du ministre, une renonciation à son droit moral à l'intégrité de ceux-ci. Dans le cas où le prestataire de services est l'auteur des travaux réalisés, il renonce à son droit moral à l'intégrité de ceux-ci.

3) Garanties

Le prestataire de services garantit au ministre qu'il détient tous les droits lui permettant de réaliser le contrat et, notamment, d'accorder la licence de droits d'auteur prévue à prévue à l'article 15.2, point 1) *Licence de droits d'auteur sur les travaux réalisés par le prestataire de services en faveur du ministre* et il 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 prestataire de services s'engage à prendre fait et cause et à indemniser le ministre advenant tout recours, réclamation, demande, poursuite et toute autre procédure pris par toute personne relativement à l'objet de ces garanties.

16. CONFLITS D'INTÉRÊTS

Le prestataire de services doit éviter toute situation qui met 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 prestataire de services doit immédiatement en informer le ministre qui peut, à sa seule discrétion, émettre une directive indiquant au prestataire de services, comment remédier à ce conflit d'intérêts ou résilier le contrat.

17. 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.

Le ministre peut céder à tout organisme visé à l'article 2 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03), en tout ou en partie, sans l'autorisation du prestataire de services les droits et obligations contenus au présent contrat.

18. LIEN D'EMPLOI

Le prestataire de services est la seule partie patronale à l'égard de l'ensemble du personnel qu'il affecte à l'exécution du présent contrat visé et il doit en assumer tous les droits, obligations et responsabilités.

19. APPLICATION DE LA TVQ ET DE LA TPS

Les services requis et payés par le ministre avec les deniers publics pour son utilisation propre 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.

20. FORCE MAJEURE

Tout événement imprévisible, irrésistible et indépendant de la volonté des parties qui survient en cours de contrat et qui rend impossible l'exécution, en tout ou en partie, d'une obligation prévue au contrat.

Ne constitue pas un cas de force majeure, une situation qui rend plus difficile ou plus onéreuse l'exécution de l'obligation.

Application :

Lorsque le prestataire de services invoque une situation de force majeure, il doit sans délai en aviser le ministre. Il doit également, par écrit :

- indiquer la situation de force majeure invoquée ;
- expliquer en quoi la situation de force majeure rend impossible l'exécution de son obligation;
- indiquer les mesures qu'il propose dans le contexte de la situation de force majeure (par exemple : suspension de l'obligation, réduction de l'obligation, annulation de l'obligation, etc.).

Par la suite, le ministre peut, à sa seule discrétion, accepter la mesure proposée ou en proposer une autre. Il peut également résilier le contrat.

Lorsque le ministre invoque une situation de force majeure, il avise sans délai le prestataire de services des mesures qu'il a mises en place en raison de la situation de force majeure.

La partie ayant invoqué la situation de force majeure doit aviser par écrit l'autre partie dès la cessation de l'événement constitutif de la force majeure.

21. CONFLITS DE TRAVAIL

Le prestataire de services n'est pas tenu responsable des délais ou retards dans l'exécution du contrat occasionnés par une grève des employés du gouvernement du Québec ou d'un lock-out déclaré par ce dernier.

Toutefois, dans de tels cas, le ministre ne verse aucun montant au prestataire de services tant que dure ce délai ou retard, tout paiement étant conditionnel à l'accomplissement des obligations du prestataire de services.

22. MODIFICATION DU CONTRAT

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

23. RÈGLEMENT DES DIFFÉRENDS

Si un différend survient dans le cours de l'exécution du contrat ou sur son interprétation, les parties s'engagent, avant d'exercer tout recours, à rechercher une solution amiable à ce différend et, si besoin est, à faire appel à un tiers, selon des modalités à convenir, pour les assister dans ce règlement.

24. COMMUNICATIONS

Tout avis exigé en vertu du présent contrat, pour être valide et lier les parties, doit être donné par écrit et être transmis par un moyen permettant de prouver la réception à un moment précis, aux coordonnées suivantes :

Ministère de la Cybersécurité et du numérique:

Francis Provencher

Directeur de la prévention, de la détection et de la gestion des incidents

Direction de la prévention, de la détection et de la gestion des incidents

880 chemin Ste-Foy, 10^{e} étage, Québec (Québec) G1S 2L2

418-643-6419

francis.provencher@mcn.gouv.qc.ca

Le prestataire de services :

Anderson Ortega

Directeur Développement commercial

Okiok DATA LTEE

655, Promenade du Centropolis, porte 230, Laval (Québec) H7T 0A3

450-681-1681

aortega@okiok.com

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

25. 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 à la date indiquée ci-dessous :

Pour le ministre,

[redacted] 2022-05-13

Dave Roussy — date
Directeur général du centre gouvernemental
de cyberdéfense

Pour OKIOK DATA LTÉE

[redacted]

Michel De Marinis — date
Vice-président ventes et marketing

ANNEXE 1
ENGAGEMENT DE CONFIDENTIALITÉ

TITTRE DU CONTRAT : RÉALISATION DE TESTS D'INTRUSION

NUMÉRO : ~~94600717~~ 96400717

Je, soussigné(e), _____ ,
(Nom de la personne)

exerçant mes fonctions au sein de _____,
(Nom du prestataire de services)

déclare formellement ce qui suit :

1. Choisir une des deux (2) options suivantes : (cochez la case appropriée)

   □ 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 précité, intervenu entre le ministre et mon employeur en date du _____.

   □ Je suis un(e) sous-contractant(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 précité, intervenu entre le ministre et cette entreprise en date du _____.

2. Je m'engage, sans limite de temps, à garder le secret le plus entier, à ne pas communiquer ni 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(e) à le faire par le ministre de la Cybersécurité et du Numérique ou par l'un de ses représentants autorisés.

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 entre mon employeur et le ministre.

4. J'ai été informé(e) que le défaut par le (la) soussigné(e) de respecter la totalité ou une partie du présent engagement de confidentialité m'expose ou expose mon employeur à des recours légaux, des réclamations, des poursuites ou toutes autres procédures en raison du préjudice causé envers quiconque est concerné par le contrat précité.

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

ET J'AI SIGNÉ À _____

CE _____ JOUR DU MOIS DE _____ DE L'AN _____

_____
(signature du déclarant ou de la déclarante)

Commission d'accès à l'information du Québec

ANNEXE 2
FICHE D'INFORMATION SUR LA DESTRUCTION
DES DOCUMENTS CONCERNANT 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 clé 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 3
ATTESTATION DE DESTRUCTION DES RENSEIGNEMENTS PERSONNELS

TITTRE DU CONTRAT : RÉALISATION DE TESTS D'INTRUSION

NUMÉRO : ~~94600717~~ 96400717

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) pour certifier que les renseignements personnels communiqués par le ministre de la Cybersécurité et du Numérique ou toute autre personne dans le cadre du projet octroyé à _____
(Nom du prestataire de services)

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

(cochez la case appropriée.)

☐	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 8 du présent contrat,

au moment de sa signature.

ANNEXE 4
DÉCLARATION CONCERNANT LES ACTIVITÉS DE LOBBYISME EXERCÉES AUPRÈS DE L'ORGANISME PUBLIC RELATIVEMENT À L'ATTRIBUTION DU CONTRAT DE GRÉ À GRÉ

TITTRE DU CONTRAT : RÉALISATION DE TESTS D'INTRUSION

NUMÉRO : ~~94600717~~ 96400717

JE, SOUSSIGNÉ (E), _____,
(NOM ET TITRE DE LA PERSONNE AUTORISÉE PAR LE PRESTATAIRE DE SERVICES)

ATTESTE QUE LES DÉCLARATIONS CI-APRÈS SONT VRAIES ET COMPLÈTES À TOUS LES ÉGARDS

AU NOM DE : _____,
(NOM DU PRESTATAIRE DE SERVICES)

(CI-APRÈS APPELÉ « PRESTATAIRE DE SERVICES »)

JE DÉCLARE CE QUI SUIT :

1. J'AI LU ET JE COMPRENDS LE CONTENU DE LA PRÉSENTE DÉCLARATION ;
2. JE SUIS AUTORISÉ(E) PAR LE PRESTATAIRE DE SERVICES À SIGNER LA PRÉSENTE DÉCLARATION ;
3. LE PRESTATAIRE DE SERVICES DÉCLARE (COCHER L'UNE OU L'AUTRE DES DÉCLARATIONS SUIVANTES) :

   ☐ QUE PERSONNE N'A EXERCÉ POUR SON COMPTE, QUE CE SOIT À TITRE DE LOBBYISTE D'ENTREPRISE OU DE LOBBYISTE-CONSEIL, DES ACTIVITÉS DE LOBBYISME, 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*, PRÉALABLEMENT À CETTE DÉCLARATION RELATIVEMENT À LA PRÉSENTE ATTRIBUTION DU CONTRAT ;

   ☐ QUE DES ACTIVITÉS DE LOBBYISME, AU SENS DE LA LOI SUR LA TRANSPARENCE ET L'ÉTHIQUE EN MATIÈRE DE LOBBYISME ET DES AVIS ÉMIS PAR LE COMMISSAIRE AU 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*, PRÉALABLEMENT À CETTE DÉCLARATION RELATIVEMENT AU PRÉSENT CONTRAT (RLRQ, CHAPITRE T-11.011, R.2).

4. JE RECONNAIS QUE, SI LE MINISTRE 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 LE MINISTRE DE LA CYBERSÉCURITÉ ET DU NUMÉRIQUE.

ET J'AI SIGNÉ, _____ _____
(SIGNATURE) (DATE)

* LA LOI, LE CODE ET LES AVIS ÉMIS PAR LE COMMISSAIRE AU LOBBYISME SONT DISPONIBLES À CETTE ADRESSE : HTTPS://WWW.COMMISSAIRELOBBY.QC.CA/LOI-ET-REGLEMENTS/

ANNEXE 5
RÈGLES DE SÉCURITÉ DU MCN

TITTRE DU CONTRAT : RÉALISATION DE TESTS D'INTRUSION
NUMÉRO : ~~94600717~~ 96400717

Service ou actif	Règles de sécurité
1. *Contrôle d'accès aux édifices et aux locaux*	- porter votre carte d'accès sur vous, en tout temps, dans les locaux du MCN ; - présenter votre carte d'accès à la demande de l'équipe responsable de la sécurité physique, des agents de sécurité ou tout autre membre du MCN; - conserver votre carte en lieu sûr; - avertir immédiatement votre représentant désigné du MCN en cas de perte de votre carte d'accès ; - ne pas faire entrer ou sortir une personne grâce à votre carte d'accès lors de vos déplacements dans les locaux du MCN.
2. *Accès logiques*	- aviser votre représentant désigné au contrat lorsque certains de vos droits d'accès ne sont plus nécessaires dans la poursuite de vos activités ; - utiliser vos privilèges d'accès aux seules fins pour lesquelles ils ont été accordés dans le cadre de vos activités.
3. *Identification*	- S'identifier en tout temps sur les lieux de travail et dans le cadre de vos activités au MCN.
4. *Authentification*	- garder confidentiel votre mot de passe ; - choisir un mot de passe robuste suivant minimalement les règles établies par le MCN ; - ne pas cocher la case de mémorisation du mot de passe apparaissant dans certains logiciels et ne pas écrire votre mot de passe pour le retenir sans mesures de protection (des trucs de composition d'un bon mot de passe, facile à retenir, sont disponibles dans l'Intranet du MCN).
5. *Poste de travail*	- ne jamais permettre à quiconque d'utiliser votre session de travail permettant l'accès aux infrastructures du MCN ; - utiliser une version actuelle d'un antivirus avec un fichier de signatures mis à jour dès sa publication sur Internet, utiliser un pare-feu et un anti-espiogiciel ; - toujours verrouiller ou fermer votre session de travail lorsque vous vous éloignez de votre poste de travail ; - protéger en tout temps l'écran des regards indiscrets lorsque vous manipulez des informations organisationnelles appartenant au MCN ; - signaler, sans délai, à votre représentant désigné au contrat la perte ou le vol de votre ordinateur notamment si ce dernier contient des informations organisationnelles appartenant au MCN ; - prendre les dispositions nécessaires pour préserver la sécurité de l'infrastructure du MCN.
6. *Réseau local*	- ne pas communiquer ou permettre que soient communiqués à quiconque des renseignements facilitants ou permettant l'accès non autorisé au réseau ; - ne pas contourner les services de sécurité (ex. pare-feu, canal VPN) ; - ne pas utiliser les infrastructures du MCN pour son usage personnel ; - ne pas installer de réseaux ou bornes sans fil (notamment WIFI, WIMAX, cellulaires ou autres) dans l'infrastructure du MCN ; - aviser votre représentant désigné au contrat, en cas de doute quant à la sécurité dans l'utilisation de l'infrastructure du MCN.
7. *Internet*	- ne pas essayer de contourner les règles de filtrage de navigation Internet ; - ne pas partager, télécharger ou copier des logiciels, des fichiers exécutables, des scripts, des jeux ou tout autre fichier susceptible de nuire au fonctionnement ou à la sécurité des infrastructures du MCN ; - ne pas diffuser sur Internet une adresse électronique du MCN ; - ne pas accepter d'offres spontanées en provenance d'Internet lorsque vous êtes branchés sur l'infrastructure du MCN.

Service ou actif	Règles de sécurité
8. *Courriel*	- ne pas utiliser la boîte courriel fournie par le MCN à des fins personnelles ou à des mandats autres que ceux du MCN ; - respecter le modèle de signature normalisée mis en place au MCN ; - utiliser seulement l'adresse de courriel appartenant au MCN lors des communications effectuées en son nom ; - ne jamais utiliser votre adresse de courriel personnelle ou celle d'un prestataire de services pour échanger des informations organisationnelles du MCN ; - ne jamais ouvrir et faire suivre les courriels et les pièces jointes acheminés par un expéditeur inconnu et qui ne s'inscrivent pas dans un contexte connu et strictement professionnel.
9. *Sauvegarde et destruction des informations*	- s'assurer de laisser à la fin de son mandat, une copie des informations organisationnelles ainsi que la boîte courriel du MCN sur un répertoire partagé identifié par votre représentant désigné du MCN ; - détruire les documents organisationnels par déchiquetage ou les déposer dans les bacs sécurisés à la fin de votre mandat ; - ne pas conserver d'informations organisationnelles sur l'infrastructure ou sur un service Web autre que ceux appartenant au MCN.
10. *Impression*	- utiliser le service d'impression sécurisé par défaut ; - récupérer immédiatement les documents confidentiels du MCN imprimés.
11. *Télécopie*	- Ne pas télécopier de l'information confidentielle du MCN.
12. *Accès à distance*	- utiliser les logiciels autorisés par le MCN pour accéder à distance à son infrastructure, si nécessaire à la réalisation de votre mandat ; - s'assurer que le travail à distance s'effectue dans un contexte permettant de préserver la confidentialité de l'information apparaissant à l'écran, ainsi que de la saisie du mot de passe ; - fermer votre session de travail à distance, lorsque la connexion n'est plus utilisée.
13. *Support amovible*	- utiliser un support amovible pourvu de mécanismes de chiffrement respectant les règles établies par le MCN ; - signaler sans délai la perte ou le vol de support amovible renfermant des informations organisationnelles du MCN ; - remettre au représentant désigné du MCN tout support amovible trouvé et ne pas tenter de le brancher ou essayer d'en lire le contenu.

Règles spécifiques de sécurité

Dans le cadre de certaines tâches spécifiques ou très spécialisées, le MCN peut fournir exceptionnellement, un poste de travail (ordinateur de table, portable ou virtuel) ou un appareil mobile au personnel des prestataires de services. À cet égard, les règles de sécurité suivantes doivent être respectées afin de ne pas contourner ou altérer les mécanismes de sécurité mis en place au MCN :

- respecter la configuration technologique du poste de travail et/ou de l'appareil mobile ;
- ne pas laisser une personne non autorisée utiliser le poste de travail et/ou l'appareil mobile ;
- brancher obligatoirement votre ordinateur portable au réseau au moins une fois par semaine, afin que les mises à jour et les correctifs des systèmes d'exploitation et logiciels fournis par le MCN soient appliqués ;
- s'assurer que les informations organisationnelles appartenant au MCN sur le poste de travail et/ou de l'appareil mobile sont aussi enregistrées sur son infrastructure ;
- retirer de votre poste de travail, le cas échéant, les logiciels fournis par le MCN à la fin du mandat ;
- ne pas transmettre de texto comportant des informations organisationnelles du MCN ;
- rendre le service Bluetooth non visible à la suite d'un appariement et retirer immédiatement le nom d'un périphérique remplacé, perdu, volé ou qui ne sera plus utilisé de la liste des appareils reconnus ;
- signaler immédiatement la perte d'un poste de travail et/ou d'un appareil mobile à votre représentant désigné du MCN et au Centre de services à la clientèle (CSC) ;
- le MCN se réserve le droit de réinitialiser à distance un appareil mobile, supprimant de ce fait toutes données s'y trouvant.

Engagement du respect des règles de sécurité du MCN

Je, soussigné(e), _____, exerçant mes fonctions au sein de
(Nom de la personne)

_____,
(Nom du prestataire de services)

déclare formellement avoir pris connaissance des règles de sécurité en vigueur au MCN et de s'y conformer :

ET J'AI SIGNÉ À _____

CE _____ JOUR DU MOIS DE _____ DE L'AN _____

_____
(Signature du déclarant ou de la déclarante)

Remettre au représentant désigné du MCN

ANNEXE 6 – DESCRIPTION DES BESOINS

TITTRE DU CONTRAT : RÉALISATION DE TESTS D'INTRUSION

NUMÉRO : ~~94600717~~ 96400717

Le prestataire de services s'engage envers le ministère de la Cybersécurité Numérique (MCN) à fournir les services suivants :

- **Réalisation de tests d'intrusion par des professionnels certifiés OSCP, sur des actifs informationnels exposés sur Internet, incluant mais sans s'y limiter, des sites internet, application et services numériques.**
- **Rédaction de rapports techniques incluant des preuves de concept et des mesures de mitigations.**
- **Le présent contrat est à exécution sur demande, le prestataire de service s'engage à fournir les services demandés dans un délai maximal de 10 jours ouvrables suivant la notification par demande d'exécution (DE) du représentant du ministre.**