



POLITIQUE DU CONSEIL DE LA NATION HURONNE-WENDAT RELATIVE À LA SÉCURITÉ DE L'INFORMATION

Mars 2025



Nom de la politique administrative : Politique du Conseil de la Nation huronne-wendat relative à la sécurité de l'information	Numéro de la politique : POL-RH-09	
Date d'entrée en vigueur : 31 mars 2025	Date de révision : Mars 2025	Numéro résolution : Réso. # 7593
Annexe(s) de la politique :		
Responsable : Direction des Ressources humaines		



TABLE DES MATIÈRES

DISPOSITIONS GÉNÉRALES	4
Définitions	4
PRÉAMBULE	6
1. OBJECTIFS	7
2. PRINCIPES GÉNÉRAUX	7
3. CADRE LÉGISLATIF	8
4. PORTÉE	8
5. ENGAGEMENT ET RESPONSABILITÉS DU CONSEIL	8
6. ENGAGEMENT ET RESPONSABILITÉS DE L'USAGER	9
I. INFORMATION ET ACTIFS INFORMATIONNELS	9
II. RESPECT DES MESURES DE SÉCURITÉ	10
7. GESTIONNAIRE DE LA POLITIQUE	11
8. VÉRIFICATION DE SÉCURITÉ INFORMATIQUE	11
9. PROCESSUS ADMINISTRATIF OU DISCIPLINAIRE	12
10. RÉVISION DE LA POLITIQUE	12
11. MISE EN ŒUVRE ET ACCEPTATION	12
12. ENTRÉE EN VIGUEUR	12
13. ACCUSÉ DE RÉCEPTION	13



DISPOSITIONS GÉNÉRALES

Définitions

À moins que le contraire ne soit expressément prévu ou que le contexte n'exige le contraire, les définitions qui suivent s'appliquent à la présente Politique.

Actif informationnel

Signifie une information, une banque d'information, un système ou un support d'information, un document, une technologie de l'information, une installation ou un ensemble de ces éléments acquis ou constitué par le Conseil habituellement accessible ou utilisable avec un Système d'information. Cela inclut l'Information ainsi que les supports tangibles ou intangibles permettant son traitement, sa transmission ou sa conservation aux fins de l'utilisation prévue (ordinateurs fixes ou portables, tablettes électroniques, téléphones intelligents, etc.), dont un support tangible, de même que l'information fixée sur un support analogique, dont le papier.

Conseil de la Nation huronne-wendat ou CNHW

Instance dirigeante du Gouvernement de la Nation huronne-wendat dont les membres sont élu·e·s selon le *Code de représentation de la Nation huronne-wendat*.

Équipement

Signifie un équipement matériel tel que, mais non limitativement, un ordinateur fixe ou portable, une tablette électronique, un cellulaire, qu'il soit la propriété du Conseil, loué ou contrôlé par le Conseil et permettant le traitement, la transmission ou la conservation aux fins de l'utilisation prévue de l'Information. Cette notion comprend également les Systèmes d'information qui sont l'ensemble organisé de moyens mis en place pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'Information en vue de répondre à un besoin déterminé, y incluant notamment les applications, progiciels, logiciels, technologies de l'information et les procédés utilisés pour accomplir ces fonctions.

Équipement personnel de l'Usager

Signifie un équipement (ordinateurs fixes ou portables, tablettes électroniques, téléphones intelligents, etc.) appartenant à l'Usager ou loué ou contrôlé par l'Usager et permettant le traitement, la transmission ou la conservation aux fins de l'utilisation prévue de l'Information.

Mars 2025

Incident

Signifie un événement qui porte atteinte ou qui est susceptible de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'Information, ou plus généralement aux Mesures de sécurité ou aux Systèmes d'information, notamment une interruption des services ou une réduction de leur qualité.

Information

Signifie un renseignement consigné sur un support quelconque pour être conservé, traité ou communiqué comme élément de connaissance.

Mesures de sécurité

Signifie les concepts, techniques, mesures techniques et mesures administratives servant à empêcher l'acquisition, l'altération, la divulgation, la manipulation, la modification ou la perte, délibérée ou accidentelle et non autorisée, des Actifs informationnels.

Politique

Signifie la *Politique du Conseil de la Nation huronne-wendat relative à la sécurité de l'information*.

Secteur des TI

Signifie le service offert par la Direction adjointe des technologies de l'information qui est responsable des contrôles relatifs aux technologies de l'information.

Système d'information

Signifie l'ensemble organisé de moyens mis en place pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'Information en vue de répondre à un besoin déterminé, y incluant notamment les applications, progiciels, logiciels, technologies de l'information et les procédés utilisés pour accomplir ces fonctions.

Usagers

Signifie tou-te-s les employé-e-s et élu-e-s du Conseil, ainsi que les utilisateur-ric-e-s et entreprises externes qui, dans le cadre de leur travail ou de leur prestation de services, utilisent de l'Équipement ou traitent de l'Information appartenant au Conseil.

PRÉAMBULE

Le Conseil de la Nation huronne-wendat (le « **Conseil** ») s'engage à assurer la sécurité des Informations qu'il détient en mettant en place des Mesures de sécurité de l'Information raisonnables et appropriées aux circonstances et à protéger les renseignements personnels et confidentiels de ses Usagers.

Le Conseil s'engage à protéger tous ses Actifs informationnels par des Mesures de sécurité raisonnables et appropriées au degré de sensibilité de l'Information.

La présente Politique s'applique conjointement avec la *Politique du Conseil de la Nation huronne-wendat relative à l'utilisation de l'Équipement, de l'Internet et des médias sociaux*.

1. OBJECTIFS

Les objectifs de la présente Politique sont les suivants :

- a) Assurer un encadrement du système de gestion et des Mesures de sécurité de l'Information;
- b) Établir des lignes directrices afin d'atténuer les risques tout en maintenant l'efficacité opérationnelle du Conseil;
- c) Protéger l'Information, les Actifs informationnels et les Systèmes d'information de manière raisonnable et appropriée aux circonstances et au degré de sensibilité de l'Information afin de réduire les risques et minimiser les effets d'Incidents potentiels;
- d) Reconnaître la nature réseautique de l'environnement informatique actuel et assurer une gestion et une surveillance raisonnables et efficaces des risques pouvant mettre en péril la sécurité de l'Information;
- e) Fournir à l'Usager des lignes directrices et un outil de référence en matière de Mesures de sécurité de l'Information;
- f) Établir les responsabilités de l'Usager relativement aux Mesures de Sécurité, à l'utilisation des Actifs informationnels, des Systèmes d'information et des Équipements personnels ou non de l'Usager;
- g) Assurer de façon raisonnable et appropriée aux circonstances et au degré de sensibilité, la protection, la confidentialité, l'intégrité et la disponibilité des Actifs informationnels;
- h) Préserver la réputation et l'image du Conseil et de ses client·e·s;
- i) Prévenir l'utilisation illégale, inappropriée ou non autorisée de l'Information et des Actifs informationnels.

2. PRINCIPES GÉNÉRAUX

- a) Le Conseil prend les mesures raisonnables et appropriées aux circonstances et au degré de sensibilité de l'Information afin d'assurer la confidentialité, l'intégrité et la disponibilité de l'Information et des Actifs informationnels, quelle que soit la façon dont l'Information est créée, distribuée, traitée ou sauvegardée;
- b) L'Information concernant les Actifs informationnels est confidentielle. Nul ne doit utiliser ou divulguer l'Information à d'autres fins que dans l'exercice de ses fonctions ou sans avoir obtenu préalablement le consentement écrit de la personne concernée ou de la personne responsable;

Mars 2025

- c) Les Actifs informationnels sont mis à la disposition de l'Usager uniquement dans le but de l'accomplissement de ses fonctions et obligations pour et au nom du Conseil, ainsi que pour la bonne conduite des opérations de ce dernier;
- d) L'Usager bénéficie d'une expectative de vie privée moindre à l'égard de l'Information qu'il crée, envoie, reçoit ou sauvegarde en utilisant les Actifs informationnels, les Systèmes d'information et les Équipements. Le CNHW peut surveiller et accéder aux Actifs informationnels lorsqu'il a un motif sérieux de le faire, notamment à toutes fins compatibles avec les fonctions et/ou la mission du Conseil, le tout sans préavis.

3. CADRE LÉGISLATIF

- *Charte canadienne des droits et libertés;*
- *Code civil du Québec;*
- *Code canadien du travail;*
- *Loi canadienne sur les droits de la personne;*
- *Loi sur la protection des renseignements personnels et les documents électroniques;*
- *Conventions collectives applicables.*

4. PORTÉE

La présente Politique s'applique à tous les Usagers et définit leur responsabilité, eu égard aux circonstances et au degré de sensibilité de l'Information, pour assurer la protection et l'utilisation raisonnable et appropriée des Actifs informationnels.

5. ENGAGEMENT ET RESPONSABILITÉS DU CONSEIL

- a) Le Conseil s'engage à maintenir des Actifs informationnels fonctionnels qui répondent aux exigences légales et réglementaires, le cas échéant, et à ses besoins opérationnels;
- b) Le Conseil s'engage à prendre les mesures et à fournir les protections physiques et électroniques raisonnables et appropriées aux circonstances et au degré de sensibilité de l'Information pour assurer la protection de l'Information et des Actifs informationnels, tant dans ses installations physiques que son environnement informatique, et pour prévenir l'accès non autorisé;
- c) Le Conseil s'engage à conclure toutes les conventions de licence applicables aux Actifs informationnels qui seront utilisés dans le cadre de ses opérations;

Mars 2025

- d) Le Conseil s'engage à prendre les mesures raisonnables et appropriées pour assurer une utilisation efficace de ses Actifs informationnels par les Usagers;
- e) Le Conseil s'engage à mettre en place des mesures adéquates et raisonnables de signalement, de détection, d'identification, de réponse et d'avis aux personnes concernées. Le CNHW réalise un examen périodique des Équipements et Systèmes d'information, afin de surveiller l'intégrité des systèmes informatiques;
- f) Le Conseil s'engage à tester toute nouvelle structure de données existantes avant d'être mis en œuvre et de tenir un processus de gestion des changements;
- g) Dans la mesure où l'accès aux Informations ou aux Actifs informationnels devait être nécessaire à un mandataire, un fournisseur, un sous-traitant ou un consultant du Conseil, dans l'exercice de ses fonctions ou à l'exécution de son mandat ou de son contrat, ce dernier obtiendra préalablement à tout accès de sa part un engagement écrit (i) à prendre les mesures nécessaires pour en assurer la confidentialité et l'intégrité au sens de la présente politique et des lois applicables et (ii) à ne conserver aucune Information au-delà de la durée nécessaire pour son mandat ou son contrat;
- h) Le Conseil s'engage à établir, mettre en œuvre et maintenir des plans raisonnables et appropriés pour la continuité des opérations afin d'assurer la disponibilité de l'Information et des Actifs informationnels lors de la survenance d'un événement restreignant la poursuite de ses activités usuelles;
- i) Le Conseil s'engage à diffuser et mettre la présente Politique à la disposition de tous les Usagers et s'engage à faire respecter la présente Politique.

6. ENGAGEMENT ET RESPONSABILITÉS DE L'USAGER

- a) L'Usager s'engage à prendre connaissance et à respecter la présente Politique;
- b) L'Usager s'engage à suivre toute formation qui lui serait exigée par l'employeur, notamment en cybersécurité, et comprend que tout refus de suivre la formation peut entraîner le retrait d'utilisation des Actifs informationnels, de l'Équipement et/ou des Systèmes d'information.

I. INFORMATION ET ACTIFS INFORMATIONNELS

- a) L'Information et les Actifs informationnels seront utilisés par l'Usager uniquement dans le cadre de l'exécution de ses fonctions pour le compte du Conseil;
- b) L'Usager doit accéder à l'Information et aux Actifs informationnels uniquement dans le cadre des opérations du Conseil et par l'entremise des Équipements et Systèmes d'information fournis et approuvés par le Conseil, et ce, dans la mesure permise par ce dernier;

- c) L'Usager ne doit pas conserver, copier, communiquer ou divulguer l'Information confidentielle, sauf dans la mesure permise dans le cadre de ses fonctions, sans le consentement écrit préalable de la personne concernée ou de la personne responsable;
- d) L'Usager peut utiliser les outils d'intelligence artificielle seulement si le Secteur des TI l'autorise et selon ses directives. Dans ce cas, l'Usager qui est autorisé à utiliser une intelligence artificielle dans le cadre de ses fonctions doit s'assurer de la protection de la confidentialité des Informations et ne doit en aucun cas divulguer de l'Information confidentielle;
- e) Les Actifs informationnels sont la propriété exclusive du Conseil et l'Usager ne doit pas les copier ou les utiliser de manière non conforme ou illégale.

II. RESPECT DES MESURES DE SÉCURITÉ

- a) L'Usager ne doit pas tenter d'accéder ou de sauvegarder de l'Information sur des systèmes autres que les Systèmes d'information fournis par le Conseil, autrement que conformément aux politiques, directives, normes ou procédures en vigueur ou sans l'approbation écrite préalable du Secteur des TI;
- b) L'Usager doit respecter les limitations aux accès qui lui sont accordés en fonction de son emploi ou de son mandat et ne pas tenter d'accéder à de l'Information qui ne le concerne pas ou qui ne le concerne plus en cas de changement d'emploi, au sein du Conseil ou non;
- c) L'Usager ne doit pas utiliser par le biais des Équipements ou des Actifs informationnels des services infonuagiques commerciaux autres que les services fournis ou approuvés par le Conseil, à moins d'avoir obtenu au préalable l'approbation écrite du Secteur des TI;
- d) L'Usager qui utilise de quelque façon une intelligence artificielle dans le cadre de ses fonctions, conformément à l'article 8 l d) de la présente, doit s'assurer en tout temps de la protection des Actifs informationnels;
- e) Tous les Actifs informationnels fournis à l'Usager doivent être protégés par un mot de passe conforme aux exigences du Conseil, si applicable, et l'Usager doit prendre toutes les mesures nécessaires afin de prévenir la divulgation non autorisée de tel mot de passe. L'Usager doit notamment changer son mot de passe de façon régulière selon les directives établies par le Secteur des TI;
- f) Les Actifs informationnels et les Équipements personnels de l'Usager laissés sans surveillance doivent être sécurisés physiquement et être inaccessibles aux usagers non autorisés.

Mars 2025

- g) Tout accès à distance aux Systèmes d'information doit être effectué en utilisant une méthode d'accès à distance approuvée par le Conseil;
- h) L'Usager s'engage à n'apporter aucune modification aux Systèmes d'information ou aux Équipements, y compris, mais sans s'y limiter, l'installation, la modification ou la suppression de logiciels, sans avoir obtenu au préalable le consentement écrit du Secteur des TI;
- i) L'Usager ne doit pas tenter de contourner les mesures de sécurité configurées sur l'Équipement;
- j) L'Usager doit évaluer le degré de prudence requis pour toute communication d'Information dans l'exercice de ses fonctions et établir si celle-ci doit être soumise à des mesures de sécurité spécifiques et supplémentaires, telles que le cryptage;
- k) L'Usager s'engage à signaler immédiatement toute violation de cette politique au Gestionnaire de la politique ainsi que tout défaut d'un Système d'information, d'un Équipement ou d'un Équipement personnel de l'Usager qui pourraient compromettre la sécurité, la confidentialité et l'intégrité de l'Information.

7. GESTIONNAIRE DE LA POLITIQUE

Le directeur ou la directrice des Ressources humaines est responsable de l'application de la présente Politique (le « **Gestionnaire de la Politique** »), en collaboration avec le Secteur des TI. Il-elle lui incombe également de veiller, en collaboration avec la Direction générale, à ce que cette Politique continue de répondre aux lois applicables, ainsi qu'aux besoins opérationnels du Conseil.

8. VÉRIFICATION DE SÉCURITÉ INFORMATIQUE

- a) Les Systèmes d'information génèrent habituellement des enregistrements de leur utilisation. Les informations contenues dans ces enregistrements peuvent être analysées à des fins de diagnostic. De plus, les activités faites sur les Équipements peuvent être analysées via la mise en place à distance d'un dispositif.
- b) Seul le Gestionnaire de la politique et le Secteur des TI, y compris les personnes qu'il détermine, peuvent prendre connaissance et surveiller ou utiliser les informations provenant des enregistrements pour identifier une activité non autorisée, inappropriée ou illégale.
- c) Le Gestionnaire de la politique et les personnes qu'il détermine peuvent procéder à des enquêtes ou vérifications spécifiques, s'il existe des motifs raisonnables de procéder à une telle enquête et/ou vérification.

9. PROCESSUS ADMINISTRATIF OU DISCIPLINAIRE

Toute violation de la présente Politique pourrait entraîner diverses mesures administratives ou disciplinaires pouvant aller jusqu'au congédiement.

Pour les utilisateur·rice·s et les entreprises externes, toute violation de la présente politique peut mener à l'annulation ou la suspension des droits d'accès et d'utilisation de l'Équipement, des Systèmes d'information et/ou des Actifs informationnels ou à la fin de la relation contractuelle.

Le Conseil pourra obtenir indemnisation de tous les dommages subis à la suite de l'utilisation ou la communication non autorisée, inappropriée ou illégale de l'Information et/ou des Actifs informationnels. Le Conseil pourra également obtenir le remboursement des frais et dommages engendrés par toute violation de la Politique.

10. RÉVISION DE LA POLITIQUE

Une révision de la présente politique doit être effectuée lorsque (i) l'exposition à un risque est détectée ou signalée; (ii) il y a un changement dans l'environnement corporatif, technologique, professionnel, législatif ou réglementaire du Conseil et que tel changement nécessite une révision de la présente politique; ou (iii) comme requis par le Gestionnaire de la politique.

Toute modification de cette Politique doit être approuvée par le Conseil.

11. MISE EN ŒUVRE ET ACCEPTATION

La présente Politique est applicable à tous les Actifs informationnels actuels et futurs.

Chaque Usager doit signer un formulaire confirmant avoir pris connaissance du contenu de la présente Politique et de toute modification postérieure ou directive du Conseil qui lui sera dénoncée. Une copie du formulaire signé sera conservée dans le dossier de l'Usager auprès des ressources humaines.

12. ENTRÉE EN VIGUEUR

La Politique entre en vigueur le 31 mars 2025 à la suite de l'adoption par le CNHW et remplace toute autre politique ou pratique antérieure.

13. ACCUSÉ DE RÉCEPTION

Toutes les personnes visées par la Politique doivent accuser réception de cette dernière et déclarer bien en saisir la portée.

Je (lettres moulées s.v.p.), _____, accuse réception de la présente *Politique du Conseil de la Nation huronne-wendat relative à la sécurité de l'information* en vigueur au Conseil de la Nation huronne-wendat. Je déclare, par la présente, avoir pris connaissance de son contenu. Je suis conscient·e que toute contravention à cette Politique peut entraîner des mesures administratives ou disciplinaires pouvant aller jusqu'au congédiement.

Signée à Wendake, ce _____^e du mois de _____ 20____.

Signature de l'employé·e