Pratique recommandée en sécurité de l'information

PR-054

# Guide d'utilisation sécuritaire des assistants numériques personnels

# Guide d’utilisation sécuritaire des assistants numériques personnels

Cette publication a été réalisée par
le Dirigeant principal de l'information et
produite par la Direction des communications
du Secrétariat du Conseil du trésor.

Vous pouvez obtenir de l'information au sujet
du Conseil du trésor et de son Secrétariat
en vous adressant à la Direction des communications
ou en consultant son site Web.

Direction des communications
Secrétariat du Conseil du trésor

2e étage, secteur 800
875, Grande Allée Est
Québec (Québec)  G1R 5R8

Téléphone : 418 643-1529
Sans frais : 1 866 552-5158

communication@sct.gouv.qc.ca

www.tresor.gouv.qc.ca

Dépôt légal – juin 2017
Bibliothèque et Archives nationales du Québec

ISBN : 978-2-550-78513-2 (en ligne)

# Remerciements

Le Secrétariat du Conseil du trésor remercie l'équipe de réalisation et le groupe de travail interministériel de leur participation au travail accompli.

## Équipe de réalisation

M. Socheat Sonn, chargé de projet

M. Mohamed Darabid, coordonnateur
Secrétariat du Conseil du trésor

## Groupe de travail interministériel

M. Jean Amiot
Sûreté du Québec

M. Mohamed Chérif Benabderrahmane
Régie du bâtiment du Québec

M. Mohamed Darabid
Secrétariat du Conseil du trésor

M. Philippe Dhers
TéléQuébec

Mme Sothida Pong
Ministère de l'Immigration, de la Diversité et de l'Inclusion

M. Socheat Sonn
Secrétariat du Conseil du trésor

# Notes à l'intention du lecteur

| | |
|---|---|
| Note 1 : | Pour ne pas alourdir le texte, le masculin est utilisé comme générique dans le présent document. |
| Note 2 : | Le terme « organisme public » désigne un ministère ou un organisme, qu'il soit budgétaire ou autre que budgétaire, ainsi que tout organisme du réseau de l'éducation, du réseau de l'enseignement supérieur et du réseau de la santé et des services sociaux.<br>[Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03)] |
| Note 3 : | Bien que les éléments du présent guide soient applicables à la plupart des organismes publics, il convient, pour ces derniers, de les adapter à leur organisation et aux risques qui leur sont propres. |
| Note 4 : | Certains termes, sigles ou acronymes sont définis dès leur première apparition dans le texte. Ces définitions sont également présentées à l'Annexe I. |

# Table des matières

# 1. Introduction

L'assistant numérique personnel (ANP) est un appareil mobile[1] de type terminal sans fil[2] comparable aux ordinateurs portatifs. Il peut recevoir, stocker, traiter et transmettre de l'information.

Les principales fonctionnalités de l'ANP sont notamment l'agenda électronique[3], le répertoire téléphonique et le bloc-notes. Les avancées technologiques ont permis de lui adjoindre des fonctionnalités multimédias supplémentaires telles que l'accès à Internet sans fil, l'accès au réseau de l'organisation, la géolocalisation[4], la messagerie électronique, les lecteurs de musique, de vidéos et de documents, la capture de son, d'images et de vidéos, le téléphone, etc. Les nombreux logiciels et outils disponibles qui peuvent être installés sur l'ANP pour augmenter la productivité en font également un outil de travail incontournable.

Ces avantages contribuent à l'accroissement de leur utilisation par les organismes publics (OP), mais les ANP peuvent également être la source d'incidents. En effet, leurs nombreuses fonctionnalités, souvent complexes, peuvent engendrer une multitude de disfonctionnements attribuables à une erreur d'utilisation ou à des actions malveillantes de cybercriminels (p. ex. interception de données, installation d'applications malveillantes, vol d'identité, etc.). Il apparaît donc nécessaire que les organismes publics encadrent l'utilisation des ANP, particulièrement au regard de la nature, souvent personnelle, confidentielle ou stratégique, de l'information qu'ils emmagasinent ou qu'ils traitent.

C'est dans le but d'offrir aux OP un cadre de référence pour une utilisation sécuritaire des ANP, principalement les téléphones intelligents, les tablettes numériques et les téléphones-tablettes, que le présent guide est mis à la disposition des OP.

## 1.1. Contexte

Le marché de l'ANP prend de l'ampleur d'année en année. En 2015, plus de la moitié des adultes (53,3 %) au Québec possédaient un téléphone intelligent comparativement à 68 % aux États-Unis[5] et près de 70 % en France[6]. En ce qui a trait aux tablettes numériques[7], près d'un adulte sur deux (46,4 %)

---

**1**. **Appareil mobile** : Appareil informatique que l'on peut transporter avec soi et qui possède l'énergie électrique nécessaire pour fonctionner de manière autonome. *[OQLF - Grand dictionnaire terminologique]*

**2**. **Terminal sans fil :** Appareil informatique ou de télécommunication qu'on peut transporter avec soi dans ses déplacements et utiliser comme terminal donnant accès sans fil à un ou à plusieurs réseaux. *[OQLF - Grand dictionnaire terminologique]*

**3**. **Agenda électronique :** Logiciel de gestion du temps qui facilite la planification horaire, quotidienne ou à plus long terme, de l'utilisateur. *[OQLF - Grand dictionnaire terminologique]*

**4**. **Géolocalisation :** Ensemble des techniques qui permettent, dans le contexte de l'utilisation d'appareils mobiles, comme les téléphones cellulaires, de déterminer leur position géographique à partir des ondes radio qu'ils émettent. *[OQLF - Grand dictionnaire terminologique]*

***5.*** Selon PEW RESEARCH CENTER, *Technology Device Ownership: 2015*, *octobre 2015, 26 p.*

***6.*** Selon DELOITTE, *Étude sur les usages mobiles 2015. A Game of Phones*, *novembre 2015, 30 p.*

***7***. Selon l'enquête NETendances du CEFRIO, *La mobilité au Québec : des appareils aux usages multiples*, *décembre 2015, 15 p.*

au Québec en possédait une, comparativement à 45 % aux États-Unis et 53 % en France. Ces chiffres sont appelés à croître dans les années futures.

Cette tendance prononcée vers l'adoption des appareils mobiles dans le quotidien est principalement attribuable à l'évolution démographique alors que les nouvelles générations sont constamment connectées à Internet. La même tendance tournée vers la mobilité se remarque également au sein des institutions gouvernementales. En effet, les OP reconnaissent de plus en plus les avantages liés à l'utilisation des ANP par les employés de l'État, lesquelles se traduisent notamment par la réduction des coûts par rapport au déploiement d'équipements informatiques fixes et par l'amélioration du rendement de travail et de la prestation des services compte tenu de l'accessibilité accrue de l'information en tout temps et en tout lieu.

Jusqu'en 2010, les appareils de type BlackBerry représentaient une forte proportion des ANP utilisés dans l'administration publique québécoise. L'évolution des technologies mobiles pousse aujourd'hui les organisations à considérer d'autres systèmes mobiles tout aussi efficaces, mais plus orientés vers l'expérience utilisateur et vers la simplicité d'utilisation, tels que le système iOS (iPhone/iPad) et le système Android (Google, Samsung, LG, Sony, etc.).

Si l'usage des ANP est désormais essentiel aux différent OP, ces appareils présentent cependant des enjeux de sécurité de l'information auxquels toute organisation doit faire face.

## 1.2. Objectif

Le présent guide a pour objet de proposer aux OP un cadre de référence pour une utilisation sécuritaire des ANP. Il décrit les risques et la vulnérabilité associés à leur usage ainsi que l'approche à adopter pour assurer leur déploiement sécuritaire. À cet effet, il :

- ✓ propose une démarche de déploiement sécuritaire;
- ✓ indique les rôles et responsabilités des principaux intervenants;
- ✓ détermine les meilleures pratiques à utiliser;
- ✓ propose un modèle de directive ministérielle (voir l'Annexe II du présent guide).

## 1.3. Portée

Le présent guide s'applique à trois catégories d'ANP : les téléphones intelligents, les tablettes numériques et les téléphones-tablettes (*phablettes*[8]) comprenant tout type de système d'exploitation (iOS, Android, BlackBerry, Windows 10 Mobile, etc.). Il exclut donc les ordinateurs portables, les

**8. Téléphone-tablette (*phablette*) :** Appareil hybride qui combine un téléphone intelligent et une tablette électronique. Le téléphone-tablette possède un écran assez grand pour permettre la lecture de caractères tout en pouvant tenir dans une seule main. *[OQLF - Grand dictionnaire terminologique]*

miniportables et les téléphones cellulaires de base ainsi que tout autre appareil mobile pouvant être relié aux réseaux sans fil.

De plus, le guide ne s'applique pas à la pratique *bring your own device* (BYOD) ou « prenez vos appareils personnels » (PAP). Les OP désirant employer une telle pratique doivent analyser rigoureusement les risques qui y sont associés et appliquer les mesures d'atténuation nécessaires.

## 1.4. Éléments d'appui

Le présent guide prend appui sur un cadre légal et normatif comprenant des lois, des directives, des normes internationales et des pratiques gouvernementales propres à la sécurité de l'information. Les principaux éléments constitutifs de ce cadre sont présentés à l'Annexe III.

# 2. Étude préalable au déploiement des assistants numériques personnels

La mobilité, la portabilité et la flexibilité des ANP rendent indéniable, voire incontournable leur utilisation. Leur déploiement est toutefois précédé d'une étude de positionnement qui permet de répondre à plusieurs interrogations, notamment :

- ✓ quelle technologie disponible sur le marché répondrait le mieux aux attentes de l'OP et serait la mieux acceptée par les utilisateurs (p. ex. iOS, Android, BlackBerry, Windows 10 Mobile, etc.)?
- ✓ quels seraient les utilisateurs potentiels des ANP au sein de l'organisation?
- ✓ de quelles applications a-t-on besoin et quelles sont les licences d'utilisation à acquérir?
- ✓ les ressources financières, technologiques et humaines sont-elles suffisantes pour assurer le déploiement et le soutien technique des ANP?

L'étude de positionnement répond également à des préoccupations de sécurité, notamment :

- ✓ l'accessibilité des ANP, en totalité ou en partie, au réseau de l'organisation;
- ✓ la formation pour une utilisation sécuritaire des ANP;
- ✓ les contrôles d'accès nécessaires;
- ✓ la destruction sécuritaire de l'information[9] stockée dans les ANP;
- ✓ les enjeux de sécurité de l'information en cas d'impartition de services par un OP, notamment dans les cas suivants :
    - o lorsque l'OP fait appel à un prestataire de services public ou privé pour le stockage de l'information, la gestion des ANP, leur configuration ou pour le soutien technique;
    - o lorsque les données consultées ou traitées sont stockées dans des serveurs localisés à l'extérieur du Canada.

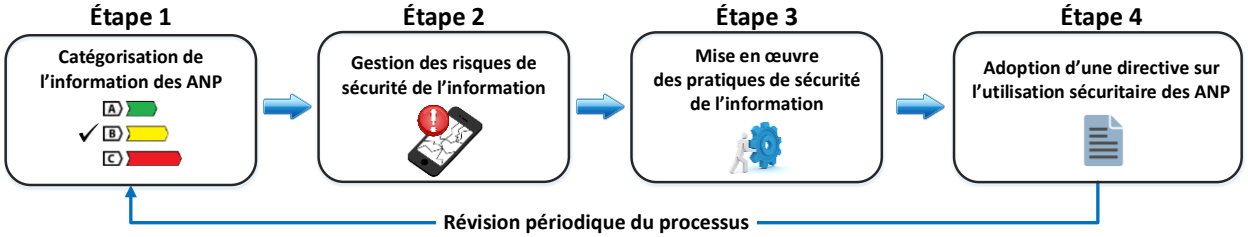
**9. Destruction sécuritaire de l'information :** Processus permettant d'effacer ou de détruire l'information emmagasinée sur un équipement, un dispositif ou sur tout autre support de données de façon à réduire le risque de récupération ou de reconstitution.

# 3. Démarche de déploiement sécuritaire des assistants numériques personnels

Le recours aux ANP est généralement encadré par des mesures de réduction des risques, lesquelles se traduisent par une démarche en quatre étapes : la catégorisation de l'information, la gestion des risques de sécurité de l'information, la mise en œuvre de pratiques de sécurité de l'information ainsi que l'élaboration et la diffusion d'une directive sur l'utilisation sécuritaire des ANP.

La démarche est complétée par une révision du processus sur une base régulière, notamment pour repérer les nouvelles menaces et situations de vulnérabilité ainsi que les nouvelles pratiques de sécurité qui seraient mieux adaptées à l'évolution du contexte organisationnel.

**Figure 1 - Démarche de déploiement sécuritaire des ANP**




## 3.1. Étape 1 – Catégorisation de l'information des ANP

La première étape consiste à catégoriser[10] l'information. Pour ce faire, l'OP détermine les intervenants qui seront concernés par le déploiement des ANP et évalue le niveau de criticité de l'information qu'ils utilisent afin de décider si son accès peut être autorisé au moyen d'un ANP, ou si elle peut y être stockée. Pour la réalisation de cette étape, les OP prendront appui sur la pratique recommandée PR-057 intitulée « Guide de catégorisation de l'information ».

## 3.2. Étape 2 – Gestion des risques de sécurité de l'information

La deuxième étape consiste à gérer les risques liés à l'utilisation des ANP. Pour ce faire, l'OP détermine les risques éventuels (p. ex. bris ou perte de l'appareil, interception des données de l'ANP dans des lieux publics, installation d'une application malveillante, etc.) et il les classe selon la priorité de traitement qui leur est accordée. Il définit par la suite les pratiques de sécurité à mettre en œuvre pour réduire les risques reconnus. Pour la réalisation de cette étape, les OP prendront appui sur la pratique recommandée PR-062 intitulée « Guide d'élaboration et de mise en œuvre d'un processus de gestion des risques de sécurité de l'information ».

**10. Catégorisation :** Processus permettant de déterminer le niveau de criticité des actifs informationnels, compte tenu de l'impact que peut engendrer un bris de disponibilité, d'intégrité ou de confidentialité de ces actifs sur l'organisme et sa clientèle ou sur d'autres organismes.

## 3.3. Étape 3 – Mise en œuvre des pratiques de sécurité de l'information

La troisième étape consiste à mettre en œuvre les pratiques de sécurité de l'information déterminées à l'étape de la gestion des risques (étape 2). À cet effet, une priorisation quant au déploiement des pratiques de sécurité est établie. De même, un calendrier de mise en œuvre précisant les échéanciers ainsi que le partage des responsabilités est adopté.

À la suite de la priorisation préalable des pratiques de sécurité, l'OP dresse un calendrier détaillé de mise en œuvre qui précise les échéanciers et les responsables clés en commençant par les pratiques les plus importantes.

## 3.4. Étape 4 – Adoption d'une directive sur l'utilisation sécuritaire des assistants numériques personnels

La dernière étape consiste à élaborer, diffuser et mettre à jour une directive permettant d'encadrer efficacement l'utilisation sécuritaire des ANP (voir le modèle de directive à l'Annexe II du présent guide). Cette directive énonce les objectifs, les principes directeurs, les règles de gestion et de distribution des ANP, les responsabilités des intervenants et la ligne de conduite relativement à la transmission, à la réception et à la conservation de l'information associée à l'utilisation d'un ANP. La directive est approuvée par la haute direction avant d'être publiée.

Il convient également de mettre en œuvre un programme de sensibilisation et, au besoin, de formation pour s'assurer de la bonne compréhension, par l'ensemble du personnel, des dispositions de la directive, des pratiques de sécurité qui en découlent et de la procédure à appliquer selon la situation de risque. En appui à ce programme, il convient de mettre à la disposition des utilisateurs concernés un résumé des pratiques clés relatives à l'utilisation sécuritaire des ANP.

# 4. Responsabilités des intervenants

Cette section présente les principaux intervenants et leurs responsabilités en matière de sécurité de l'information associée à l'utilisation des ANP. Bien que les responsabilités décrites soient applicables à la plupart des OP, il convient, pour ces derniers, de les adapter à leur contexte.

## 4.1. Responsable organisationnel de la sécurité de l'information (ROSI)

En tant que porte-parole du dirigeant principal de l'information (DPI), le ROSI assiste son dirigeant d'organisme dans la détermination des orientations stratégiques et des priorités d'intervention relativement à la sécurité de l'information. En matière de sécurité de l'information associée à l'utilisation des ANP, il :

- ✓ coordonne l'élaboration et la mise en application d'une directive ministérielle énonçant les principes directeurs pour une utilisation sécuritaire des ANP;
- ✓ coordonne l'élaboration et la mise en œuvre d'un programme de sensibilisation en matière d'utilisation sécuritaire des ANP;
- ✓ soumet la directive ministérielle et le programme de sensibilisation à la consultation du comité chargé de la sécurité de l'information de son organisation et tient compte des éventuelles recommandations et suggestions;
- ✓ soumet la directive ministérielle et le programme de sensibilisation en matière d'utilisation sécuritaire des ANP à l'approbation de la haute direction.

## 4.2. Conseiller organisationnel en sécurité de l'information (COSI)

Le COSI apporte son soutien au ROSI, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques touchant la sécurité de l'information. En ce qui a trait à la sécurité de l'information associée à l'utilisation des ANP, il :

- ✓ analyse les risques de sécurité de l'information associés à l'utilisation des ANP;
- ✓ élabore la directive ministérielle en matière d'utilisation sécuritaire des ANP;
- ✓ s'assure de la mise en application de la directive ministérielle;
- ✓ élabore un programme de sensibilisation pour conscientiser le personnel aux bonnes pratiques d'utilisation sécuritaire des ANP;
- ✓ s'assure de la mise en œuvre du programme de sensibilisation;
- ✓ évalue régulièrement l'application de la directive ministérielle et le programme de sensibilisation en matière d'utilisation sécuritaire des ANP et procède aux ajustements nécessaires.

## 4.3. Coordonnateur organisationnel de gestion des incidents (COGI)

Fort de sa connaissance des menaces et des situations de vulnérabilité ainsi que de son expertise en matière de gestion des risques et des incidents, le COGI apporte au ROSI le soutien technique nécessaire à l'exercice de ses fonctions. À cet effet, il :

- ✓ contribue à l'analyse des risques de sécurité de l'information, notamment à l'identification des menaces et des situations de vulnérabilité associées à l'utilisation des ANP;
- ✓ détermine les mesures de sécurité appropriées et s'assure de leur mise en œuvre;
- ✓ détermine les stratégies de réaction et les procédures associées à appliquer en cas d'incident lié à l'utilisation des ANP;
- ✓ évalue régulièrement les stratégies de réaction aux incidents et les mesures de sécurité en place et s'assure de leur efficacité.

## 4.4. Direction des ressources informationnelles

La Direction des ressources informationnelles est responsable de fournir à l'organisation l'encadrement, le soutien et les mécanismes d'exploitation et de prévention nécessaires à l'utilisation sécuritaire des ANP. À cette fin, elle :

- ✓ assure la gestion, la distribution et l'administration des ANP et en définit les règles associées;
- ✓ met en application des mesures de sécurité relevant de sa compétence, en avise les utilisateurs et en contrôle l'efficacité;
- ✓ s'assure que l'information est détruite dans des situations d'urgence, lors du transfert d'un ANP d'un utilisateur à un autre ou avant que l'appareil ne soit acheminé à la réparation, au recyclage ou au rebut;
- ✓ assure la sensibilisation, la formation et le soutien aux personnes concernées pour une utilisation sécuritaire des ANP;
- ✓ effectue la reddition de comptes exigée par le responsable organisationnel de la sécurité de l'information de l'organisation.

## 4.5. Utilisateurs

L'utilisateur est responsable de la protection de l'information transitant par son ANP de même que de son traitement et de sa conservation sécuritaire. À cette fin, il :

- ✓ s'engage à respecter les lignes de conduite énoncées dans la directive ministérielle en matière d'utilisation sécuritaire des ANP.
- ✓ applique en tout temps et en tout lieu les bonnes pratiques en matière d'utilisation sécuritaire de son ANP;
- ✓ s'engage à ne pas modifier la configuration et les mesures de sécurité mises en place sur son ANP;
- ✓ informe les entités responsables de toute violation des mesures de sécurité dont il pourrait être témoin et de toute anomalie ou incident pouvant nuire à la sécurité de l'information stockée dans son ANP.

# 5. Pratiques de sécurité recommandées

Cette section présente sommairement les risques, les situations de vulnérabilité et les objectifs de sécurité (DIC : disponibilité[11], intégrité[12] et confidentialité[13]) associés aux fonctionnalités et aux caractéristiques d'un ANP. Elle propose également des pratiques de sécurité à adopter afin de réduire les risques et les conséquences qui en découlent. La liste complète des pratiques recommandées figure à l'Annexe IV.

Il est à noter que les pratiques de gestion de l'ANP (p. ex. contrôle d'accès, configuration du système, etc.) relèvent de l'unité administrative responsable de la gestion et de l'administration des ANP au sein de l'OP. Les autres pratiques concernent les utilisateurs de l'ANP. Il est de la responsabilité de l'organisation de s'assurer que chacun des usagers concernés est formé et sensibilisé aux pratiques recommandées.

Les sujets de la présente section ne sont pas présentés selon un ordre d'importance. Le lecteur peut consulter la totalité des sujets abordés ou uniquement ceux qu'il juge pertinents selon le contexte de son organisation.

---

**11**. **Disponibilité :** Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée. *[Directive sur la sécurité de l'information gouvernementale]*

**12**.**Intégrité :** Propriété d'une information de ne pas être détruite ou altérée de quelque façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues. *[Directive sur la sécurité de l'information gouvernementale]*

**13. Confidentialité :** Propriété d'une information de n'être accessible qu'aux personnes autorisées. *[Directive sur la sécurité de l'information gouvernementale]*

## 5.1. Transportabilité

La taille réduite de l'ANP en fait un outil pratique et convivial lors de déplacements, puisqu'il offre la plupart des fonctionnalités du micro-ordinateur[14]. Toutefois, cette caractéristique peut également rendre l'ANP vulnérable, puisqu'il peut facilement être perdu, volé ou détérioré.

### 5.1.1 Risques

1. **Bris de l'ANP et perte des données –** En raison de son côté pratique et facile à transporter, l'ANP accompagne l'utilisateur dans la plupart de ses déplacements. Cela contribue à accroître le risque de bris de l'appareil, souvent par inadvertance ou par maladresse. Un tel bris peut rendre indisponible l'information si elle n'est pas sauvegardée et accessible sur un autre support.
2. **Perte, vol et violation de la confidentialité –** Compte tenu de sa taille réduite et des fonctionnalités multiples qu'il offre, l'ANP peut être utilisé hors des locaux de l'OP. Cela accroît notamment le risque de perte ou de vol de l'appareil, principalement dans les lieux publics. La perte ou le vol de l'ANP peut, dans certains cas, entraîner l'accès non autorisé par une personne malintentionnée aux données sensibles contenu dans l'appareil. Cette même personne pourrait également divulguer les données sensibles ou s'en servir pour perpétrer d'autres actes malveillants (p. ex. usurpation d'identité, accès non autorisé au réseau de l'organisation, etc.).

### 5.1.2 Pratiques recommandées

**P1 :** **Désactiver l'ANP après un nombre déterminé de tentatives d'accès infructueuses –** Configurer un temps d'attente de plus en plus long à chaque tentative d'accès à l'appareil. Activer le blocage ou la désactivation automatique de l'ANP après plusieurs tentatives d'accès infructueuses (établir un nombre optimal d'essais, par exemple cinq). Cette mesure permet d'empêcher des attaques informatiques visant à connaître le mot de passe de l'ANP pour accéder à son contenu.

**P2 :** **Activer le verrouillage automatique de l'ANP après un court délai d'inactivité –** Un délai de 1 à 5 minutes avant un verrouillage automatique ou la mise en veille de l'appareil ajoute une protection supplémentaire en cas de perte ou lorsque l'ANP est laissé sans surveillance. En effet, si le délai d'inactivité est expiré, une personne malintentionnée ne pourra pas accéder au contenu de l'appareil sans connaître le mot de passe.

**P3 :** **Désactiver l'affichage des messages de notification lorsque l'ANP est verrouillé –** Certaines applications envoient des messages de notification d'événements à l'utilisateur, qui peuvent revêtir un caractère confidentiel. Ces messages sont signalés au moyen d'un son, d'une vibration ou d'un message d'alerte, et ce, même si l'appareil est verrouillé (p. ex. nouveau courriel ou message texte entrant, approche d'un événement planifié dans le calendrier, etc.). La non-désactivation de cette fonction permet à une personne malintentionnée de consulter des alertes privées sans avoir à déverrouiller l'ANP.

**14. Micro-ordinateur :** Ordinateur de dimension réduite dont l'unité centrale est constituée d'un ou plusieurs microprocesseurs. *[OQLF - Grand dictionnaire terminologique]*

**P4 :** **Verrouiller l'ANP avec un mot de passe –** L'accès à l'ANP doit toujours être protégé par un mot de passe. Cette mesure simple et efficace permet d'assurer la confidentialité des données que contient l'appareil.

**P8 :** **Chiffrer les données sensibles –** Chiffrer les données sensibles stockées sur l'ANP. Cette mesure permet de préserver la confidentialité de l'information en cas d'interception ou d'extraction des données par une personne malintentionnée. Le chiffrement des données doit être fait à l'aide d'un algorithme dont la robustesse est éprouvée.

**P9 :** **Supprimer le contenu de l'ANP à distance –** Activer l'option d'administration de données à distance pour pouvoir supprimer l'information que contient l'ANP en cas de perte ou de vol. Cette pratique peut être combinée avec la pratique 1. Les données seraient alors automatiquement effacées après un nombre défini de tentatives d'accès infructueuses.

**P26 :** **Ne pas inscrire ou afficher le nom de l'organisation sur l'ANP –** Ne pas inscrire ou afficher sur l'appareil de l'information permettant d'identifier l'organisme public (logo, nom de l'OP, etc.) pour ne pas susciter l'intérêt de personnes mal intentionnées.

**P27 :** **Communiquer avec les entités responsables –** En cas de perte ou de vol de l'appareil, communiquer sans délai la situation à l'unité administrative responsable de la gestion de l'ANP ou au fournisseur de services de l'appareil pour connaître la procédure à suivre. Ces spécialistes peuvent notamment verrouiller et localiser l'appareil, supprimer le contenu de l'ANP à distance et bloquer la carte SIM en cas de nécessité.

**P28 :** **Établir une communication avec l'ANP (messagerie ou téléphonie) –** En cas de perte de l'ANP, tenter d'établir une communication avec l'appareil, notamment en envoyant un message sur l'écran de verrouillage à l'intention de la personne qui l'aurait trouvé, en indiquant les coordonnées nécessaires pour le récupérer. S'il s'agit d'un téléphone intelligent ou d'un téléphone-tablette, une communication téléphonique peut également être établie.

**P35 :** **Chiffrer les données sensibles stockées sur la carte mémoire amovible –** Cette mesure permet de préserver la confidentialité de l'information des données contenues dans la carte mémoire amovible insérée dans l'ANP. Le chiffrement des données doit être fait à l'aide d'un algorithme dont la robustesse est éprouvée.

**P44 :** **Garder l'ANP dans un endroit sûr pendant les déplacements – Lors** des déplacements, ne pas laisser l'ANP dans un endroit non sécuritaire ou sans surveillance (p. ex. poche arrière du pantalon, sur une table, sur un comptoir, etc.), même pour une courte durée. Prendre l'habitude de garder l'ANP sur soi (poche avant ou accroché à la ceinture) ou dans un sac à portée de la main.

**P51 :** **Effacer les données sensibles de l'ANP à la fin de leur utilisation –** Lorsqu'une information sensible n'est plus utile, la supprimer de l'ANP élimine le risque qu'elle soit consultée par une personne malveillante.

**P53 :** **Stocker uniquement de l'information utile sur l'ANP –** Stocker seulement les données qui sont utiles au travail lors des déplacements pour ne pas compromettre d'autres données sensibles en cas d'incident.

**P62 : Effectuer régulièrement la sauvegarde des données contenues dans l'ANP –** Une copie de sécurité de l'ANP doit être faite sur une base régulière. Cette action est généralement prise en charge par l'unité administrative responsable de la gestion de l'ANP. Après un incident (p. ex. perte, vol, bris ou disfonctionnement de l'appareil), les copies de sécurité peuvent être utilisées pour récupérer l'information perdue ou restaurer l'état fonctionnel de l'ANP.

### 5.1.3 Tableau récapitulatif

| Risque | Vulnérabilité | Objectif de sécurité (DIC[15]) | Pratique recommandée |
|---|---|---|---|
| 1. Bris de l'ANP et perte des données | ✓ Transportabilité<br>✓ Accident ou maladresse de l'utilisateur | D | ✓ **P62 :** Effectuer régulièrement la sauvegarde des données de l'ANP |
| 2. Perte, vol et violation de la confidentialité | ✓ Transportabilité | D et C | ✓ **P1 :** Désactiver l'ANP après un nombre défini de tentatives d'accès infructueuses<br>✓ **P2 :** Activer le verrouillage automatique de l'ANP après un court délai d'inactivité<br>✓ **P3 :** Désactiver l'affichage des messages de notification lorsque l'ANP est verrouillé<br>✓ **P4 :** Verrouiller l'ANP avec un mot de passe<br>✓ **P8 :** Chiffrer les données sensibles<br>✓ **P9 :** Supprimer le contenu de l'ANP à distance<br>✓ **P26 :** Ne pas inscrire ou afficher le nom de l'organisation sur l'ANP<br>✓ **P27 :** Communiquer avec les entités responsables<br>✓ **P28 :** Établir une communication avec l'ANP (messagerie ou téléphonie)<br>✓ **P35 :** Chiffrer les données sensibles stockées sur la carte mémoire amovible |

15. **DIC :** Disponibilité, Intégrité, Confidentialité

| Risque | Vulnérabilité | Objectif de sécurité (DIC[15]) | Pratique recommandée |
|---|---|---|---|
| | | | ✓ **P44 :** Garder l'ANP dans un endroit sûr lors des déplacements<br>✓ **P51 :** Effacer les données sensibles de l'ANP à la fin de leur utilisation<br>✓ **P53 :** Stocker uniquement de l'information utile sur l'ANP<br>✓ **P62 :** Effectuer régulièrement la sauvegarde des données de l'ANP |

## 5.2. Connexion aux réseaux sans fil

L'ANP a accès, grâce à la technologie des radiofréquences, à un large éventail d'interfaces de communication sans fil. Cela lui permet d'échanger des données directement avec d'autres ANP et de se synchroniser avec toute une gamme d'appareils électroniques sans fil (p. ex. casque d'écoute ou haut-parleurs sans fil, caméra sans fil, etc.). Toutefois, cette capacité de se connecter presque partout fait de l'ANP une cible idéale pour le piratage et l'interception des communications par les cybercriminels.

La présente section s'intéresse principalement aux risques liés à trois types de connexion sans fil : le Wi-Fi, le Bluetooth et le NFC.

**La technologie Wi-Fi**

Le Wi-Fi est une technologie de transmission de données destinée à un *réseau local sans fil* (WLAN[16]) conforme aux normes IEEE 802.11[17]. Elle utilise des ondes électromagnétiques ou radiofréquences pour transmettre et recevoir des données au lieu des réseaux locaux câblés traditionnels. Elle simplifie et accélère l'installation des réseaux et accroît leur souplesse et leur évolutivité tout en favorisant une plus grande mobilité des utilisateurs.

**La technologie Bluetooth**

Bluetooth est une technologie de *réseau personnel sans fil* (WPAN[18]) de faible portée[19] permettant à plusieurs appareils proches de communiquer entre eux sans liaison filaire, tout en consommant peu d'énergie. Elle a été conçue pour des applications commerciales (p. ex. casque d'écoute ou haut-parleur sans fil, transmission de données médicales d'un capteur sans fil, etc.), sans nécessairement se soucier de la protection de l'information qui est échangée entre les appareils. Cette technologie ne comporte que peu de solutions de sécurisation de l'information.

---

**16. Le réseau local sans fil (WLAN)** couvre l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre eux les terminaux présents dans la zone de couverture. Il renferme notamment la technologie Wi Fi qui, lorsqu'elle est conforme à la norme IEEE 802.11n, offre des débits théoriques de plus de 150 Mbit/s. En utilisant la norme IEEE 802.11ac, la technologie Wi-Fi peut offrir des débits pouvant atteindre 1,3 Gbit/s.

**17. Les normes IEEE 802.11** font référence à une gamme de spécifications mises au point par l'Institute of Electrical and Electronics Engineers (IEEE) (ou l'Institut des ingénieurs électriciens et électroniciens) destinées à l'implémentation de réseaux locaux sans fil (WLAN). Elles définissent notamment les principes de communication radio entre unités (client-point d'accès, point d'accès-point d'accès, client-client).

**La technologie NFC**

La communication en champ proche ou *near field communication* (NFC) est une technologie de communication sans fil de courte portée (environ 10 cm) qui permet à divers appareils électroniques, notamment les ANP, d'échanger de petites quantités de données entre eux ou avec une carte à puce sans contact. Intégrée aux ANP, la technologie NFC permet notamment aux utilisateurs d'acheter des produits en magasin avec un simple rapprochement de l'ANP du lecteur NFC du commerçant. L'ANP peut aussi servir de lecteur NFC. Ainsi, avec un simple rapprochement de deux ANP ou d'un ANP et d'une étiquette électronique NFC[20] (*NFC tag*) préalablement configurée, l'utilisateur peut exécuter rapidement certaines tâches et lire ou partager des données (p. ex. déverrouiller l'ANP, activer une option comme la connexion Wi-Fi ou Bluetooth, partager la connexion Wi-Fi avec des invités, partager des contacts, lire le contenu d'un passeport, etc.).

### 5.2.1. Risques

1. **Écoute clandestine – faux point d'accès –** Un pirate informatique peut établir un faux point d'accès sans fil en usurpant le nom (SSID[21]) du réseau de l'organisation ou celui d'un lieu public (p. ex. un café, un hôtel, un aéroport, etc.). Il peut, par cet intermédiaire, intercepter des mots de passe ou prendre connaissance de renseignements sensibles qui lui sont transmis lorsque la victime accède à Internet. Si l'ANP est configuré pour être connecté automatiquement à un réseau sans fil[22] connu à proximité, il se connectera directement au faux point d'accès, car ce dernier émet généralement un signal plus fort que le vrai point d'accès.

2. **Écoute clandestine – réseau Wi-Fi –** Qu'il s'agisse du réseau sans fil de l'organisation ou de celui d'un lieu public, les données qui y transitent peuvent être interceptées par un cybercriminel. En effet, il existe des outils gratuits d'administration de réseau qui permettent à une personne

---

**18. Le réseau personnel sans fil (WPAN)** est d'une faible portée, soit de l'ordre de quelques dizaines de mètres. Il sert généralement à relier un ordinateur à un ANP ou à un périphérique (imprimante, combiné de téléphone portable, appareils domestiques, etc.). De fait, le réseau personnel sans fil est utilisé surtout pour permettre une liaison entre des équipements rapprochés.

**19.** La portée de la majorité des ANP compatibles avec Bluetooth est d'une dizaine de mètres, mais elle peut aller jusqu'à près de 100 mètres.

**20. Étiquette électronique NFC (NFC *tag*)** : Étiquette qui sert à identifier des objets et qui est constituée d'une puce contenant des données et d'un dispositif électronique capable, à l'aide d'une antenne radio, de transmettre les informations à un lecteur spécialisé. [*OQLF - Grand dictionnaire terminologique*]

**21. SSID :** Le *Service set identifier* est le nom du réseau sans fil.

**22. Réseau sans fil :** Réseau qui permet de relier sans fil, c'est-à-dire par des liaisons radioélectriques ou des liaisons infrarouges, les appareils informatiques d'un groupe de personnes qui doivent communiquer entre elles. *[OQLF - Grand dictionnaire terminologique]*

connectée à un réseau d'intercepter toute information qui y circule et de la lire si elle n'est pas chiffrée.

3. **Accès non autorisé aux données de l'ANP par connexion Bluetooth –** Le mot de passe initial de la connexion Bluetooth d'un ANP est généralement identique pour tous les ANP du même modèle. Il correspond souvent à « 1234 » ou « 0000 ». Une personne malintentionnée pourrait simplement faire une recherche sur Internet pour découvrir, selon le modèle de l'appareil, le mot de passe par défaut. Une fois connecté à l'ANP, elle pourra accéder aux données personnelles de la victime (p. ex. mots de passe, documents, contacts, etc.) et commettre d'autres actions malveillantes comme l'usurpation d'identité, l'intrusion dans le réseau de l'organisation, etc.

4. **Exécution de tâches non souhaitées par connexion Bluetooth –** Après connexion à l'ANP par Bluetooth, une personne malintentionnée peut exécuter des commandes lui permettant d'avoir le contrôle de l'appareil. Elle peut notamment lire ou écrire dans le répertoire téléphonique, lire ou envoyer des messages textes (SMS), faire des appels surtaxés ou malveillants, modifier la configuration de l'appareil (activation de la connexion Wi-Fi, contrôle du volume sonore, etc.).

5. **Accès non autorisé aux données de l'ANP avec un lecteur NFC** – Les utilisateurs d'un ANP doté de la technologie NFC peuvent partager, à leur insu, des données confidentielles (p. ex. adresses, contacts, numéros de cartes de crédit, mots de passe, etc.) avec une personne malintentionnée. Un pirate informatique peut notamment obtenir certains de ces renseignements avec un simple rapprochement entre l'ANP de la victime et un lecteur NFC ou un autre ANP.

6. **Exécution de tâches non souhaitées et installation de logiciels malicieux –** Un pirate informatique peut programmer un appareil ou une étiquette électronique (NFC *tag*) équipée de la technologie NFC pour obliger un ANP qui se trouve à proximité (environ 10 cm) à exécuter une tâche non souhaitée (p. ex. activer la connexion Wi-Fi ou Bluetooth, activer le partage de la connexion Internet, ouvrir une page Web indésirable, etc.). Une telle attaque peut également être utilisée pour transférer automatiquement un logiciel malicieux vers l'ANP, qui se chargera de récupérer des données sensibles de la victime par la suite.

### 5.2.2. Pratiques recommandées

**P6 :** **Sécuriser le réseau de l'organisation par le chiffrement des communications et un système d'authentification –** Les réseaux Wi-Fi offrent des solutions robustes de chiffrement des communications à l'exemple de l'infrastructure à clés publiques. Le protocole de chiffrement WEP est fortement déconseillé, car la clé de chiffrement peut être décryptée en quelques minutes. La solution WPA2 est recommandée, car elle utilise un mécanisme de chiffrement plus robuste. Selon le niveau de sensibilité du réseau de l'organisation, une authentification composée d'un identifiant et d'un mot de passe pourrait être envisagée afin d'éviter les intrusions.

**P23 :** **Utiliser un réseau privé virtuel (RPV) pour accéder à distance au réseau de l'organisation –** Lors d'une connexion à un point d'accès sans fil en dehors des locaux de l'organisation, il est recommandé d'utiliser le réseau privé virtuel pour tout accès au réseau de l'organisation. La connexion doit être sécurisée par un identifiant et un mot de passe robuste. Le RPV (ou VPN en

anglais) permet de créer une connexion directe et chiffrée entre l'ANP et les serveurs de l'organisation, rendant ainsi les communications sécuritaires.

**P29 : Sensibiliser les utilisateurs d'ANP et les former –** Mettre en œuvre des plans de formation et de sensibilisation périodiques destinés aux utilisateurs d'ANP pour, d'une part, les informer des risques de sécurité de l'information liés à l'utilisation d'un ANP et, d'autre part, leur présenter la directive ministérielle et les mesures de sécurité établies par l'OP à cet égard.

**P45 : Désactiver la connexion Wi-Fi lorsqu'elle n'est pas utilisée –** La désactivation de la connexion Wi-Fi empêche l'ANP de se connecter automatiquement à des points d'accès connus, mais dont le nom (SSID) a été usurpé. Lorsque le besoin se présente, activer la connexion Wi-Fi et s'assurer que l'ANP est connecté au bon réseau.

**P46 : Être vigilant lors de la connexion aux réseaux sans fil ouverts –** La connexion de l'ANP à un réseau sans fil en dehors des locaux de l'organisation, notamment dans des lieux publics (p. ex. café, hôtel, aéroport, etc.), doit être faite avec prudence et se limiter au minimum de temps nécessaire, car les données qui y circulent peuvent être interceptées par une personne malintentionnée. Il est recommandé de ne pas consulter ou transférer des données critiques à l'occasion d'une telle connexion.

**P47 : Désactiver la connexion Bluetooth lorsqu'elle n'est pas utilisée –** La désactivation de la connexion Bluetooth rend l'ANP « invisible » et permet d'éviter son pairage avec des appareils inconnus utilisant la même technologie. En théorie, lors d'une demande de pairage, l'utilisateur est averti et les deux parties doivent convenir d'un mot de passe pour permettre la connexion. En pratique, plusieurs ANP ne permettent pas de modifier la configuration par défaut en vue de paramétrer les mesures de sécurité nécessaires. Dans un tel cas, un pirate informatique pourrait se connecter à l'ANP à l'aide de Bluetooth et, par exemple, en extraire la liste des contacts.

**P48 : Désactiver la connexion NFC lorsqu'elle n'est pas utilisée –** La désactivation de la connexion NFC permet d'éviter un échange de données confidentielles, à l'insu de l'utilisateur, avec un autre appareil malicieux. Cette pratique empêche également un pirate informatique d'envoyer des logiciels malicieux à l'ANP par un simple contact ou rapprochement physique avec l'ANP.

**P49 : Réduire l'utilisation de la technologie NFC au minimum –** La technologie NFC dans un ANP est très pratique et simple à utiliser. Elle est néanmoins tout aussi vulnérable, car elle ne comporte aucun système d'authentification pour s'assurer que l'échange de données entre deux appareils est légitime. Des attaques informatiques peuvent alors être lancées sans que l'utilisateur s'en aperçoive.

**P57 : Modifier le mot de passe ou le NIP par défaut de la connexion Bluetooth de l'ANP – Cette** pratique permet d'éviter le jumelage de l'ANP avec un appareil inconnu qui tenterait d'utiliser le mot de passe par défaut. Éviter d'utiliser un ANP qui ne permet pas le changement du mot de passe de la connexion Bluetooth.

### 5.2.3. Tableau récapitulatif

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| 1. Écoute clandestine – faux point d'accès | ✓ La connexion à un point d'accès connu se fait de façon automatique, même si le nom du réseau (SSID) a été usurpé | C | ✓ **P29 :** Sensibiliser les utilisateurs d'ANP et les former<br>✓ **P45 :** Désactiver la connexion Wi-Fi lorsqu'elle n'est pas utilisée<br>✓ **P46 :** Être vigilant lors de la connexion aux réseaux sans fil ouverts |
| 2. Écoute clandestine – réseau Wi-Fi | ✓ Réseau non sécurisé<br>✓ Communications non chiffrées | C | ✓ **P6 :** Sécuriser le réseau de l'organisation par le chiffrement des communications et un système d'authentification<br>✓ **P23 :** Utiliser un réseau privé virtuel (RPV) pour accéder à distance au réseau de l'organisation<br>✓ **P29 :** Sensibiliser les utilisateurs d'ANP et les former<br>✓ **P46 :** Être vigilant lors de la connexion aux réseaux sans fil ouverts |
| 3. Accès non autorisé aux données de l'ANP par connexion Bluetooth | ✓ Mot de passe par défaut identique pour tous les ANP d'un même fabricant | C | ✓ **P29 :** Sensibiliser les utilisateurs d'ANP et les former<br>✓ **P47 :** Désactiver la connexion Bluetooth lorsqu'elle n'est pas utilisée<br>✓ **P57 :** Modifier le mot de passe ou le NIP par défaut de la connexion Bluetooth de l'ANP |
| 4. Exécution de tâches non souhaitées par | ✓ Mot de passe par défaut identique pour tous les ANP d'un même fabricant | C et I | ✓ **P29 :** Sensibiliser les utilisateurs d'ANP et les former |

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| connexion Bluetooth | | | ✓ **P47 :** Désactiver la connexion Bluetooth lorsqu'elle n'est pas utilisée<br>✓ **P57 :** Modifier le mot de passe ou le NIP par défaut de la connexion Bluetooth de l'ANP |
| 5. Accès non autorisé aux données de l'ANP avec un lecteur NFC | ✓ Absence de système d'authentification pour s'assurer que l'échange de données entre deux appareils est légitime | C et I | ✓ **P29 :** Sensibiliser les utilisateurs d'ANP et les former<br>✓ **P48 :** Désactiver la connexion NFC lorsqu'elle n'est pas utilisée<br>✓ **P49 :** Réduire l'utilisation de la technologie NFC au minimum |
| 6. Exécution de tâches non souhaitées et installation de logiciels malicieux | ✓ Absence de système d'authentification pour s'assurer que l'échange de données entre deux appareils est légitime | I | ✓ **P29 :** Sensibiliser les utilisateurs d'ANP et les former<br>✓ **P48 :** Désactiver la connexion NFC lorsqu'elle n'est pas utilisée<br>✓ **P49 :** Réduire l'utilisation de la technologie NFC au minimum |

## 5.3. Services SMS et SMM

Le SMS (service de messages succincts) permet la transmission des messages textes à partir d'un ANP. Le SMM (service de messagerie multimédia) permet quant à lui de transmettre des messages textes accompagnés de fichiers numériques tels que des vidéos, des sons ou des images[23].

### 5.3.1. Risques

1. **Interception des données transmises par SMS ou SMM –** Les messages SMS et les données accompagnant les messages SMM peuvent être interceptés par une tierce personne non autorisée.

**23.** Rappelons que les SMS et les SMM constituent des documents au sens de la Loi concernant le cadre juridique des technologies de l'information.

Cela est possible en utilisant un appareil qui amplifie le signal cellulaire pour que l'ANP s'y connecte automatiquement. Étant programmable, cet appareil peut également intercepter et conserver toutes les communications cellulaires (messages textes, sons, vidéos, images, etc.) des ANP qui entrent dans sa zone de couverture, laquelle peut s'étendre jusqu'à 10 à 12 mètres.

2. **Consultation non autorisée des messages SMS ou SMM –** En cas d'intrusion dans le système de l'ANP, ou lorsque l'ANP est laissé déverrouillé sans surveillance, les messages SMS et SMM peuvent être consultés, de même que la date et l'heure d'envoi ou de réception et le nom des destinataires. La lecture d'un message critique peut avoir des conséquences graves pour l'utilisateur, pour l'organisation ou pour les destinataires concernés.

3. **Exposition à des logiciels malicieux –** Les logiciels malicieux peuvent être envoyés par SMS ou SMM. Ils se présentent généralement sous la forme d'un lien hypertexte ou d'un logiciel à installer en pièce jointe. L'infection de l'ANP par un logiciel malicieux peut compromettre la disponibilité, l'intégrité et la confidentialité des données qui y sont stockées. Dans certains cas, lorsque l'ANP a été infecté, le logiciel malicieux peut répéter l'attaque en envoyant le même message piégé à tous les contacts de l'utilisateur, augmentant alors de façon exponentielle le nombre de victimes.

4. **Divulgation d'information sensible par SMS ou SMM –** Puisqu'ils sont un moyen de communication rapide, les SMS et les SMM sont souvent privilégiés pour envoyer de courts messages ou de faibles volumes de données. L'envoi par inadvertance d'un message critique (p. ex. un mot de passe, une décision importante et confidentielle, etc.) peut avoir des conséquences graves pour l'utilisateur ou pour l'organisation.

### 5.3.2. Pratiques recommandées

**P3 :** **Désactiver l'affichage des messages de notification lorsque l'ANP est verrouillé –** Certaines applications envoient des messages de notification d'événements à l'utilisateur, qui peuvent revêtir un caractère confidentiel. Ces messages sont signalés au moyen d'un son, d'une vibration ou d'un message d'alerte, et ce, même si l'appareil est verrouillé (p. ex. nouveau courriel ou message texte entrant, approche d'un événement planifié dans le calendrier, etc.). La non-désactivation de cette fonction permet à une personne malintentionnée de consulter des alertes privées sans avoir à déverrouiller l'ANP.

**P12 :** **Utiliser des applications qui sécurisent l'envoi des messages –** Il existe des applications de messagerie instantanée qui permettent d'envoyer des messages sécurisés. Ces messages sont notamment entièrement chiffrés, rendant ainsi l'information illisible même si elle est interceptée par une personne malintentionnée lors de sa transmission.

**P13 :** **Désactiver les services SMS et SMM s'ils ne sont pas requis par l'organisation –** Si l'organisme public ne voit aucune utilité aux SMS ou aux SMM pour la réalisation de sa mission, il est préférable de désactiver ces services.

**P15 :** **Installer un antivirus sur l'ANP –** L'installation d'un antivirus sur l'ANP peut aider à éliminer certains logiciels malicieux installés par mégarde. Par ailleurs, sa mise à jour périodique est essentielle pour maintenir un niveau élevé de sécurité sur l'ANP.

**P22 : Effacer les messages SMS ou SMM sensibles lorsqu'ils ont été lus –** Les services de messagerie SMS et SMM ne sont pas adaptés au stockage de données sensibles. Les messages SMS à caractère sensible doivent donc être supprimés après leur lecture. L'information sensible pourrait être stockée dans un endroit plus sûr (p. ex. poste de travail) avant sa suppression.

**P41 : Éviter de communiquer des données sensibles au moyen des services SMS et SMM –** Étant donné la facilité d'interception des messages SMS et SMM, ces services de messagerie ne sont pas adaptés à l'envoi de données sensibles.

### 5.3.3. Tableau récapitulatif

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| 1. Interception des données | ✓ La connexion à une antenne est automatique lorsque l'ANP entre dans sa zone de couverture. Il n'y a pas de mécanisme d'authentification de l'antenne. Une fausse antenne peut donc facilement intercepter les messages SMS ou SMM. | C | ✓ **P12 :** Utiliser des applications qui sécurisent l'envoi des messages<br>✓ **P13 :** Désactiver les services SMS et SMM s'ils ne sont pas requis par l'organisation<br>✓ **P41 :** Éviter de communiquer des données sensibles au moyen des services SMS et SMM |
| 2. Consultation non autorisée des messages SMS ou SMM | ✓ L'usage des messages SMS et SMM pour l'envoi d'information critique | | ✓ **P3 :** Désactiver l'affichage des messages de notification lorsque l'ANP est verrouillé<br>✓ **P22 :** Effacer les messages SMS ou SMM sensibles lorsqu'ils ont été lus<br>✓ **P41 :** Éviter de communiquer des données sensibles au moyen des services SMS et SMM |
| 3. Exposition à des logiciels malicieux | ✓ Possibilité de transférer des logiciels malicieux par SMM<br>✓ Absence d'antivirus à jour sur l'ANP | D, I et C | ✓ **P13 :** Désactiver les services SMS et SMM s'ils ne sont pas requis par l'organisation<br>✓ **P15 :** Installer un antivirus sur l'ANP |

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| 4. Divulgation d'information sensible par SMS ou SMM | ✓ Maladresse de l'utilisateur | C | ✓ **P12 :** Utiliser des applications qui sécurisent l'envoi des messages<br>✓ **P13 :** Désactiver les services SMS et SMM s'ils ne sont pas requis par l'organisation<br>✓ **P41 :** Éviter de communiquer des données sensibles au moyen des services SMS et SMM |

## 5.4. Courrier électronique

La plupart des ANP ont accès à Internet, ce qui leur permet d'envoyer et de recevoir du courrier électronique[24] peu importe où ils se trouvent. Les courriels peuvent être envoyés grâce à des applications de service de messagerie d'entreprise (p. ex. Lotus Notes, Outlook, GroupWise, etc.) ou des applications de messagerie externe (p. ex. Gmail, Outlook, Yahoo, etc.).

Ce moyen de communication efficace constitue toutefois une cible de choix pour les cybercriminels qui pourraient intercepter les échanges d'information ou infecter l'ANP par l'envoi d'un courriel contenant un logiciel malicieux.

### 5.4.1. Risques

1. **Interception des données transmises par courriel –** Les courriels et les pièces jointes peuvent être interceptés et consultés par une tierce personne non autorisée. Cela est possible, notamment, en utilisant des outils gratuits d'administration de réseau qui permettent d'intercepter toute information qui circule dans le réseau et de la lire si elle n'est pas chiffrée. Un faux point d'accès peut également être utilisé pour intercepter les courriels des utilisateurs qui s'y connectent.
2. **Consultation non autorisée des messages –** En cas d'intrusion dans le système de l'ANP, ou lorsque l'ANP est laissé déverrouillé sans surveillance, les courriels peuvent être consultés, de même que la date et l'heure de leur envoi ou de leur réception et les noms des destinataires. La lecture d'un message critique peut avoir des conséquences graves pour l'utilisateur, pour l'organisation ou pour les destinataires concernés.

**24**. Rappelons que les courriers électroniques constituent des documents au sens de la Loi concernant le cadre juridique des technologies de l'information.

3. **Exposition à des logiciels malicieux –** Les logiciels malicieux peuvent être envoyés par courriel. Ils se présentent généralement sous la forme d'un lien hypertexte ou d'un logiciel à installer en pièce jointe. L'infection par un logiciel malicieux peut compromettre la disponibilité, l'intégrité et la confidentialité des données qui sont stockées dans l'ANP.

4. **Divulgation d'information sensible par courriel –** Comme moyen de communication accessible sur plusieurs plateformes (ANP, ordinateur, etc.), le courriel est souvent privilégié pour envoyer des messages de tout genre. Un utilisateur peut ainsi envoyer de l'information sensible par inadvertance dans un courriel banal ou se tromper de destinataire.

### 5.4.2. Pratiques recommandées

**P3 :** **Désactiver l'affichage des messages de notification lorsque l'ANP est verrouillé –** Certaines applications envoient des messages de notification d'événements à l'utilisateur, qui peuvent revêtir un caractère confidentiel. Ces messages sont signalés au moyen d'un son, d'une vibration ou d'un message d'alerte, et ce, même si l'appareil est verrouillé (p. ex. nouveau courriel ou message texte entrant, approche d'un événement planifié dans le calendrier, etc.). La non-désactivation de cette fonction permet à une personne malintentionnée de consulter des alertes privées sans avoir à déverrouiller l'ANP.

**P15 :** **Installer un antivirus sur l'ANP – L'installation** d'un antivirus sur l'ANP peut aider à éliminer certains logiciels malicieux installés par mégarde. Par ailleurs, sa mise à jour périodique est essentielle pour maintenir un niveau élevé de sécurité sur l'ANP.

**P17 :** **Utiliser un serveur de courriels sécurisé –** Mettre en place et utiliser un serveur de courriels sécurisé pour les communications des utilisateurs d'ANP. Sensibiliser l'utilisateur au fait qu'il ne doit pas employer les serveurs de courriels grand public (p. ex. Gmail, Outlook, Yahoo, etc.) pour envoyer des courriels associés à son travail, car l'organisation n'a pas la maîtrise de ces serveurs.

**P36 :** **Chiffrer les courriels si l'option est disponible –** Si le chiffrement des courriels est possible, l'activation de cette option permet d'assurer la confidentialité des messages envoyés. Le chiffrement des courriels doit être fait à l'aide d'un algorithme dont la robustesse est éprouvée.

**P37 :** **Mettre un avis de confidentialité en signature aux courriels envoyés –** L'avis de confidentialité est utile notamment lorsqu'un courriel est envoyé à un mauvais destinataire. L'avis le prévient, entre autres, de supprimer le courriel reçu si ce dernier ne lui est pas destiné et d'en avertir l'expéditeur.

**P38 :** **Respecter les règles régissant les échanges par courriel –** L'organisme public doit se conformer à la Directive sur l'utilisation éthique du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique. Ce document est disponible à l'adresse suivante : http://www.rpg.tresor.qc/pdf/1-1-1-5.pdf.

**P39 :** **Vérifier la crédibilité du courriel et des pièces jointes –** Les cybercriminels ont souvent recours à l'hameçonnage ou au piratage psychologique par courriel pour soutirer de l'information sensible ou pour infecter l'ANP avec un logiciel malicieux. Ces courriels sont souvent douteux et illogiques et ils mettent l'utilisateur dans des situations inhabituelles ou inconfortables. La pièce

jointe peut également être un code malicieux qui s'exécute dès son ouverture. Une vérification de l'authenticité de ces courriels est de mise pour éviter des incidents désastreux.

**P40 : Éviter de communiquer des données sensibles par courriel –** Étant donné les risques de divulgation d'information par inadvertance, par hameçonnage, par piratage psychologique ou par tout autre moyen, il est essentiel, dans la mesure du possible, de limiter la communication de données sensibles par courriel.

### 5.4.3. Tableau récapitulatif

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| 1. Interception des données transmises par courriel | ✓ Réseau non sécurisé<br>✓ Communications non chiffrées | C | ✓ **P17 :** Utiliser un serveur de courriels sécurisé<br>✓ **P36 :** Chiffrer les courriels si l'option est disponible<br>✓ **P40 :** Éviter de communiquer des données sensibles par courriel |
| 2. Consultation non autorisée des messages | ✓ L'usage des courriels pour envoyer des messages sensibles | C | ✓ **P3 :** Désactiver l'affichage des messages de notification lorsque l'ANP est verrouillé<br>✓ **P37 :** Mettre un avis de confidentialité en signature aux courriels envoyés<br>✓ **P38 :** Respecter les règles régissant les échanges par courriel<br>✓ **P40 :** Éviter de communiquer des données sensibles par courriel |
| 3. Exposition à des logiciels malicieux | ✓ Possibilité de transférer des logiciels malicieux par courriel<br>✓ Absence d'antivirus à jour sur l'ANP | D, I et C | ✓ **P15 :** Installer un antivirus sur l'ANP<br>✓ **P39 :** Vérifier la crédibilité du courriel et des pièces jointes<br>✓ **P40 :** Éviter de communiquer des données sensibles par courriel |
| 4. Divulgation d'information | ✓ Maladresse de l'utilisateur | C | ✓ **P37 :** Mettre un avis de confidentialité en signature aux courriels envoyés |

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| sensible par courriel | | | ✓ **P38 :** Respecter les règles régissant les échanges par courriel<br>✓ **P40 :** Éviter de communiquer des données sensibles par courriel |

## 5.5. Synchronisation des données sur des périphériques externes

Dans certains cas d'utilisation d'un ANP, une application centrale de communication est installée sur l'ordinateur de l'utilisateur ou sur le serveur de l'organisation. Par l'intermédiaire d'une liaison de données (câble ou sans fil), elle assure la synchronisation avec l'ANP. Certains ANP permettent de faire la synchronisation sans application de communication.

Dans le contexte de l'ANP, la synchronisation est l'opération qui consiste à mettre à jour les données de l'ordinateur personnel ou du serveur à partir de celles de l'ANP ou, à l'inverse, à transférer les versions de documents mis à jour sur l'ordinateur ou sur le serveur vers l'ANP[25].

Advenant la perte, le vol ou la défaillance de l'ANP, la synchronisation constitue une pratique à même d'assurer la disponibilité de l'information.

La synchronisation est généralement faite par câble en connectant l'ANP à l'ordinateur. En ce qui a trait à la synchronisation sans fil, elle est pratique, mais elle offre aux attaquants l'occasion d'intercepter et d'accéder aux données stockées sur l'ANP et, par extension, à celles stockées sur les périphériques qui lui sont connectés.

### 5.5.1. Risques

1. **Interception des données lors d'une synchronisation sans fil –** La synchronisation effectuée à l'aide d'une connexion sans fil expose l'utilisateur au risque d'interception des données par une personne non autorisée.
2. **Installation d'un logiciel malicieux lors d'une synchronisation –** Lors de la synchronisation, un programme malveillant implanté sur le poste de travail de l'utilisateur ou sur le serveur de l'organisation pourrait être transféré sur l'ANP, ou inversement, et causer des dommages. Certains câbles non homologués servant à synchroniser les données peuvent également contenir un programme malicieux qui s'installe sur l'ordinateur ou sur l'ANP au moment de son utilisation.

**25**. Adaptation de la définition tirée du *Grand dictionnaire terminologique* pour le mot « synchronisation ».

3. **Indisponibilité de l'information par manque de synchronisation –** En plus de mettre à jour les données et les applications de l'ANP, la synchronisation sert également à sauvegarder le contenu de l'appareil à un instant donné. Un oubli, un manque de synchronisation ou une synchronisation selon un intervalle trop long expose l'utilisateur à un risque d'indisponibilité de l'information si les données de l'ANP sont corrompues ou si l'appareil est endommagé, perdu ou volé.

### 5.5.2. Pratiques recommandées

**P8 :** **Chiffrer les données sensibles –** Chiffrer les données sensibles stockées sur l'ANP. Cette mesure permet de préserver la confidentialité de l'information en cas d'interception ou d'extraction des données par une personne malintentionnée. Le chiffrement des données doit être fait à l'aide d'un algorithme dont la robustesse est éprouvée.

**P24 :** **Privilégier la synchronisation par câble –** La synchronisation par câble est plus sécuritaire que la synchronisation sans fil, car les données transférées ne peuvent pas être interceptées à distance.

**P25 :** **Utiliser les équipements homologués pour la synchronisation ou la recharge de l'ANP –** Certains câbles non homologués de recharge de l'ANP et de synchronisation des données peuvent contenir des logiciels malicieux qui sont transférés au poste de travail ou à l'ANP lors de leur utilisation. Pour éviter cette situation, l'usage des équipements homologués est recommandé.

**P14 :** **Installer un antivirus sur le poste de travail et le serveur de l'organisation –** L'installation d'un antivirus sur le poste de travail et le serveur de l'organisation de même que sa mise à jour périodique permettent de réduire les risques de transmission de logiciels malicieux à l'ANP.

**P15 :** **Installer un antivirus sur l'ANP – L'installation** d'un antivirus sur l'ANP peut aider à éliminer certains logiciels malicieux installés par mégarde. Par ailleurs, sa mise à jour périodique est essentielle pour maintenir un niveau élevé de sécurité sur l'ANP.

**P19 :** **Planifier la synchronisation des données sur une base régulière –** La synchronisation des données doit être exécutée de façon régulière pour conserver une copie de sécurité qui pourra être récupérée en cas d'incident. L'intervalle entre deux synchronisations peut être raccourci, particulièrement dans le cas où le niveau de confidentialité des données est élevé.

**P35 :** **Chiffrer les données sensibles stockées sur la carte mémoire amovible –** Cette mesure permet de préserver la confidentialité de l'information des données contenues dans la carte mémoire amovible insérée dans l'ANP. Le chiffrement des données doit être fait à l'aide d'un algorithme dont la robustesse est éprouvée.

**P50 :** **Synchroniser l'ANP avec un terminal fiable –** Certains postes de travail non connus de l'ANP et que ne maîtrise pas l'utilisateur peuvent contenir des logiciels malicieux qui sont transférés à l'ANP à l'occasion de la synchronisation.

**P63 :** **Sauvegarder les données sensibles avant leur suppression de l'ANP – Toute** information sensible et importante pour la mission de l'organisation doit être transférée à l'ordinateur personnel de l'utilisateur ou au serveur de l'organisation avant d'être supprimée.

### 5.5.3. Tableau récapitulatif

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| 1. Interception des données lors d'une synchronisation sans fil | ✓ Les données interceptées ne sont pas toujours chiffrées | C | ✓ **P8 :** Chiffrer les données sensibles<br>✓ **P24 :** Privilégier la synchronisation par câble<br>✓ **P35 :** Chiffrer les données sensibles stockées sur la carte mémoire amovible |
| 2. Installation d'un logiciel malicieux lors d'une synchronisation | ✓ Des logiciels malicieux implantés dans des câbles de synchronisation<br>✓ La synchronisation peut entraîner l'installation de logiciels malicieux entre les appareils | D, C et I | ✓ **P14 :** Installer un antivirus sur le poste de travail et le serveur de l'organisation<br>✓ **P15 :** Installer un antivirus sur l'ANP<br>✓ **P25 :** Utiliser les équipements homologués pour la synchronisation<br>✓ **P50 :** Synchroniser l'ANP avec un terminal de confiance |
| 3. Indisponibilité de l'information par manque de synchronisation | ✓ Planification déficiente ou absente des périodes de synchronisation des données | D | ✓ **P19 :** Planifier la synchronisation des données sur une base régulière<br>✓ **P63 :** Sauvegarder les données sensibles avant leur suppression de l'ANP |

## 5.6. Enregistrement sonore ou visuel

Plusieurs modèles d'ANP disposent de fonctions intégrées d'enregistrement sonore et visuel de l'information en format numérique. Les sons, images et vidéos peuvent être enregistrés par la simple pression d'un bouton mettant en fonction des capteurs vidéo et des microphones sensibles. L'utilisation de ces fonctionnalités peut constituer un risque d'atteinte à la confidentialité de l'information si les données enregistrées sont de nature sensible (p. ex. conversation privée, photo ou vidéo compromettante, etc.).

### 5.6.1. Risques

1. **Atteinte à la confidentialité de l'information –** Les ANP contiennent des microphones sensibles qui peuvent enregistrer le bruit ambiant et les conversations distantes. Des conversations

confidentielles peuvent donc être enregistrées et sauvegardées. Ainsi, il est possible que l'utilisateur enregistre lui-même de l'information confidentielle sur son ANP ou que sa conversation (audio ou vidéo) soit enregistrée à son insu par une tierce personne. Les documents papier, les écrans d'ordinateur, les notes collées au mur et toute autre information de nature confidentielle peuvent également être pris en photo ou capturés sous format vidéo par une personne malintentionnée. Dans tous les cas, la confidentialité de l'information peut être compromise.

2. **Atteinte à la vie privée pouvant mener à des poursuites judiciaires –** Les fonctions d'enregistrement sonore ou visuel peuvent poser un problème d'atteinte à la vie privée si des conversations, des photos ou des enregistrements vidéo sont captés sans le consentement des personnes concernées. Cela peut mener à des poursuites à l'encontre de l'utilisateur de l'ANP et de l'organisation qui le lui a fourni.

### 5.6.2. Pratiques recommandées

**P18 :** **Restreindre l'utilisation de la fonction d'enregistrement sonore ou visuel –** Des restrictions adaptées au contexte organisationnel doivent être établies quant à l'activation des fonctionnalités multimédias comme la prise de photos, de vidéos ou d'enregistrements sonores à l'intérieur de l'organisation.

**P42 :** **Interdire l'enregistrement de données multimédias confidentielles sur l'ANP** – Les données telles que des photos, des vidéos et des sons de nature confidentielle (p. ex. photo d'une page d'un rapport, enregistrement d'une conversation téléphonique, etc.) ne doivent pas être enregistrées sur l'ANP pour ne pas porter atteinte à la confidentialité de l'information ou à la vie privée des personnes concernées.

**P43 :** **Interdire les ANP à proximité des zones d'échange d'information sensible –** Pour assurer la confidentialité des conversations, des présentations visuelles ou des réunions, l'ANP ne doit pas être autorisé dans les zones d'échange d'information sensible. Dans le cas contraire, les personnes présentes doivent au moins être avisées que leurs discussions ou présentations peuvent être enregistrées. Il est à noter que la mise hors tension de l'ANP n'est pas suffisante, car certains logiciels espions peuvent activer le microphone de l'ANP même si l'appareil est éteint.

### 5.6.3. Tableau récapitulatif

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| 1. Atteinte à la confidentialité de l'information | ✓ Les fonctions d'enregistrement sonore et visuel peuvent être utilisées | C | ✓ **P18 :** Restreindre l'utilisation de la fonction d'enregistrement sonore ou visuel |

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| | en toute discrétion à l'insu de tous | | ✓ **P42 :** Interdire l'enregistrement des données multimédias confidentielles sur l'ANP<br>✓ **P43 :** Interdire ou mettre hors tension les ANP à proximité des zones d'échange d'information sensible |
| 2. Atteinte à la vie privée pouvant mener à des poursuites judiciaires | ✓ Absence de règles strictes pour restreindre l'utilisation des fonctions d'enregistrement sonore et visuel<br>✓ Enregistrement de l'information sans le consentement des participants | C | ✓ **P18 :** Restreindre l'utilisation de la fonction d'enregistrement sonore ou visuel<br>✓ **P42 :** Interdire l'enregistrement des données multimédias confidentielles sur l'ANP<br>✓ **P43 :** Interdire ou mettre hors tension les ANP à proximité des zones d'échange d'information sensible |

## 5.7. Contrôle des accès

L'accès à l'information enregistrée sur un ANP est régi par les fonctionnalités de contrôle d'accès intégrées dans l'appareil ou gérées à distance par l'organisation. Le contrôle d'accès est généralement assuré par un mot de passe composé de lettres, de chiffres et de symboles ou un numéro d'identification personnel (NIP) composé uniquement de chiffres. Certains ANP intègrent également d'autres mécanismes de contrôle d'accès tels que le déverrouillage par symbole (traçage d'un schéma en reliant des points), l'empreinte digitale, la reconnaissance faciale et la reconnaissance oculaire.

En plus de stocker de l'information sensible, l'ANP peut également servir de jeton d'authentification[26] à l'aide d'une application qui génère automatiquement un code unique toutes les 1 ou 2 minutes. La combinaison de ce code et de l'authentification par nom d'usager et mot de passe constitue un mécanisme d'authentification forte à deux facteurs. Un tel mécanisme est généralement employé pour obtenir l'accès à distance au réseau de l'organisation.

Non seulement l'accès non autorisé à l'ANP constitue un risque pour l'information qui y est stockée, mais il met également en danger celle qui se trouve sur le réseau de l'organisation.

**26. Jeton d'authentification :** Dispositif électronique que l'on transporte avec soi et qui sert à produire des codes ou des mots de passe à partir desquels l'appareil qui les reçoit peut reconnaître l'identité de la personne qui désire obtenir l'accès à un réseau, à un système ou à un ordinateur. *[OQLF - Grand dictionnaire terminologique]*

### 5.7.1. Risques

1. **Accès non autorisé à l'ANP –** Un ANP qui n'intègre aucun mécanisme de contrôle d'accès ou qui intègre un mécanisme déficient est une cible parfaite pour une personne malintentionnée qui voudrait y accéder. Elle aurait alors accès au contenu local de l'appareil (contacts, calendrier, courriels, documents, etc.), mais aussi aux données du réseau de l'organisation.
2. **Modification ou suppression d'information contenue dans l'ANP –** Un accès non autorisé à l'ANP, même de courte durée, permet à l'attaquant de modifier ou de supprimer des données sensibles stockées sur l'appareil ou sur le réseau de l'organisation. Cette personne peut également installer des logiciels malicieux à l'insu de l'utilisateur.
3. **Usurpation d'identité –** Une personne qui brise le mécanisme d'accès de l'ANP peut usurper l'identité de l'utilisateur pour commettre d'autres attaques (p. ex. envoyer des courriels ou des messages textes indésirables au nom de l'utilisateur, appeler un contact avec une fausse identité, utiliser le profil de l'utilisateur pour accéder au réseau de l'organisation, etc.).

### 5.7.2. Pratiques recommandées

**P1 :** **Désactiver l'ANP après un nombre déterminé de tentatives d'accès infructueuses –** Configurer un temps d'attente de plus en plus long à chaque tentative d'accès à l'appareil. Activer le blocage ou la désactivation automatique de l'ANP après plusieurs tentatives d'accès infructueuses (établir un nombre optimal d'essais, par exemple cinq). Cette mesure permet d'empêcher des attaques informatiques visant à connaître le mot de passe de l'ANP pour accéder à son contenu.

**P5 :** **Changer régulièrement le mot de passe pour accéder au contenu de l'ANP –** Planifier un changement périodique du mot de passe. Si le système le permet, l'utilisateur peut être forcé d'effectuer ce changement. Dans le cas contraire, des rappels peuvent être envoyés aux utilisateurs pour qu'ils appliquent cette mesure.

**P7 :** **Utiliser un mécanisme de contrôle d'accès robuste –** Utiliser un mécanisme qui exige un mot de passe fort constitué de chiffres, de lettres et de symboles pour assurer la protection des données sensibles. Dans le cas où la sensibilité de l'information est faible et où le risque peut être acceptable, l'utilisation d'un code NIP (généralement composé de quatre chiffres) peut être suffisante dès lors que la pratique recommandée P1 est appliquée.

Il est à noter que le déverrouillage par symbole (points à relier) n'est pas recommandé en raison de l'insuffisance de sa richesse combinatoire. Le déverrouillage par reconnaissance faciale, quant à lui, n'est pas encore au point, puisqu'il peut, dans certains cas, être contourné en utilisant une photo de l'utilisateur. Le contrôle d'accès par empreinte digitale ou par reconnaissance oculaire est également à proscrire car, contrairement à un mot de passe, il est impossible de modifier une empreinte biométrique lorsqu'elle a été piratée.

**P29 :** **Sensibiliser les utilisateurs d'ANP et les former –** Mettre en œuvre des plans de formation et de sensibilisation périodiques destinés aux utilisateurs d'ANP pour, d'une part, les informer

des risques de sécurité de l'information liés à l'utilisation d'un ANP et, d'autre part, leur présenter la directive ministérielle et les mesures de sécurité établies par l'OP à cet égard.

### 5.7.3. Tableau récapitulatif

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| 1. Accès non autorisé à l'ANP | ✓ Absence de mécanisme de contrôle d'accès | C | ✓ **P1 :** Désactiver l'ANP après un nombre défini de tentatives d'accès infructueuses<br>✓ **P7 :** Utiliser un mécanisme de contrôle d'accès robuste |
| 2. Modification ou suppression d'information contenue dans l'ANP | ✓ Faiblesse du mécanisme de contrôle d'accès | I et D | ✓ **P5 :** Changer régulièrement le mot de passe pour accéder au contenu de l'ANP<br>✓ **P7 :** Utiliser un mécanisme de contrôle d'accès robuste |
| 3. Usurpation d'identité | ✓ Faiblesse du mécanisme de contrôle d'accès<br>✓ Faiblesse du mot de passe | C et I | ✓ **P1 :** Désactiver l'ANP après un nombre défini de tentatives d'accès infructueuses<br>✓ **P7 :** Utiliser un mécanisme de contrôle d'accès robuste<br>✓ **P29 :** Sensibiliser les utilisateurs d'ANP et les former |

## 5.8. Stockage d'information

L'ANP permet le stockage d'un grand nombre de données de diverses natures : textes, tableurs, présentations, fichiers PDF et multimédias (images, fichiers audios, vidéos), applications, etc.

La capacité de stockage de l'ANP allant croissant, il est de plus en plus utilisé pour gérer l'information de l'organisation, laquelle peut être de nature confidentielle, d'où le risque d'accès, d'interception ou de divulgation par une personne malveillante.

Certains modèles d'ANP offrent également la possibilité d'ajouter un espace de stockage additionnel à l'aide d'une carte mémoire. L'avènement de l'infonuagique[27] supprime même cette limite de stockage

**27. Infonuagique :** Modèle informatique qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services, évolutifs, adaptables dynamiquement et facturés à l'utilisation. *[OQLF - Grand dictionnaire terminologique]*

de l'ANP en permettant à l'utilisateur de stocker ses données dans des serveurs externes pour pouvoir y accéder en tout temps indépendamment de l'endroit où il se trouve.

### 5.8.1. Risques

1. **Accès non autorisé à de l'information confidentielle –** L'augmentation croissante de la capacité de stockage de l'ANP incite les utilisateurs à y déposer un plus grand nombre de données sensibles, d'où la motivation pour une personne malintentionnée d'y accéder. Certaines applications non vérifiées, installées sur l'ANP, peuvent également accéder à de l'information confidentielle à l'insu de l'utilisateur.
2. **Indisponibilité de l'information stockée dans un serveur externe –** Un OP qui choisit une solution de stockage de données sur des serveurs localisés à l'extérieur de l'organisation (utilisation d'une solution infonuagique, site de relève informatique, etc.) s'expose à des risques d'indisponibilité de l'information, voire d'interruption du service.
3. **Atteinte à la confidentialité de l'information stockée dans un serveur externe –** Un OP qui choisit une solution de stockage de données sur des serveurs localisés à l'extérieur de l'organisation (utilisation d'une solution infonuagique, site de relève informatique, etc.), s'expose à des risques de sécurité de l'information qui peuvent avoir un impact sur la protection des renseignements personnels et la vie privée.
4. **Bris de l'ANP et perte des données –** Étant donné sa taille réduite, l'ANP peut se briser, souvent par inadvertance ou par maladresse, rendant alors indisponible l'information qu'il contient si elle n'est pas sauvegardée et accessible sur un autre support.

### 5.8.2. Pratiques recommandées

**P8 :** **Chiffrer les données sensibles –** Chiffrer les données sensibles stockées sur l'ANP. Cette mesure permet de préserver la confidentialité de l'information en cas d'interception ou d'extraction des données par une personne malintentionnée. Le chiffrement des données doit être fait à l'aide d'un algorithme dont la robustesse est éprouvée.

**P16 :** **Installer uniquement les applications et les services requis pour répondre aux besoins de l'utilisateur –** Les applications et les services installés sur l'ANP doivent être vérifiés et contrôlés périodiquement pour s'assurer qu'ils n'accèdent pas à de l'information critique ou ne la transmettent pas à une tierce personne non autorisée, qu'ils n'installent pas de logiciels malicieux et qu'ils répondent aux critères de sécurité appliqués par l'organisation.

**P35 :** **Chiffrer les données sensibles stockées sur la carte mémoire amovible –** Cette mesure permet de préserver la confidentialité de l'information des données contenues dans la carte mémoire amovible insérée dans l'ANP. Le chiffrement des données doit être fait à l'aide d'un algorithme dont la robustesse est éprouvée.

**P51 :** **Effacer les données sensibles de l'ANP à la fin de leur utilisation –** Lorsqu'une information sensible n'est plus utile, la supprimer de l'ANP élimine le risque qu'elle soit consultée par une personne malveillante.

**P52 :** **Établir des restrictions concernant le stockage d'information – L'ANP ne** doit pas servir de support de stockage pour des mots de passe, des numéros d'identification personnels ou de l'information personnelle ou confidentielle sur son utilisateur.

**P53 :** **Stocker uniquement de l'information utile sur l'ANP –** Stocker seulement les données qui sont utiles au travail lors des déplacements pour ne pas compromettre d'autres données sensibles en cas d'incident.

**P54 :** **Intégrer les clauses de sécurité de l'information et de protection des renseignements personnels dans les ententes et les contrats; celles-ci sont généralement déterminées après une analyse des risques –** Cette mesure a pour objectif d'assurer la sécurité de l'information dans plusieurs cas, notamment : lorsque l'OP fait appel à un prestataire de services public ou privé pour le stockage de l'information à l'extérieur de ses locaux ou à l'extérieur du Canada, pour la gestion des ANP, leur configuration ou pour le soutien technique.

**P62 :** **Effectuer régulièrement la sauvegarde des données contenues dans l'ANP –** Une copie de sécurité de l'ANP doit être faite sur une base régulière. Cette action est généralement prise en charge par l'unité administrative responsable de la gestion de l'ANP. Après un incident (p. ex. perte, vol, bris ou disfonctionnement de l'appareil), les copies de sécurité peuvent être utilisées pour récupérer l'information perdue ou restaurer l'état fonctionnel de l'ANP.

### 5.8.3. Tableau récapitulatif

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| 1. Accès non autorisé à de l'information confidentielle | ✓ L'augmentation croissante de la capacité de stockage de l'ANP incite les utilisateurs à y déposer un grand nombre de données sensibles | C | ✓ **P8 :** Chiffrer les données sensibles<br>✓ **P16 :** Installer uniquement les applications requises pour répondre aux besoins de l'utilisateur<br>✓ **P35 :** Chiffrer les données sensibles stockées sur la carte mémoire amovible<br>✓ **P51 :** Effacer les données sensibles de l'ANP à la fin de leur utilisation<br>✓ **P52 :** Établir de restrictions sur le stockage d'information |

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| | | | ✓ **P53 :** Stocker uniquement de l'information utile sur l'ANP |
| 2. Indisponibilité de l'information stockée dans un serveur externe | ✓ Les serveurs externes sont indépendants de la volonté de l'OP | D | ✓ **P54 :** Intégrer les clauses de sécurité de l'information et de protection des renseignements personnels dans les ententes et les contrats, généralement déterminées après une analyse des risques |
| 3. Atteinte à la confidentialité de l'information stockée dans un serveur externe | ✓ Les serveurs externes sont indépendants de la volonté de l'OP | C | ✓ **P54 :** Intégrer les clauses de sécurité de l'information et de protection des renseignements personnels dans les ententes et les contrats, généralement déterminées après une analyse des risques |
| 4. Bris de l'ANP et perte des données | ✓ Transportabilité<br>✓ Accident ou maladresse de l'utilisateur | D | ✓ **P62 :** Effectuer régulièrement la sauvegarde des données de l'ANP |

## 5.9. Mémoire amovible

Certains ANP offrent la possibilité d'augmenter la capacité de stockage en y ajoutant une carte mémoire amovible. Puisqu'elle est une composante externe à l'ANP, la carte mémoire est utilisée pour sauvegarder des données qui pourront être lues sur plusieurs types d'ANP ou sur tout autre appareil électronique qui la supporte. Tout comme le disque dur de l'ANP, la carte mémoire doit être protégée, puisqu'elle est susceptible de contenir des données sensibles.

### 5.9.1. Risques

1. **Perte ou vol de la carte mémoire –** N'étant pas protégée par un quelconque mécanisme, la carte mémoire peut être enlevée en tout temps. En cas de perte, de vol ou de non-surveillance de l'ANP, même pour une courte durée, la carte mémoire peut être enlevée, mettant ainsi en péril la confidentialité de l'information qu'elle contient.

2. **Bris ou disfonctionnement de la carte mémoire –** Étant donné sa taille réduite, la carte mémoire peut être endommagée ou se briser, souvent par inadvertance ou par maladresse, ce qui rend illisible l'information qu'elle contient. L'information sera alors indisponible si elle n'a pas été sauvegardée et rendue accessible sur un autre support.
3. **Contamination de l'ANP par une carte mémoire contenant un logiciel malicieux –** L'utilisateur peut transporter par inadvertance un logiciel malicieux dans sa carte mémoire et ainsi altérer les données de la carte de même que, par extension, les données de l'ANP, les rendant alors illisibles ou inaccessibles.

### 5.9.2. Pratiques recommandées

**P15 :** **Installer un antivirus sur l'ANP –** L'installation d'un antivirus sur l'ANP peut aider à éliminer certains logiciels malicieux installés par mégarde. Par ailleurs, sa mise à jour périodique est essentielle pour maintenir un niveau élevé de sécurité sur l'ANP.

**P33 :** **Établir des règles relatives à l'utilisation sécuritaire d'une carte mémoire –** Toutes les règles de sécurité concernant le stockage de l'information sur l'ANP s'appliquent également aux cartes mémoire qui peuvent y être connectées.

**P34 :** **Sensibiliser les utilisateurs à la protection et à l'utilisation sécuritaire des cartes mémoire de l'ANP –** La sensibilisation des utilisateurs contribue fortement à la réduction des risques associés à une utilisation inadéquate des cartes mémoire.

**P35 :** **Chiffrer les données sensibles stockées sur la carte mémoire amovible –** Cette mesure permet de préserver la confidentialité de l'information des données contenues dans la carte mémoire amovible insérée dans l'ANP. Le chiffrement des données doit être fait à l'aide d'un algorithme dont la robustesse est éprouvée.

**P55 :** **Garder la carte mémoire dans un endroit sûr pendant les déplacements –** Ne pas placer la carte mémoire d'un ANP dans des endroits à la vue ou à la portée de tous. S'il n'y a aucune raison valable de la sortir, la carte mémoire devrait demeurer à l'intérieur de l'ANP lors des déplacements.

**P56 :** **Éviter de stocker des fichiers douteux sur la carte mémoire –** S'assurer que les fichiers stockés sur la carte mémoire proviennent d'une source fiable. Certains fichiers douteux peuvent contenir des codes malicieux qui nuiront à l'ANP. Ces fichiers peuvent notamment avoir comme extension : *.exe, *.vbs, *.bin, *.com, *.bat, *.pif, etc.

**P61 :** **Effectuer une destruction sécuritaire de l'information emmagasinée sur une carte mémoire** – Une carte mémoire sur laquelle a été sauvegardée de l'information sensible doit faire l'objet d'une destruction sécuritaire de ces données à la fin de leur utilisation. L'OP s'assure ainsi de réduire le risque de récupération de données sensibles. Pour plus d'information sur la destruction sécuritaire des données, se référer à la pratique recommandée PR-055 intitulée « Guide de destruction sécuritaire de l'information ».

### 5.9.3. Tableau récapitulatif

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| 1. Perte ou vol de la carte mémoire | ✓ Transportabilité<br>✓ Étant donné sa taille réduite, la carte mémoire peut facilement être perdue | D et C | ✓ **P33 :** Établir des règles d'utilisation sécuritaire d'une carte mémoire<br>✓ **P34 :** Sensibiliser les utilisateurs à la protection et à l'utilisation sécuritaire des cartes mémoire de l'ANP<br>✓ **P35 :** Chiffrer les données sensibles stockées sur la carte mémoire amovible<br>✓ **P55 :** Garder la carte mémoire dans un endroit sûr pendant les déplacements |
| 2. Bris ou disfonctionnement de la carte mémoire | ✓ Transportabilité<br>✓ Accident ou maladresse de l'utilisateur | D | ✓ **P33 :** Établir des règles d'utilisation sécuritaire d'une carte mémoire<br>✓ **P34 :** Sensibiliser les utilisateurs à la protection et à l'utilisation sécuritaire des cartes mémoire de l'ANP<br>✓ **P61 :** Effectuer la destruction sécuritaire de l'information emmagasinée sur une carte mémoire |
| 3. Contamination de l'ANP par une carte mémoire contenant un logiciel malicieux | ✓ Sauvegarde par inadvertance de logiciels malicieux sur la carte mémoire | C, I et D | ✓ **P15 :** Installer un antivirus sur l'ANP<br>✓ **P33 :** Établir des règles d'utilisation sécuritaire d'une carte mémoire<br>✓ **P34 :** Sensibiliser les utilisateurs à la protection et à l'utilisation sécuritaire des cartes mémoire de l'ANP<br>✓ **P56 :** Éviter de stocker des fichiers douteux sur la carte mémoire |

## 5.10. Exposition aux logiciels malicieux

Les multiples fonctionnalités de l'ANP, sa transportabilité et la diversité des canaux de communication qu'il supporte l'exposent inévitablement aux risques d'infection par un logiciel malicieux et aux actions malveillantes. En effet, avec sa popularité qui ne cesse de croître, l'ANP est devenu une cible de choix pour les cybercriminels.

### 5.10.1. Risques

1. **Infection par un logiciel malicieux et actions malveillantes –** Un logiciel malicieux (p. ex. ver[28], virus[29], cheval de Troie[30], logiciel espion[31], etc.) se propage à l'ANP de façon aussi variée que les fonctionnalités et les modes de communication supportés par l'assistant numérique personnel : propagation par navigation Web, protocole Bluetooth, technologie Wi-Fi, technologie NFC, ouverture d'une pièce jointe à un courriel, installation d'une application malveillante à apparence inoffensive (p. ex. jeu, outil, etc.), connexion à un micro-ordinateur infecté, usage d'une carte à puce infectée, etc.
2. **Indisponibilité de l'information et des applications de l'ANP –** L'exécution d'un code malicieux pourrait corrompre des applications ou des fichiers de l'ANP, le rendant ainsi indisponible. Le code malicieux pourrait également réduire considérablement l'autonomie de l'ANP en exécutant un processus en arrière-plan qui peut consommer une importante quantité de ressources énergétiques.
3. **Atteinte à l'intégrité de l'information et des applications –** Un code malicieux qui s'exécute sur l'ANP peut modifier la configuration de l'appareil ou celle des applications, notamment pour permettre à l'attaquant d'avoir un meilleur accès aux données de l'ANP (p. ex. activation de la connexion Bluetooth). Le code malicieux pourrait également corrompre ou modifier le contenu de certains fichiers stratégiques (p. ex. plans d'action, calendrier des projets, états financiers, etc.).
4. **Perte de confidentialité –** Le code malicieux qui s'exécute sur l'ANP pourrait utiliser la connexion Internet de ce dernier pour transmettre des données à l'attaquant.

---

**28. Ver :** Programme autonome capable de s'exécuter seul dans la mémoire d'un ordinateur, qu'il surcharge et mine progressivement, en consommant jusqu'à la paralysie les ressources du système informatique. *[OQLF - Grand dictionnaire terminologique]*

**29. Virus :** Programme malveillant qui se propage en modifiant d'autres programmes pour y inclure une copie éventuellement modifiée de lui-même, et qui est exécuté quand le programme visé est appelé. *[OQLF - Grand dictionnaire terminologique]*

**30. Cheval de Troie :** Programme malveillant qui, dissimulé à l'intérieur d'un autre programme en apparence inoffensif (par exemple un jeu ou un petit utilitaire), exécute des opérations nuisibles à l'insu de l'utilisateur. *[OQLF - Grand dictionnaire terminologique]*

**31. Logiciel espion :** Tout logiciel qui contient un programme espion et qui emploie en arrière-plan la connexion Internet de l'utilisateur pour recueillir et transmettre, à son insu et sans sa permission, des données personnelles, notamment sur ses intérêts et ses habitudes de navigation, à une régie publicitaire. *[OQLF - Grand dictionnaire terminologique]*

## 5.10.2. Pratiques recommandées

**P10 :** **Activer le pare-feu de l'ANP –** Si l'option est disponible, l'activation du pare-feu permet de bloquer les connexions douteuses que certaines applications pourraient utiliser.

**P14 :** **Installer un antivirus sur le poste de travail et le serveur de l'organisation –** L'installation d'un antivirus sur le poste de travail et le serveur de l'organisation de même que sa mise à jour périodique permettent de réduire les risques de transmission de logiciels malicieux à l'ANP.

**P15 :** **Installer un antivirus sur l'ANP –** L'installation d'un antivirus sur l'ANP peut aider à éliminer certains logiciels malicieux installés par mégarde. Par ailleurs, sa mise à jour périodique est essentielle pour maintenir un niveau élevé de sécurité sur l'ANP.

**P16 :** **Installer uniquement les applications et les services requis pour répondre aux besoins de l'utilisateur –** Les applications et les services installés sur l'ANP doivent être vérifiés et contrôlés périodiquement pour s'assurer qu'ils n'accèdent pas à de l'information critique ou ne la transmettent pas à une tierce personne non autorisée, qu'ils n'installent pas de logiciels malicieux et qu'ils répondent aux critères de sécurité appliqués par l'organisation.

**P29 :** **Sensibiliser les utilisateurs d'ANP et les former –** Mettre en œuvre des plans de formation et de sensibilisation périodiques destinés aux utilisateurs d'ANP pour, d'une part, les informer des risques de sécurité de l'information liés à l'utilisation d'un ANP et, d'autre part, leur présenter la directive ministérielle et les mesures de sécurité établies par l'OP à cet égard.

**P30 :** **Être vigilant en cas de comportement inhabituel de l'ANP –** Certains indicateurs peuvent révéler la présence d'un logiciel malveillant : le fonctionnement de l'ANP ralentit, celui-ci ne répond plus, se fige ou redémarre fréquemment, l'appareil est chaud même si rien ne semble être ouvert, la batterie se vide rapidement, certains fichiers ne sont plus accessibles, etc. Lorsque le doute subsiste, il est judicieux d'avertir l'unité administrative responsable de la gestion de l'ANP pour que le problème soit réglé.

**P60 :** **Maintenir à jour le système d'exploitation de l'ANP et les applications installées –** La mise à jour régulière et automatique du système d'exploitation de l'ANP et de ses applications permet de corriger les éventuelles failles de sécurité de l'appareil, diminuant ainsi les risques d'infection de l'ANP par un code malicieux.

**P62 :** **Effectuer régulièrement la sauvegarde des données contenues dans l'ANP –** Une copie de sécurité de l'ANP doit être faite sur une base régulière. Cette action est généralement prise en charge par l'unité administrative responsable de la gestion de l'ANP. Après un incident (p. ex. perte, vol, bris ou disfonctionnement de l'appareil), les copies de sécurité peuvent être utilisées pour récupérer l'information perdue ou restaurer l'état fonctionnel de l'ANP.

## 5.10.3. Tableau récapitulatif

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| 1. Infection par un logiciel malicieux et actions malveillantes | ✓ La variété des fonctionnalités et des modes de communication de l'ANP l'expose à un grand nombre d'actions malveillantes | D, I et C | ✓ **P10 :** Activer le pare-feu de l'ANP<br>✓ **P14 :** Installer un antivirus sur le poste de travail et le serveur de l'organisation<br>✓ **P15 :** Installer un antivirus sur l'ANP<br>✓ **P16 :** Installer uniquement les applications et les services requis pour répondre aux besoins de l'utilisateur<br>✓ **P29 :** Sensibiliser les utilisateurs d'ANP et les former<br>✓ **P30 :** Être vigilant en cas de comportement inhabituel de l'ANP<br>✓ **P60 :** Maintenir à jour le système d'exploitation de l'ANP et les applications installées<br>✓ **P62 :** Effectuer régulièrement la sauvegarde des données de l'ANP |
| 2. Indisponibilité de l'information et des applications de l'ANP | ✓ La variété des fonctionnalités et des modes de communication de l'ANP l'expose à un grand nombre d'actions malveillantes | D | ✓ **P15 :** Installer un antivirus sur l'ANP<br>✓ **P29 :** Sensibiliser les utilisateurs d'ANP et les former<br>✓ **P30 :** Être vigilant en cas de comportement inhabituel de l'ANP<br>✓ **P60 :** Maintenir à jour le système d'exploitation de l'ANP et les applications installées<br>✓ **P62 :** Effectuer régulièrement la sauvegarde des données de l'ANP |
| 3. Atteinte à l'intégrité de l'information et des applications | ✓ La variété des fonctionnalités et des modes de communication de l'ANP l'expose à un grand nombre d'actions malveillantes | I | ✓ **P15 :** Installer un antivirus sur l'ANP<br>✓ **P16 :** Installer uniquement les applications et les services requis pour répondre aux besoins de l'utilisateur<br>✓ **P29 :** Sensibiliser les utilisateurs d'ANP et les former<br>✓ **P30 :** Être vigilant en cas de comportement inhabituel de l'ANP |

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| | | | ✓ **P60 :** Maintenir à jour le système d'exploitation de l'ANP et les applications installées |
| 4. Perte de confidentialité | ✓ La variété des fonctionnalités et des modes de communication de l'ANP l'expose à un grand nombre d'actions malveillantes | C | ✓ **P15 :** Installer un antivirus sur l'ANP<br>✓ **P29 :** Sensibiliser les utilisateurs d'ANP et les former<br>✓ **P30 :** Être vigilant en cas de comportement inhabituel de l'ANP<br>✓ **P60 :** Maintenir à jour le système d'exploitation de l'ANP et les applications installées |

## 5.11. Configuration de l'ANP

La configuration d'un ANP concerne principalement le paramétrage du système d'exploitation, notamment les fonctions d'activation d'une connexion sans fil (Wi-Fi, Bluetooth, NFC), la gestion des droits d'accès (mot de passe, empreinte digitale, etc.), la synchronisation, l'installation des applications, la réception de courriels (connexion au serveur de messagerie et au compte utilisateur), etc. La configuration peut être faite à distance ou directement sur l'ANP.

### 5.11.1. Risques

1. **Activation par mégarde des paramètres à risque –** La configuration d'un ANP peut le rendre vulnérable sur le plan de la sécurité quand des paramètres à risque sont activés. À titre d'exemple, la fonction d'accès à Internet par connexion Wi-Fi pourrait être activée sans que la connexion réseau ait été préalablement sécurisée. La communication par Bluetooth pourrait aussi être activée sans aucune protection par mot de passe. Un utilisateur pourrait également oublier de désactiver un paramètre après son utilisation, exposant alors l'ANP à des actions malveillantes.
2. **Accès non autorisé en raison d'une mauvaise gestion des restrictions associées aux applications –** Une mauvaise configuration des restrictions pourrait permettre à une application douteuse d'accéder à de l'information sensible à l'insu de l'utilisateur. En effet, certaines applications pourrait vouloir accéder au microphone intégré de l'ANP, à la caméra ou à la liste des contacts, par exemple, même si ces éléments ne sont pas nécessaires à leur fonctionnement. L'utilisateur pourrait autoriser ces accès sans s'en rendre compte et exposer son ANP à des actions malveillantes.
3. **Infection par un logiciel malveillant attribuable à un système désuet –** Un ANP dont le système d'exploitation n'est pas à jour pourrait être fortement vulnérable à de nouvelles attaques lancées par les cybercriminels.

### 5.11.2. Pratiques recommandées

**P16 :** **Installer uniquement les applications et les services requis pour répondre aux besoins de l'utilisateur –** Les applications et les services installés sur l'ANP doivent être vérifiés et contrôlés périodiquement pour s'assurer qu'ils n'accèdent pas à de l'information critique ou ne la transmettent pas à une tierce personne non autorisée, qu'ils n'installent pas de logiciels malicieux et qu'ils répondent aux critères de sécurité appliqués par l'organisation.

**P29 :** **Sensibiliser les utilisateurs d'ANP et les former – Mettre en œuvre** des plans de formation et de sensibilisation périodiques destinés aux utilisateurs d'ANP pour, d'une part, les informer des risques de sécurité de l'information liés à l'utilisation d'un ANP et, d'autre part, leur présenter la directive ministérielle et les mesures de sécurité établies par l'OP à cet égard.

**P58 :** **Centraliser la gestion de la configuration des paramètres de l'ANP –** Dans la mesure du possible, il est recommandé de centraliser la configuration de l'ANP des utilisateurs et non de

laisser celle-ci à leur libre choix. Cette responsabilité doit être assignée au responsable de la gestion et de l'administration des ANP de l'organisation.

**P59 :** **Vérifier périodiquement les permissions accordées aux applications –** Les applications installées sur l'ANP doivent avoir les permissions strictement suffisantes à l'exercice de leurs fonctions (accès aux données, à Internet ou au contrôle des capteurs supportés par l'appareil). Les permissions accordées à une application doivent être vérifiées lors de son installation et à l'occasion de sa mise à jour pour s'assurer que les exigences de sécurité sont toujours respectées.

**P60 :** **Maintenir à jour le système d'exploitation de l'ANP et les applications installées –** La mise à jour régulière et automatique du système d'exploitation de l'ANP et de ses applications permet de corriger les éventuelles failles de sécurité de l'appareil, diminuant ainsi les risques d'infection de l'ANP par un code malicieux. Un ANP qui ne prend plus en charge l'évolution de son système d'exploitation doit être remplacé.

### 5.11.3. Tableau récapitulatif

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| 1. Activation par mégarde des paramètres à risque | ✓ Oubli ou maladresse de l'utilisateur<br>✓ Dans certains cas, les utilisateurs ont accès sans restriction à la configuration de tous les paramètres de l'ANP | C | ✓ **P29 :** Sensibiliser les utilisateurs d'ANP et les former<br>✓ **P58 :** Centraliser la gestion de la configuration des paramètres de l'ANP |
| 2. Accès non autorisé en raison d'une mauvaise gestion des restrictions associées aux applications | ✓ Manque de vérification lors de l'installation de nouvelles applications | C | ✓ **P16 :** Installer uniquement les applications et les services requis pour répondre aux besoins de l'utilisateur<br>✓ **P29 :** Sensibiliser les utilisateurs d'ANP et les former<br>✓ **P59 :** Vérifier périodiquement les permissions accordées aux applications |
| 3. Infection par un logiciel | ✓ Le modèle de l'ANP est désuet | D, I et C | ✓ **P16 :** Installer uniquement les applications et les services requis |

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| malveillant attribuable à un système désuet | ✓ Le système d'exploitation installé dans l'ANP ne répond plus aux exigences de sécurité actuelles | | pour répondre aux besoins de l'utilisateur<br>✓ **P29 :** Sensibiliser les utilisateurs d'ANP et les former<br>✓ **P60 :** Maintenir à jour le système d'exploitation de l'ANP et les applications installées |

## 5.12. Administration à distance de l'ANP

Certains ANP possèdent des fonctions permettant de les commander à distance grâce à une connexion sans fil. À son tour, un ANP peut, grâce à un logiciel d'administration à distance, commander un autre périphérique tel un poste de travail ou un serveur de l'organisation.

### 5.12.1. Risques

1. **Accès à distance non autorisé aux données de l'ANP** – La fonctionnalité d'administration à distance de l'ANP permet à un administrateur de réseau ou à l'équipe de soutien technique de l'organisation de le commander à distance. Or, l'administration à distance par une personne malveillante mettra en péril aussi bien l'information consignée sur l'ANP que celle accessible par l'entremise du réseau de l'organisation.
2. **Accès à distance non autorisé aux données de l'organisation** – L'accès aux fonctionnalités d'administration à distance à partir de l'ANP permet à un utilisateur ou à un administrateur de réseau de commander à distance un système implanté dans le réseau de l'organisation. Une telle connexion peut constituer une brèche si elle est établie par une personne malveillante en cas de vol ou de perte d'un ANP. Une fois en possession de l'appareil, cette personne pourrait avoir accès au réseau de l'organisation.
3. **Interception des données** – En utilisant les fonctionnalités d'administration à distance à partir de son ANP, l'utilisateur autorisé établit une connexion avec les postes et les serveurs de l'organisation. Les échanges d'information peuvent alors être interceptés si la connexion n'est pas entièrement sécurisée.

## 5.12.2. Pratiques recommandées

### P11 : Permettre à l'utilisateur d'autoriser la prise en charge à distance de son ANP

Mettre en place un système permettant à l'utilisateur de l'ANP d'accepter ou de refuser chaque demande de prise en charge de son ANP par l'équipe de soutien technique de l'organisation. L'équipe technique doit idéalement communiquer avec l'utilisateur pour le prévenir que son appareil fera l'objet d'une telle prise en charge.

### P23 : Utiliser un réseau privé virtuel (RPV) pour accéder à distance au réseau de l'organisation

Lors d'une connexion à un point d'accès sans fil en dehors des locaux de l'organisation, il est recommandé d'utiliser le réseau privé virtuel pour tout accès au réseau de l'organisation. La connexion doit être sécurisée par un identifiant et un mot de passe robuste. Le RPV (ou VPN en anglais) permet de créer une connexion directe et chiffrée entre l'ANP et les serveurs de l'organisation, rendant ainsi les communications sécuritaires.

### P31 : Être vigilant lorsque l'ANP est contrôlé à distance par l'équipe de soutien technique

L'utilisateur doit s'assurer de l'identité du technicien qui contrôle son ANP. Il doit aviser le responsable de la sécurité de l'information de tout comportement inhabituel observé à cet égard.

### P32 : Établir une procédure applicable en cas d'incident et en informer le personnel

Un document qui présente le détail de la procédure peut être remis à l'utilisateur d'un ANP pour l'informer des mesures à prendre en cas d'incident. Ce document indique également les coordonnées des personnes-ressources chargées de l'administration à distance des ANP.

## 5.12.3. Tableau récapitulatif

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| 1. Accès à distance non autorisé aux données de l'ANP | ✓ L'administration à distance de l'ANP peut être faite par une personne malveillante | C | ✓ **P11 :** Permettre à l'utilisateur d'autoriser la prise en charge à distance de son ANP<br>✓ **P31 :** Être vigilant lorsque l'ANP est contrôlé à distance par l'équipe de soutien technique<br>✓ **P32 :** Établir une procédure à appliquer en cas d'incident |
| 2. Accès à distance non autorisé aux | ✓ Faiblesse du mécanisme d'authentification du réseau de l'organisation | C | ✓ **P23 :** Utiliser un réseau privé virtuel (RPV) pour accéder à distance au réseau de l'organisation |
| données de l'organisation | | | ✓ **P32 :** Établir une procédure à appliquer en cas d'incident et en informer le personnel |
| 3. Interception des données | ✓ Utilisation d'une connexion non sécurisée pour l'administration à distance de l'ANP | C | ✓ **P23 :** Utiliser un réseau privé virtuel (RPV) pour accéder à distance au réseau de l'organisation<br>✓ **P32 :** Établir une procédure à appliquer en cas d'incident |

## 5.13. Système de géolocalisation

La plupart des ANP sont munis d'un système de géolocalisation qui permet de les situer en tout temps partout sur la planète. Les données de localisation recueillies par une application peuvent être utilisées pour connaître les habitudes de déplacement de l'utilisateur. Ces données servent ensuite à afficher sur une carte des institutions financières, des stations-service, des restaurants, des boutiques ou tout autre établissement qui se trouve à proximité de l'ANP. Certaines applications utilisent aussi la géolocalisation pour afficher le trafic routier en temps réel ou tout simplement le parcours à suivre pour se rendre à une destination donnée.

Grâce à une précision de l'ordre de quelques mètres (10 m à 200 m), le système de géolocalisation de l'ANP est suffisamment précis pour pister une personne, souvent à son insu, durant une ou plusieurs journées.

### 5.13.1. Risques

1. **Atteinte à la vie privée de l'utilisateur –** Dans un contexte familial, il n'est pas rare qu'un parent installe une application qui utilise le système de géolocalisation de l'ANP pour connaître les moindres déplacements de ses enfants. Cette technique pourrait cependant porter atteinte à la vie privée lorsqu'elle est employée pour connaître les déplacements d'une autre personne (conjoint, conjointe, employés, etc.).
2. **Usages malintentionnés des données de localisation –** Certaines applications pourraient recueillir les données de localisation de l'utilisateur, parfois sans son consentement, et les vendre aux entreprises commerciales. Ces entreprises les utilisent pour constituer des statistiques, notamment pour mieux cibler leur clientèle. Un logiciel malicieux pourrait également, à l'insu de l'utilisateur, transmettre ses données de localisation à une personne malintentionnée qui espionnerait ses déplacements.

### 5.13.2. Pratiques recommandées

**P16 : Installer uniquement les applications et les services requis pour répondre aux besoins de l'utilisateur –** Les applications et les services installés sur l'ANP doivent être vérifiés et contrôlés périodiquement pour s'assurer qu'ils n'accèdent pas à de l'information critique ou ne la transmettent pas à une tierce personne non autorisée, qu'ils n'installent pas de logiciels malicieux et qu'ils répondent aux critères de sécurité appliqués par l'organisation.

**P20 : Interdire l'accès à la géolocalisation pour les applications qui ne requièrent pas ce service –** Si le fonctionnement d'une application ne nécessite pas l'utilisation du service de géolocalisation, il est important d'interdire l'accès à ce service dans les paramètres de l'ANP, si ce n'est pas déjà fait par défaut.

**P21 : Encadrer l'utilisation du système de géolocalisation –** Si l'utilisation du système de géolocalisation de l'ANP peut porter atteinte à la vie privée et à la liberté de déplacement, il n'en demeure pas moins que, lorsque la sécurité des personnes est en jeu, l'OP peut être amené

à appliquer des mesures de surveillance strictes pour assurer la sécurité de ses employés. Ainsi, des règles d'encadrement du service de géolocalisation, proportionnelles aux risques courus, peuvent être appropriées. Il convient, dans ce cas, d'informer les personnes concernées des mesures de surveillance dont elles font l'objet.

### 5.13.3. Tableau récapitulatif

| Risque | Vulnérabilité | Objectif de sécurité (DIC) | Pratique recommandée |
|---|---|---|---|
| 1. Atteinte à la vie privée de l'utilisateur | ✓ Manque de règles claires concernant l'utilisation du système de géolocalisation de l'ANP | C | ✓ **P16 :** Installer uniquement les applications et les services requis pour répondre aux besoins de l'utilisateur<br>✓ **P21 :** Encadrer l'utilisation du système de géolocalisation |
| 2. Usages malintentionnés des données de localisation | ✓ Manque de contrôle quant à l'activation du système de géolocalisation de l'ANP | C | ✓ **P16 :** Installer uniquement les applications et les services requis pour répondre aux besoins de l'utilisateur<br>✓ **P20 :** Interdire l'accès au service de géolocalisation pour les applications qui ne le requièrent pas |

# 6. Conclusion

Les ANP font partie des outils de base essentiels mis à la disposition du personnel d’un grand nombre d’organisations. Leur utilisation constitue un avantage en termes de réduction des coûts et d’augmentation de la productivité. Cependant, leur usage ne convient pas nécessairement à tous les OP étant donné le contexte particulier de chacun, d’où l’importance d’une étude de positionnement préalablement à l’adoption d’une telle solution.

De plus, considérant le niveau de sensibilité de l'information qui peut transiter par l’ANP ou y être stockée, il est essentiel de s’assurer que toutes les mesures de sécurité sont appliquées pour en garantir l'utilisation sécuritaire.

# Annexe I. Sigles et acronymes

## I.1 Sigles et acronymes

1. **ANP** : Assistant numérique personnel
2. **BYOD** : *Bring Your Own Device*
3. **COGI :** Coordonnateur organisationnel de gestion des incidents
4. **COSI :** Conseiller organisationnel en sécurité de l'information
5. **DIC :** Disponibilité, intégrité et confidentialité
6. **DPI :** Dirigeant principal de l'information
7. **IEEE** : *Institute of Electrical and Electronics Engineers* (ou Institut des ingénieurs électriciens et électroniciens)
8. **NFC** : *Near Field Communication* (ou communication en champ proche)
9. **NIP** : Numéro d'identification personnel (ou *Personal identification number – PIN*)
10. **OP :** Organisme public
11. **OQLF :** Office québécois de la langue française
12. **PAP :** Prenez vos appareils personnels
13. **ROSI :** Responsable organisationnel de la sécurité de l'information
14. **RPV** : Réseau privé virtuel *(ou Virtual Private Network – VPN*)
15. **SMM** : Service de messagerie multimédia (ou *Multimedia Message Service - MMS*)
16. **SMS** : Service de messages succincts (*Short Message Service*)
17. **SSID :** *Service Set Identifier est le nom du réseau sans fil*
18. **WEP :** *Wired Equivalent Privacy*
19. **Wi-Fi :** *Wireless Fidelity*
20. **WLAN :** Réseau local sans fil (*Wireless Local Area Network*)
21. **WPA2 :** *Wi-Fi Protected Access 2*

**22. WPAN :** Réseau personnel sans fil (ou *Wireless Personal Area Network*)

## I.2 Définitions

1. **Agenda électronique :** Logiciel de gestion du temps qui facilite la planification horaire, quotidienne ou à plus long terme, de l'utilisateur. *[OQLF - Grand dictionnaire terminologique]*

2. **Appareil mobile :** Appareil informatique que l'on peut transporter avec soi et qui possède l'énergie électrique nécessaire pour fonctionner de manière autonome. *[OQLF - Grand dictionnaire terminologique]*

3. **Catégorisation :** Processus permettant de déterminer le niveau de criticité des actifs informationnels, compte tenu de l'impact que peut engendrer un bris de disponibilité, d'intégrité ou de confidentialité de ces actifs sur l'organisme et sa clientèle ou sur d'autres organismes.

4. **Cheval de Troie :** Programme malveillant qui, dissimulé à l'intérieur d'un autre programme en apparence inoffensif (par exemple un jeu ou un petit utilitaire), exécute des opérations nuisibles à l'insu de l'utilisateur. *[OQLF - Grand dictionnaire terminologique]*

5. **Chiffrement :** Opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possédant pas la clé permettant de le ramener à sa forme initiale. Synonyme : **cryptage** *[OQLF - Grand dictionnaire terminologique]*

6. **Confidentialité :** Propriété d'une information de n'être accessible qu'aux personnes autorisées. *[Directive sur la sécurité de l'information gouvernementale]*

7. **Destruction sécuritaire de l'information :** Processus permettant d'effacer ou de détruire l'information emmagasinée sur un équipement, un dispositif ou sur tout autre support de données de façon à réduire le risque de récupération ou de reconstitution.

8. **Disponibilité :** Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée. *[Directive sur la sécurité de l'information gouvernementale]*

9. **Géolocalisation :** Ensemble des techniques qui permettent, dans le contexte de l'utilisation d'appareils mobiles, comme les téléphones cellulaires, de déterminer leur position géographique à partir des ondes radio qu'ils émettent. *[OQLF - Grand dictionnaire terminologique]*

10. **Hameçonnage :** Technique de fraude visant à obtenir des informations confidentielles au moyen de messages ou de sites usurpant l'identité d'une tierce personne. *[OQLF - Grand dictionnaire terminologique]*

11. **Infonuagique :** Modèle informatique qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services, évolutifs, adaptables dynamiquement et facturés à l'utilisation. *[OQLF - Grand dictionnaire terminologique]*

12. **Intégrité :** Propriété d'une information de ne pas être détruite ou altérée de quelque façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues. *[Directive sur la sécurité de l'information gouvernementale]*

13. **Jeton d'authentification :** Dispositif électronique que l'on transporte avec soi et qui sert à produire des codes ou des mots de passe à partir desquels l'appareil qui les reçoit peut reconnaître l'identité de la personne qui désire obtenir l'accès à un réseau, à un système ou à un ordinateur. *[OQLF - Grand dictionnaire terminologique]*

14. **Logiciel espion :** Tout logiciel qui contient un programme espion et qui emploie en arrière-plan la connexion Internet de l'utilisateur pour recueillir et transmettre, à son insu et sans sa permission, des données personnelles, notamment sur ses intérêts et ses habitudes de navigation, à une régie publicitaire. *[OQLF - Grand dictionnaire terminologique]*

15. **Micro-ordinateur :** Ordinateur de dimension réduite dont l'unité centrale est constituée d'un ou plusieurs microprocesseurs. *[OQLF - Grand dictionnaire terminologique]*

16. **Organiseur :** Petit ordinateur de poche capable de mémoriser et de gérer des informations utiles. *[OQLF - Grand dictionnaire terminologique]*

17. **Piratage psychologique ou fraude psychologique :** Tromperie qui résulte d'échanges entre individus afin d'extorquer des informations dans le but de pénétrer frauduleusement un système. La désignation « ingénierie sociale » constitue un calque de l'anglais. *[OQLF - Grand dictionnaire terminologique]*

18. **Réseau sans fil :** Réseau qui permet de relier sans fil, c'est-à-dire par des liaisons radioélectriques ou des liaisons infrarouges, les appareils informatiques d'un groupe de personnes qui doivent communiquer entre elles. *[OQLF - Grand dictionnaire terminologique]*

19. **Réseau privé virtuel (RPV) :** Réseau de communication privé qui peut se servir de l'infrastructure d'un réseau public pour transmettre des données qui sont protégées grâce à l'utilisation de techniques de chiffrement ou d'encapsulation. Terme anglais : **VPN** (*Virtual Private Network*) *[OQLF - Grand dictionnaire terminologique]*

20. **Risque :** De manière générale, sans être nécessairement appliqué au domaine de la sécurité de l'information, un risque est une probabilité d'apparition d'une menace qui, face à l'exploitabilité d'une vulnérabilité, peut potentiellement entraîner un impact sur un actif informationnel (actif ou information). *[Source : Norme ISO/IEC 27005]*

21. **Téléphone-tablette (phablette) :** Appareil hybride qui combine un téléphone intelligent et une tablette électronique. Le téléphone-tablette possède un écran assez grand pour permettre la lecture de caractères tout en pouvant tenir dans une seule main. *[OQLF - Grand dictionnaire terminologique]*

22. **Temps de latence :** En termes de transfert de données, le temps de latence est le délai qui s'écoule entre l'envoi des données et leur réception.

23. **Terminal sans fil :** Appareil informatique ou de télécommunication qu'on peut transporter avec soi dans ses déplacements et utiliser comme terminal donnant accès sans fil à un ou à plusieurs réseaux. *[OQLF - Grand dictionnaire terminologique]*

24. **Ver :** Programme autonome capable de s'exécuter seul dans la mémoire d'un ordinateur, qu'il surcharge et mine progressivement, en consommant jusqu'à la paralysie les ressources du système informatique. *[OQLF - Grand dictionnaire terminologique]*

25. **Virus :** Programme malveillant qui se propage en modifiant d’autres programmes pour y inclure une copie éventuellement modifiée de lui-même, et qui est exécuté quand le programme visé est appelé. *[OQLF - Grand dictionnaire terminologique]*

# Annexe II. Modèle de directive ministérielle

La directive ministérielle sur l'utilisation sécuritaire des ANP permet d'énoncer les objectifs, les principes directeurs, les responsabilités des intervenants et la ligne de conduite de l'organisation et de son personnel relativement à la protection, aux échanges et à la conservation de l'information lors de l'utilisation d'un ANP.

Bien que les éléments du modèle de directive proposé à la présente annexe soient applicables à la plupart des organismes publics, il convient, pour ces derniers, de les adapter à leur organisation respective et aux risques qui leur sont propres.

# Modèle de directive ministérielle concernant l'utilisation sécuritaire des assistants numériques personnels (ANP)

**INTRODUCTION**

Les nombreuses fonctionnalités des assistants numériques personnels (ANP) en font incontestablement un outil pratique pour les organisations. Leur utilisation doit toutefois être encadrée afin d'assurer la protection de l'information qu'ils emmagasinent ou qu'ils traitent étant donné sa nature souvent personnelle, confidentielle ou stratégique.

Pour assurer la continuité de ses services et accroître sa productivité, le …, ci-après nommé le Ministère, permet l'utilisation, par son personnel autorisé, des assistants numériques personnels (téléphones intelligents, tablettes et téléphones-tablettes), ci-après désignés « ANP ».

**DÉFINITIONS**

1. Dans la présente directive, est défini par :

Définition 1 : ……

Définition 2 : ……

Note : Seront retenues dans cette section les définitions que le Ministère jugera pertinentes à la compréhension des dispositions de la présente directive. Il pourra à cet effet s'inspirer de celles proposées à l'Annexe I.

**OBJET**

2. La présente directive énonce les objectifs, les principes directeurs, les responsabilités des intervenants et la ligne de conduite du Ministère et de tout utilisateur d'ANP de ce ministère relativement à la transmission, à la réception et à la conservation de l'information lors de l'utilisation d'un ANP.

**CHAMP D'APPLICATION ET PORTÉE**

3. La présente directive s'applique aux intervenants visés par les articles 7 à 9. Elle concerne trois catégories d'ANP, soit les téléphones intelligents, les tablettes et les téléphones-tablettes (*phablettes*). L'ANP concerné est notamment doté des fonctionnalités d'agenda, de répertoire téléphonique, de gestion des courriels, de création, d'édition et de lecture de fichiers de tout genre tels des fichiers texte, des tableurs, des présentations, des fichiers PDF et des fichiers multimédias. Les fichiers multimédias comprennent notamment les messages vocaux, les images et les fichiers audios et vidéos.

   Cette directive exclut de son champ d'application les ordinateurs portables, les miniportables et les téléphones cellulaires de base ainsi que tout autre appareil pouvant être relié aux réseaux sans fil du Ministère et dont les fonctionnalités diffèrent de celles énoncées ci-dessus.

## OBJECTIFS ET PRINCIPES DIRECTEURS

4. La présente directive a pour objet de :

   a) doter l'utilisateur d'un cadre de référence qui lui permettra d'assurer la sécurité et la protection de renseignements personnels, confidentiels et stratégiques qui transitent par son appareil sans fil ou qui y sont emmagasinés;
   b) sensibiliser l'utilisateur aux risques inhérents à l'usage non protégé d'un ANP;
   c) préciser les responsabilités des intervenants relativement à l'utilisation sécuritaire des ANP appartenant au Ministère.

5. En matière de sécurité de l'information, l'utilisation de l'ANP doit respecter les principes directeurs suivants :

   a) **évolution** : les pratiques et les solutions retenues en matière d'utilisation sécuritaire de l'ANP doivent être réévaluées périodiquement pour tenir compte des changements juridiques, organisationnels et technologiques ainsi que de l'évolution des menaces et des risques;
   b) **universalité** : les pratiques et les solutions retenues en matière de sécurité concernant l'utilisation de l'ANP doivent correspondre, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées à l'échelle nationale et internationale;
   c) **éthique** : le processus de gestion et d'utilisation sécuritaire de l'ANP doit être soutenu par une démarche d'éthique visant à assurer la régulation des conduites et la responsabilisation individuelle.

## RESPONSABILITÉS DES INTERVENANTS

### Le sous-ministre

6. Le sous-ministre approuve et diffuse la présente directive.

### Le responsable organisationnel de la sécurité de l'information du Ministère

7. Le responsable organisationnel de la sécurité de l'information nommé par le sous-ministre en vertu de la Directive sur la sécurité de l'information gouvernementale s'assure de la mise en application de la présente directive et de sa mise à jour. De plus, il avise les autorités du Ministère de toute dérogation à cette directive.

### La Direction des ressources informationnelles

8. La Direction des ressources informationnelles du Ministère est responsable de fournir à celui-ci l'encadrement, le soutien et les mécanismes d'exploitation et de prévention nécessaires à l'utilisation sécuritaire des ANP. À cette fin, elle :

   a) assure la gestion, la distribution et l'administration des ANP et en définit les règles associées;
   b) met en place des mesures de sécurité relevant de sa compétence, en avise les utilisateurs et en contrôle l'efficacité;
   c) s'assure que l'information est détruite dans des situations d'urgence, lors du transfert d'un ANP d'un utilisateur à un autre ou avant que l'appareil ne soit acheminé à la réparation, au recyclage ou au rebut;
   d) assure la sensibilisation, la formation et le soutien pour une utilisation sécuritaire des ANP;
   e) effectue la reddition de comptes exigée par le responsable organisationnel de la sécurité de l'information du Ministère.

**L'utilisateur**

9. L'utilisateur est responsable de la protection de l'information transitant par son ANP de même que de son traitement et de sa conservation sécuritaire. À cette fin, il :
   a) protège l'accès à son ANP à l'aide d'un mot de passe;
   b) applique en tout temps et en tout lieu les bonnes pratiques en matière d'utilisation sécuritaire de son ANP;
   c) s'engage à respecter les droits d'auteur des logiciels installés sur l'ANP et à ne pas télécharger, reproduire électroniquement ou transmettre à un tiers tout logiciel protégé par un droit d'auteur, une marque de commerce ou un brevet;
   d) s'engage à ne pas modifier la configuration et les mesures de sécurité mises en place sur son ANP;
   e) informe son responsable de toute violation des mesures de sécurité dont il pourrait être témoin et de toute anomalie ou incident qui pourrait nuire à la protection de l'information stockée dans son ANP;
   f) procède à la destruction sécuritaire de l'information lorsqu'elle n'est plus requise;
   g) s'engage à respecter les dispositions de la présente directive.

**LIGNE DE CONDUITE**

**Principes d'attribution des ANP**

10. L'attribution des ANP est faite selon les principes décrits dans la Directive ministérielle concernant l'attribution et la gestion de l'équipement en téléphonie mobile et des ordinateurs portables.

**Propriété de l'ANP et droit d'accès**

11. Les ANP fournis par le Ministère demeurent la propriété de ce dernier et ils peuvent être récupérés en tout temps.
12. Toute information emmagasinée sur les ANP est réputée constituer une information à laquelle le Ministère a accès.
13. Le Ministère se réserve le droit d'accéder aux courriels, messages vocaux ou fichiers électroniques traités ou emmagasinés sur l'ANP de l'utilisateur. Ces actions peuvent être réalisées uniquement à l'intérieur des activités de maintenance de l'équipement et des logiciels ou pour repérer des communications qui ne seraient pas conformes aux conditions d'utilisation prescrites, sans s'y limiter, par la présente directive.
14. Seuls les ANP fournis par le Ministère peuvent être reliés au réseau ministériel.

**Gestion centralisée des mesures de sécurité**

15. Les mécanismes de sécurité des ANP sont gérés à distance par la direction des ressources informationnelles du Ministère et, selon les besoins, ils sont déterminés par le responsable organisationnel de la sécurité de l'information.

**Utilisation d'un mot de passe**

16. L'utilisation d'un mot de passe d'au moins six (6) caractères permettant d'accéder aux ANP est obligatoire à compter de la date d'entrée en vigueur de la présente directive. Les autres mécanismes d'accès ne sont pas autorisés (déverrouillage par symboles ou points à relier, code NIP composé uniquement de chiffres, reconnaissance faciale, empreinte digitale, etc.).

17. Le mot de passe doit être changé au plus tard tous les quatre-vingt-dix (90) jours.

**Chiffrement**

18. Lorsqu'elle est transmise ou emmagasinée dans l'ANP ou dans ses cartes d'extension de mémoire, l'information personnelle, confidentielle ou stratégique doit être chiffrée. À défaut de disposer de la possibilité de chiffrement des cartes d'extension de mémoire, l'utilisation de ces cartes est interdite.

**Courrier électronique et annexes**

19. Toute information personnelle, confidentielle ou stratégique résultant d'échanges de courriels, avec ou sans fichiers joints, doit être chiffrée, limitée à l'essentiel et, lorsqu'elle n'est plus requise, effacée de l'ANP.
20. Une mise en garde sous forme d'avis de confidentialité doit accompagner les courriels transmis par l'ANP.
21. L'utilisation des serveurs de courriels grand public (p. ex. Gmail, Outlook, Yahoo, etc.) n'est pas autorisée.

**Synchronisation de l'ANP avec le serveur**

22. La synchronisation avec le serveur du Ministère permet de limiter le risque d'indisponibilité de l'information emmagasinée sur l'ANP, particulièrement en cas de perte, de vol ou de défaillance de celui-ci. La fréquence de synchronisation doit raisonnablement tenir compte de la valeur de l'information à protéger, des risques potentiels et de leur incidence sur la mission du Ministère. De façon générale, la synchronisation doit être faite au moins une fois par mois.
23. La synchronisation de l'ANP doit être faite par une connexion filaire en utilisant les câbles approuvés fournis par le Ministère. La synchronisation sans fil doit être désactivée par défaut pour éliminer les risques d'interception des données.

**Désactivation de compte**

24. Le compte de l'utilisateur est désactivé après cinq (5) tentatives de saisie consécutives d'un mot de passe erroné. La réactivation doit être faite à la demande de l'utilisateur et après vérification de son identité par le personnel du centre d'assistance aux utilisateurs de la direction des ressources informationnelles du Ministère.

**Bris ou perte de l'appareil**

25. L'utilisateur qui constate un bris ou la disparition de son ANP doit, sans délai, informer le centre d'assistance aux utilisateurs de la direction des ressources informationnelles du Ministère. Celle-ci procédera au remplacement de l'ANP endommagé ou à la désactivation de l'ANP perdu et en informera le responsable de la sécurité de l'information du Ministère.

**Périphérique main libre Bluetooth (téléphonie)**

26. La technologie Bluetooth utilise des ondes radio sur une distance d'environ 10 mètres pour établir un lien sans fil entre l'ANP et un dispositif qui lui est relié (haut-parleur et microphone). En vue de protéger la communication entre l'ANP et les dispositifs :

    a) la fonctionnalité de Bluetooth (main libre sans fil) est activée selon le besoin justifié de l'utilisateur;

b) la détection automatique des appareils compatibles avec la technologie Bluetooth doit être désactivée;
c) étant donné que le mot de passe initialement utilisé au moment du jumelage est identique sur tous les appareils, il doit être modifié à la première utilisation.

**Technologie Near Field Communication (NFC)**

27. Les ANP disposant de la technologie NFC (technologie de communication en champ proche) sont très vulnérables aux attaques informatiques, car la NFC n'utilise aucun système d'authentification pour s'assurer que l'échange de données entre deux appareils est légitime. Cette technologie doit donc être désactivée dans tout ANP qui en est pourvu.

**Contrôle de l'application de la directive**

28. Le sous-ministre peut appliquer des mesures de contrôle appropriées relativement à l'utilisation d'un ANP et à l'information qui y est stockée. Ces mesures, ad hoc ou automatisées, sont exécutées conformément au cadre législatif et administratif en vigueur. De plus, le sous ministre peut vérifier l'utilisation faite de l'ANP lorsqu'il a des raisons de soupçonner qu'elle déroge à la présente directive et au cadre législatif et administratif en vigueur.

**Sanctions**

29. Tout utilisateur d'un ANP qui enfreint les dispositions de la présente directive s'expose à des mesures administratives ou disciplinaires en fonction de la gravité et des conséquences de son geste. Ces mesures peuvent inclure la révocation du droit d'utilisation de l'ANP, une suspension ou un congédiement, et ce, conformément aux dispositions des lois et règlements, des conventions collectives et des contrats de travail en vigueur.

**Approbation de la directive**

La présente directive est approuvée par le sous-ministre le :……..

**Entrée en vigueur de la directive**

La présente directive entre en vigueur le ……

# Annexe III. Cadre légal et normatif

Le présent document prend appui sur des fondements légaux et normatifs tels que les lois, les directives, les normes, les standards et les pratiques gouvernementales.

Fondements légaux

1. Directive sur la sécurité de l’information gouvernementale;
2. Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1);
3. Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1);
4. Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03);
5. Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics;
6. Lois sectorielles régissant la mission de chaque organisme.

Fondements normatifs

7. Cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l’information;
8. Cadre gouvernemental de gestion de la sécurité de l’information;
9. Normes internationales, notamment : ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 et ISO/IEC 31000;
10. Politiques et directives relatives à la sécurité de l’information propres à chaque organisme;
11. Pratiques gouvernementales en matière de sécurité de l’information.

# Annexe IV. Liste des pratiques recommandées

## Préparation et installation

**P1 :** **Désactiver l'ANP après un nombre déterminé de tentatives d'accès infructueuses –** Configurer un temps d'attente de plus en plus long à chaque tentative d'accès à l'appareil. Activer le blocage ou la désactivation automatique de l'ANP après plusieurs tentatives d'accès infructueuses (établir un nombre optimal d'essais, par exemple cinq). Cette mesure permet d'empêcher des attaques informatiques visant à connaître le mot de passe de l'ANP pour accéder à son contenu.

**P2 :** **Activer le verrouillage automatique de l'ANP après un court délai d'inactivité –** Un délai de 1 à 5 minutes avant un verrouillage automatique ou la mise en veille de l'appareil ajoute une protection supplémentaire en cas de perte ou lorsque l'ANP est laissé sans surveillance. En effet, si le délai d'inactivité est expiré, une personne malintentionnée ne pourra pas accéder au contenu de l'appareil sans connaître le mot de passe.

**P3 :** **Désactiver l'affichage des messages de notification lorsque l'ANP est verrouillé –** Certaines applications envoient des messages de notification d'événements à l'utilisateur, qui peuvent revêtir un caractère confidentiel. Ces messages sont signalés au moyen d'un son, d'une vibration ou d'un message d'alerte, et ce, même si l'appareil est verrouillé (p. ex. nouveau courriel ou message texte entrant, approche d'un événement planifié dans le calendrier, etc.). La non-désactivation de cette fonction permet à une personne malintentionnée de consulter des alertes privées sans avoir à déverrouiller l'ANP.

**P4 :** **Verrouiller l'ANP avec un mot de passe –** L'accès à l'ANP doit toujours être protégé par un mot de passe. Cette mesure simple et efficace permet d'assurer la confidentialité des données que contient l'appareil.

**P5 :** **Changer régulièrement le mot de passe pour accéder au contenu de l'ANP –** Planifier un changement périodique du mot de passe. Si le système le permet, l'utilisateur peut être forcé d'effectuer ce changement. Dans le cas contraire, des rappels peuvent être envoyés aux utilisateurs pour qu'ils appliquent cette mesure.

**P6 :** **Sécuriser le réseau de l'organisation par le chiffrement[32] des communications et un système d'authentification –** Les réseaux Wi-Fi offrent des solutions robustes de chiffrement des communications à l'exemple de l'infrastructure à clés publiques. Le protocole de chiffrement WEP[33] est fortement déconseillé, car la clé de chiffrement peut être décryptée en quelques minutes. La solution WPA2[34] est recommandée, car elle utilise un mécanisme de chiffrement plus

**32. Chiffrement :** Opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possédant pas la clé permettant de le ramener à sa forme initiale. Synonyme : cryptage *[OQLF - Grand dictionnaire terminologique]*

**33. WEP :** Le *Wired Equivalent Privacy* est un protocole servant à sécuriser les réseaux sans fil de type Wi-Fi à l'aide d'une clé de chiffrement. Ce protocole est peu utilisé, car il comporte une faille de sécurité importante qui permet à une personne malintentionnée de trouver la clé de chiffrement par une simple écoute clandestine du réseau pendant quelques minutes ou quelques heures.

**34. WPA2 :** Le *Wi-Fi Protected Access 2*, successeur du WPA, est un protocole servant à sécuriser les réseaux sans fil de type Wi-Fi. Le WPA2 a été développé pour contrer les failles de sécurité que comportait le protocole WEP. Il possède ainsi une clé de chiffrement plus grande et utilise un mécanisme de chiffrement plus robuste. Il n'est plus possible d'obtenir la clé de chiffrement par une simple écoute du réseau. WPA garantit également une intégrité nettement améliorée des données transmises.

robuste. Selon le niveau de sensibilité du réseau de l'organisation, une authentification composée d'un identifiant et d'un mot de passe pourrait être envisagée afin d'éviter les intrusions.

**P7 :** **Utiliser un mécanisme de contrôle d'accès robuste –** Utiliser un mécanisme qui exige un mot de passe fort constitué de chiffres, de lettres et de symboles pour assurer la protection des données sensibles. Dans le cas où la sensibilité de l'information est faible et où le risque peut être acceptable, l'utilisation d'un code NIP (généralement composé de quatre chiffres) peut être suffisante dès lors que la pratique recommandée P1 est appliquée.

Il est à noter que le déverrouillage par symbole (points à relier) n'est pas recommandé en raison de l'insuffisance de sa richesse combinatoire. Le déverrouillage par reconnaissance faciale, quant à lui, n'est pas encore au point, puisqu'il peut, dans certains cas, être contourné en utilisant une photo de l'utilisateur. Le contrôle d'accès par empreinte digitale ou par reconnaissance oculaire est également à proscrire car, contrairement à un mot de passe, il est impossible de modifier une empreinte biométrique lorsqu'elle a été piratée.

**P8 :** **Chiffrer les données sensibles –** Chiffrer les données sensibles stockées sur l'ANP. Cette mesure permet de préserver la confidentialité de l'information en cas d'interception ou d'extraction des données par une personne malintentionnée. Le chiffrement des données doit être fait à l'aide d'un algorithme dont la robustesse est éprouvée.

**P9 :** **Supprimer le contenu de l'ANP à distance –** Activer l'option d'administration de données à distance pour pouvoir supprimer l'information que contient l'ANP en cas de perte ou de vol. Cette pratique peut être combinée avec la pratique 1. Les données seraient alors automatiquement effacées après un nombre défini de tentatives d'accès infructueuses.

**P10 :** **Activer le pare-feu de l'ANP –** Si l'option est disponible, l'activation du pare-feu permet de bloquer les connexions douteuses que certaines applications pourraient utiliser.

**P11 :** **Permettre à l'utilisateur d'autoriser la prise en charge à distance de son ANP –** Mettre en place un système permettant à l'utilisateur de l'ANP d'accepter ou de refuser chaque demande de prise en charge de son ANP par l'équipe de soutien technique de l'organisation. L'équipe technique doit idéalement communiquer avec l'utilisateur pour le prévenir que son appareil fera l'objet d'une telle prise en charge.

**P12 :** **Utiliser des applications qui sécurisent l'envoi des messages –** Il existe des applications de messagerie instantanée qui permettent d'envoyer des messages sécurisés. Ces messages sont notamment entièrement chiffrés, rendant ainsi l'information illisible même si elle est interceptée par une personne malintentionnée lors de sa transmission.

**P13 :** **Désactiver les services SMS et SMM s'ils ne sont pas requis par l'organisation –** Si l'organisme public ne voit aucune utilité aux SMS ou aux SMM pour la réalisation de sa mission, il est préférable de désactiver ces services.

**P14 :** **Installer un antivirus sur le poste de travail et le serveur de l'organisation –** L'installation d'un antivirus sur le poste de travail et le serveur de l'organisation de même que sa mise à jour périodique permettent de réduire les risques de transmission de logiciels malicieux à l'ANP.

**P15 :** **Installer un antivirus sur l'ANP –** L'installation d'un antivirus sur l'ANP peut aider à éliminer certains logiciels malicieux installés par mégarde. Par ailleurs, sa mise à jour périodique est essentielle pour maintenir un niveau élevé de sécurité sur l'ANP.

**P16 :** **Installer uniquement les applications et les services requis pour répondre aux besoins de l'utilisateur –** Les applications et les services installés sur l'ANP doivent être vérifiés et contrôlés périodiquement pour s'assurer qu'ils n'accèdent pas à de l'information critique ou ne la transmettent pas à une tierce personne non autorisée, qu'ils n'installent pas de logiciels malicieux et qu'ils répondent aux critères de sécurité appliqués par l'organisation.

**P17 :** **Utiliser un serveur de courriels sécurisé –** Mettre en place et utiliser un serveur de courriels sécurisé pour les communications des utilisateurs d'ANP. Sensibiliser l'utilisateur au fait qu'il ne doit pas employer les serveurs de courriels grand public (p. ex. Gmail, Outlook, Yahoo, etc.) pour envoyer des courriels associés à son travail, car l'organisation n'a pas la maîtrise de ces serveurs.

**P18 :** **Restreindre l'utilisation de la fonction d'enregistrement sonore ou visuel –** Des restrictions adaptées au contexte organisationnel doivent être établies quant à l'activation des fonctionnalités multimédias comme la prise de photos, de vidéos ou d'enregistrements sonores à l'intérieur de l'organisation.

**P19 :** **Planifier la synchronisation des données sur une base régulière –** La synchronisation des données doit être exécutée de façon régulière pour conserver une copie de sécurité qui pourra être récupérée en cas d'incident. L'intervalle entre deux synchronisations peut être raccourci, particulièrement dans le cas où le niveau de confidentialité des données est élevé.

**P20 :** **Interdire l'accès à la géolocalisation pour les applications qui ne requièrent pas ce service –** Si le fonctionnement d'une application ne nécessite pas l'utilisation du service de géolocalisation, il est important d'interdire l'accès à ce service dans les paramètres de l'ANP, si ce n'est pas déjà fait par défaut.

**P21 :** **Encadrer l'utilisation du système de géolocalisation –** Si l'utilisation du système de géolocalisation de l'ANP peut porter atteinte à la vie privée et à la liberté de déplacement, il n'en demeure pas moins que, lorsque la sécurité des personnes est en jeu, l'OP peut être amené à appliquer des mesures de surveillance strictes pour assurer la sécurité de ses employés. Ainsi, des règles d'encadrement du service de géolocalisation, proportionnelles aux risques courus, peuvent être appropriées. Il convient, dans ce cas, d'informer les personnes concernées des mesures de surveillance dont elles font l'objet.

## Formation et utilisation

**P22 :** **Effacer les messages SMS ou SMM sensibles lorsqu'ils ont été lus –** Les services de messagerie SMS et SMM ne sont pas adaptés au stockage de données sensibles. Les messages SMS à caractère sensible doivent donc être supprimés après leur lecture. L'information sensible pourrait être stockée dans un endroit plus sûr (p. ex. poste de travail) avant sa suppression.

**P23 : Utiliser un réseau privé virtuel (RPV[35]) pour accéder à distance au réseau de l'organisation –** Lors d'une connexion à un point d'accès sans fil en dehors des locaux de l'organisation, il est recommandé d'utiliser le réseau privé virtuel pour tout accès au réseau de l'organisation. La connexion doit être sécurisée par un identifiant et un mot de passe robuste. Le RPV (ou VPN en anglais) permet de créer une connexion directe et chiffrée entre l'ANP et les serveurs de l'organisation, rendant ainsi les communications sécuritaires.

**P24 : Privilégier la synchronisation par câble –** La synchronisation par câble est plus sécuritaire que la synchronisation sans fil, car les données transférées ne peuvent pas être interceptées à distance.

**P25 : Utiliser les équipements homologués pour la synchronisation ou la recharge de l'ANP –** Certains câbles non homologués de recharge de l'ANP et de synchronisation des données peuvent contenir des logiciels malicieux qui sont transférés au poste de travail ou à l'ANP lors de leur utilisation. Pour éviter cette situation, l'usage des équipements homologués est recommandé.

**P26 : Ne pas inscrire ou afficher le nom de l'organisation sur l'ANP –** Ne pas inscrire ou afficher sur l'appareil de l'information permettant d'identifier l'organisme public (logo, nom de l'OP, etc.) pour ne pas susciter l'intérêt de personnes mal intentionnées.

**P27 : Communiquer avec les entités responsables –** En cas de perte ou de vol de l'appareil, communiquer sans délai la situation à l'unité administrative responsable de la gestion de l'ANP ou au fournisseur de services de l'appareil pour connaître la procédure à suivre. Ces spécialistes peuvent notamment verrouiller et localiser l'appareil, supprimer le contenu de l'ANP à distance et bloquer la carte SIM en cas de nécessité.

**P28 : Établir une communication avec l'ANP (messagerie ou téléphonie) –** En cas de perte de l'ANP, tenter d'établir une communication avec l'appareil, notamment en envoyant un message sur l'écran de verrouillage à l'intention de la personne qui l'aurait trouvé, en indiquant les coordonnées nécessaires pour le récupérer. S'il s'agit d'un téléphone intelligent ou d'un téléphone-tablette, une communication téléphonique peut également être établie.

**P29 : Sensibiliser les utilisateurs d'ANP et les former –** Mettre en œuvre des plans de formation et de sensibilisation périodiques destinés aux utilisateurs d'ANP pour, d'une part, les informer des risques de sécurité de l'information liés à l'utilisation d'un ANP et, d'autre part, leur présenter la directive ministérielle et les mesures de sécurité établies par l'OP à cet égard.

**P30 : Être vigilant en cas de comportement inhabituel de l'ANP –** Certains indicateurs peuvent révéler la présence d'un logiciel malveillant : le fonctionnement de l'ANP ralentit, celui-ci ne répond plus, se fige ou redémarre fréquemment, l'appareil est chaud même si rien ne semble être ouvert, la batterie se vide rapidement, certains fichiers ne sont plus accessibles, etc. Lorsque le doute subsiste, il est judicieux d'avertir l'unité administrative responsable de la gestion de l'ANP pour que le problème soit réglé.

**35. Réseau privé virtuel (**RPV) : Réseau de communication privé qui peut se servir de l'infrastructure d'un réseau public pour transmettre des données qui sont protégées grâce à l'utilisation de techniques de chiffrement ou d'encapsulation. Terme anglais *: VPN (Virtual Private Network) [OQLF - Grand dictionnaire terminologique]*

**P31 :** **Être vigilant lorsque l'ANP est contrôlé à distance par l'équipe de soutien technique –** L'utilisateur doit s'assurer de l'identité du technicien qui contrôle son ANP. Il doit aviser le responsable de la sécurité de l'information de tout comportement inhabituel observé à cet égard.

**P32 :** **Établir une procédure applicable en cas d'incident et en informer le personnel :** Un document qui présente le détail de la procédure peut être remis à l'utilisateur d'un ANP pour l'informer des mesures à prendre en cas d'incident. Ce document indique également les coordonnées des personnes-ressources chargées de l'administration à distance des ANP.

**P33 :** **Établir des règles relatives à l'utilisation sécuritaire d'une carte mémoire –** Toutes les règles de sécurité concernant le stockage de l'information sur l'ANP s'appliquent également aux cartes mémoire qui peuvent y être connectées.

**P34 :** **Sensibiliser les utilisateurs à la protection et à l'utilisation sécuritaire des cartes mémoire de l'ANP –** La sensibilisation des utilisateurs contribue fortement à la réduction des risques associés à une utilisation inadéquate des cartes mémoire.

**P35 :** **Chiffrer les données sensibles stockées sur la carte mémoire amovible –** Cette mesure permet de préserver la confidentialité de l'information des données contenues dans la carte mémoire amovible insérée dans l'ANP. Le chiffrement des données doit être fait à l'aide d'un algorithme dont la robustesse est éprouvée.

**P36 :** **Chiffrer les courriels si l'option est disponible –** Si le chiffrement des courriels est possible, l'activation de cette option permet d'assurer la confidentialité des messages envoyés. Le chiffrement des courriels doit être fait à l'aide d'un algorithme dont la robustesse est éprouvée.

**P37 :** **Mettre un avis de confidentialité en signature aux courriels envoyés –** L'avis de confidentialité est utile notamment lorsqu'un courriel est envoyé à un mauvais destinataire. L'avis le prévient, entre autres, de supprimer le courriel reçu si ce dernier ne lui est pas destiné et d'en avertir l'expéditeur.

**P38 :** **Respecter les règles régissant les échanges par courriel –** L'organisme public doit se conformer à la Directive sur l'utilisation éthique du courriel, d'un collecticiel et des services d'Internet par le personnel de la fonction publique. Ce document est disponible à l'adresse suivante : http://www.rpg.tresor.qc/pdf/1-1-1-5.pdf.

**P39 :** **Vérifier la crédibilité du courriel et des pièces jointes –** Les cybercriminels ont souvent recours à l'hameçonnage[36] ou au piratage psychologique[37] par courriel pour soutirer de l'information sensible ou pour infecter l'ANP avec un logiciel malicieux. Ces courriels sont souvent douteux et illogiques et ils mettent l'utilisateur dans des situations inhabituelles ou inconfortables. La pièce jointe peut également être un code malicieux qui s'exécute dès son ouverture. Une vérification de l'authenticité de ces courriels est de mise pour éviter des incidents désastreux.

[36] **Hameçonnage :** Technique de fraude visant à obtenir des informations confidentielles au moyen de messages ou de sites usurpant l'identité d'une tierce personne. *[OQLF - Grand dictionnaire terminologique]*

[37] **Piratage psychologique ou fraude psychologique :** Tromperie qui résulte d'échanges entre individus afin d'extorquer des informations dans le but de pénétrer frauduleusement un système. La désignation « ingénierie sociale » constitue un calque de l'anglais. *[OQLF - Grand dictionnaire terminologique]*

**P40 :** **Éviter de communiquer des données sensibles par courriel –** Étant donné les risques de divulgation d'information par inadvertance, par hameçonnage, par piratage psychologique ou par tout autre moyen, il est essentiel, dans la mesure du possible, de limiter la communication de données sensibles par courriel.

**P41 :** **Éviter de communiquer des données sensibles au moyen des services SMS et SMM –** Étant donné la facilité d'interception des messages SMS et SMM, ces services de messagerie ne sont pas adaptés à l'envoi de données sensibles.

**P42 :** **Interdire l'enregistrement de données multimédias confidentielles sur l'ANP –** Les données telles que des photos, des vidéos et des sons de nature confidentielle (p. ex. photo d'une page d'un rapport, enregistrement d'une conversation téléphonique, etc.) ne doivent pas être enregistrées sur l'ANP pour ne pas porter atteinte à la confidentialité de l'information ou à la vie privée des personnes concernées.

**P43 :** **Interdire les ANP à proximité des zones d'échange d'information sensible –** Pour assurer la confidentialité des conversations, des présentations visuelles ou des réunions, l'ANP ne doit pas être autorisé dans les zones d'échange d'information sensible. Dans le cas contraire, les personnes présentes doivent au moins être avisées que leurs discussions ou présentations peuvent être enregistrées. Il est à noter que la mise hors tension de l'ANP n'est pas suffisante, car certains logiciels espions peuvent activer le microphone de l'ANP même si l'appareil est éteint.

**P44 :** **Garder l'ANP dans un endroit sûr pendant les déplacements –** Lors des déplacements, ne pas laisser l'ANP dans un endroit non sécuritaire ou sans surveillance (p. ex. poche arrière du pantalon, sur une table, sur un comptoir, etc.), même pour une courte durée. Prendre l'habitude de garder l'ANP sur soi (poche avant ou accroché à la ceinture) ou dans un sac à portée de la main.

**P45 :** **Désactiver la connexion Wi-Fi lorsqu'elle n'est pas utilisée –** La désactivation de la connexion Wi-Fi empêche l'ANP de se connecter automatiquement à des points d'accès connus, mais dont le nom (SSID) a été usurpé. Lorsque le besoin se présente, activer la connexion Wi-Fi et s'assurer que l'ANP est connecté au bon réseau.

**P46 :** **Être vigilant lors de la connexion aux réseaux sans fil ouverts –** La connexion de l'ANP à un réseau sans fil en dehors des locaux de l'organisation, notamment dans des lieux publics (p. ex. café, hôtel, aéroport, etc.), doit être faite avec prudence et se limiter au minimum de temps nécessaire, car les données qui y circulent peuvent être interceptées par une personne malintentionnée. Il est recommandé de ne pas consulter ou transférer des données critiques à l'occasion d'une telle connexion.

**P47 :** **Désactiver la connexion Bluetooth lorsqu'elle n'est pas utilisée –** La désactivation de la connexion Bluetooth rend l'ANP « invisible » et permet d'éviter son pairage avec des appareils inconnus utilisant la même technologie. En théorie, lors d'une demande de pairage, l'utilisateur est averti et les deux parties doivent convenir d'un mot de passe pour permettre la connexion. En pratique, plusieurs ANP ne permettent pas de modifier la configuration par défaut en vue de paramétrer les mesures de sécurité nécessaires. Dans un tel cas, un pirate informatique pourrait se connecter à l'ANP à l'aide de Bluetooth et, par exemple, en extraire la liste des contacts.

**P48 :** **Désactiver la connexion NFC lorsqu'elle n'est pas utilisée –** La désactivation de la connexion NFC permet d'éviter un échange de données confidentielles, à l'insu de l'utilisateur, avec un autre appareil malicieux. Cette pratique empêche également un pirate informatique d'envoyer des logiciels malicieux à l'ANP par un simple contact ou rapprochement physique avec l'ANP.

**P49 :** **Réduire l'utilisation de la technologie NFC au minimum –** La technologie NFC dans un ANP est très pratique et simple à utiliser. Elle est néanmoins tout aussi vulnérable, car elle ne comporte aucun système d'authentification pour s'assurer que l'échange de données entre deux appareils est légitime. Des attaques informatiques peuvent alors être lancées sans que l'utilisateur s'en aperçoive.

**P50 :** **Synchroniser l'ANP avec un terminal fiable –** Certains postes de travail non connus de l'ANP et que ne maîtrise pas l'utilisateur peuvent contenir des logiciels malicieux qui sont transférés à l'ANP à l'occasion de la synchronisation.

**P51 :** **Effacer les données sensibles de l'ANP à la fin de leur utilisation –** Lorsqu'une information sensible n'est plus utile, la supprimer de l'ANP élimine le risque qu'elle soit consultée par une personne malveillante.

**P52 :** **Établir des restrictions concernant le stockage d'information –** L'ANP ne doit pas servir de support de stockage pour des mots de passe, des numéros d'identification personnels ou de l'information personnelle ou confidentielle sur son utilisateur.

**P53 :** **Stocker uniquement de l'information utile sur l'ANP –** Stocker seulement les données qui sont utiles au travail lors des déplacements pour ne pas compromettre d'autres données sensibles en cas d'incident.

**P54 :** **Intégrer les clauses de sécurité de l'information et de protection des renseignements personnels dans les ententes et les contrats; celles-ci sont généralement déterminées après une analyse des risques –** Cette mesure a pour objectif d'assurer la sécurité de l'information dans plusieurs cas, notamment : lorsque l'OP fait appel à un prestataire de services public ou privé pour le stockage de l'information à l'extérieur de ses locaux ou à l'extérieur du Canada, pour la gestion des ANP, leur configuration ou pour le soutien technique.

**P55 :** **Garder la carte mémoire dans un endroit sûr pendant les déplacements –** Ne pas placer la carte mémoire d'un ANP dans des endroits à la vue ou à la portée de tous. S'il n'y a aucune raison valable de la sortir, la carte mémoire devrait demeurer à l'intérieur de l'ANP lors des déplacements.

**P56 :** **Éviter de stocker des fichiers douteux sur la carte mémoire –** S'assurer que les fichiers stockés sur la carte mémoire proviennent d'une source fiable. Certains fichiers douteux peuvent contenir des codes malicieux qui nuiront à l'ANP. Ces fichiers peuvent notamment avoir comme extension : *.exe, *.vbs, *.bin, *.com, *.bat, *.pif, etc.

**P57 :** **Modifier le mot de passe ou le NIP par défaut de la connexion Bluetooth de l'ANP –** Cette pratique permet d'éviter le jumelage de l'ANP avec un appareil inconnu qui tenterait d'utiliser le mot de passe par défaut. Éviter d'utiliser un ANP qui ne permet pas le changement du mot de passe de la connexion Bluetooth.

## Soutien et maintenance

**P58 :** **Centraliser la gestion de la configuration des paramètres de l'ANP –** Dans la mesure du possible, il est recommandé de centraliser la configuration de l'ANP des utilisateurs et non de laisser celle-ci à leur libre choix. Cette responsabilité doit être assignée au responsable de la gestion et de l'administration des ANP de l'organisation.

**P59 :** **Vérifier périodiquement les permissions accordées aux applications –** Les applications installées sur l'ANP doivent avoir les permissions strictement suffisantes à l'exercice de leurs fonctions (accès aux données, à Internet ou au contrôle des capteurs supportés par l'appareil). Les permissions accordées à une application doivent être vérifiées lors de son installation et à l'occasion de sa mise à jour pour s'assurer que les exigences de sécurité sont toujours respectées.

**P60 :** **Maintenir à jour le système d'exploitation de l'ANP et les applications installées –** La mise à jour régulière et automatique du système d'exploitation de l'ANP et de ses applications permet de corriger les éventuelles failles de sécurité de l'appareil, diminuant ainsi les risques d'infection de l'ANP par un code malicieux. Un ANP qui ne prend plus en charge l'évolution de son système d'exploitation doit être remplacé.

**P61 :** **Effectuer une destruction sécuritaire de l'information emmagasinée sur une carte mémoire** – Une carte mémoire sur laquelle a été sauvegardée de l'information sensible doit faire l'objet d'une destruction sécuritaire de ces données à la fin de leur utilisation. L'OP s'assure ainsi de réduire le risque de récupération de données sensibles. Pour plus d'information sur la destruction sécuritaire des données, se référer à la pratique recommandée PR-055 intitulée « Guide de destruction sécuritaire de l'information ».

**P62 :** **Effectuer régulièrement la sauvegarde des données contenues dans l'ANP –** Une copie de sécurité de l'ANP doit être faite sur une base régulière. Cette action est généralement prise en charge par l'unité administrative responsable de la gestion de l'ANP. Après un incident (p. ex. perte, vol, bris ou disfonctionnement de l'appareil), les copies de sécurité peuvent être utilisées pour récupérer l'information perdue ou restaurer l'état fonctionnel de l'ANP.

**P63 :** **Sauvegarder les données sensibles avant leur suppression de l'ANP –** Toute information sensible et importante pour la mission de l'organisation doit être transférée à l'ordinateur personnel de l'utilisateur ou au serveur de l'organisation avant d'être supprimée.

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique