Volet Infrastructure

Guide de référence des réseaux sans fil (Wi-Fi)

Table des matières

Liste des sigles et acronymes

BYOD	*Bring your own device*
CST	Centre de la sécurité des télécommunications
DI	Dirigeant de l'information
DSI	Dirigeant sectoriel de l'information
IP	*Internet Protocol*
NIST	National Institute of Standards and Technology
ROSI	Responsable organisationnel en sécurité de l'information
SaaS	*Software as a Service* (logiciel en tant que service)
SQI	Société québécoise des infrastructures
WPA	*Wi-Fi Protected Access*
WEP	*Wired Equivalent Privacy*
WLAN	*Wireless Local Area Network*
WLANs	*Guidelines for Securing Wireless Local Area Network*

Historique des changements

Version	Date de publication	Modifications
4.0	Octobre 2018	Publication de la première édition

Avis aux lecteurs

Ce document en est à sa première version et se veut très évolutif. Des changements y seront donc apportés à la sortie des futures versions. Il est aussi à prévoir qu'une version numérique navigable en ligne sera produite sous peu.

Même si certains points abordés dans ce document peuvent s'appliquer à d'autres technologies sans fil, comme le cellulaire et le Bluetooth, l'intention des auteurs du document est de se concentrer uniquement sur le Wi-Fi. Ce choix est justifié par le besoin des organismes publics qui demandent un positionnement sur le réseau Wi-Fi.

Sommaire

La première partie du présent document se veut un outil pour bien saisir les besoins d'affaires liés à l'implantation des services de réseaux sans fil dans un organisme public. La seconde partie devrait susciter chez le lecteur une réflexion sur les enjeux de sécurité de l'information associés à l'usage de ces réseaux.

Pour aider les organismes publics dans la mise en place sécuritaire de leurs réseaux sans fil de type Wi-Fi, des recommandations ont été formulées. Voici un tableau récapitulatif de celles-ci :

1 – L'implantation du sans fil de type Wi-Fi dans les organismes publics doit être appuyée par une vision des besoins afin que son succès soit assuré.
2 – Il est recommandé que les organismes publics qui ont des aires d'attente ou des lieux susceptibles de recevoir des citoyens mettent en place des services Wi-Fi sécuritaires de type public avec accès à Internet seulement.
3 – Des services de réseaux sans fil de type Wi-Fi mis à la disposition de l'ensemble du personnel sont implantés dans tous les établissements. Il est primordial d'offrir une couverture complète dans l'ensemble des édifices afin que les employés de l'administration publique puissent collaborer aisément avec leurs pairs.
4 – Les technologies sans fil, les procédures pour les exploiter et les mesures de mitigation des risques sont établies selon la gestion du risque relatif à la nature de l'information qui y circule.
5 – On devra choisir des technologies sans fil performantes, évolutives et sécuritaires, qui répondent adéquatement aux besoins et dont l'exploitation nécessite peu de ressources.
6 – L'utilisation de la technologie sans fil Wi-Fi induit de nouveaux risques de sécurité de l'information qu'il importe de mitiger. Chaque organisme public doit s'assurer d'adopter une politique de sécurité de l'information qui prévoit des éléments précis sur les particularités des réseaux sans fil Wi-Fi. La documentation liée à la sécurité des réseaux sans fil doit être révisée régulièrement afin qu'elle suive l'évolution des menaces et des mesures qui s'y rattachent.

1. Les différents besoins d'affaires

Que ce soit dans des lieux publics, dans les locaux des entreprises, des moyens de transport ou encore à la maison, le citoyen québécois veut être branché à ses services numériques.

> CEFRIO – ÉTUDE 2017
>
> « 6 DÉTENTEURS DE TÉLÉPHONE INTELLIGENT SUR 10 UTILISENT RÉGULIÈREMENT DES RÉSEAUX WI-FI LORSQU'ILS SONT À L'EXTÉRIEUR DE LEUR DOMICILE[1]. »

Les employés de l'État, eux, adoptent des façons de travailler modernes qui impliquent la mobilité et la collaboration.

De leur côté, les organismes publics changent tant sur le plan physique, par le réaménagement des lieux de travail, que sur le plan de l'organisation du travail. Ces organismes ont aussi la responsabilité de sécuriser l'information qu'ils détiennent.

Ces trois volets se traduisent en trois besoins d'affaires distincts, qui seront traités dans ce guide.

Besoins d'affaires du grand public

- Accéder à Internet pour répondre à des besoins personnels (réseaux sociaux, courriels, transactions bancaires, appels vocaux et vidéo);
- Naviguer de façon sécuritaire;
- Accéder par défaut à l'offre de services numériques de l'organisme public où il se trouve;
- Autres en fonction du contexte de l'organisme.

Besoins d'affaires des employés des organismes publics

- Accéder à l'information de l'organisme public (courriels, agenda, documents, systèmes d'information, outils de collaboration et de bureautique);
- Avoir des accès sans fil sécuritaires;
- Avoir une couverture sans fil complète et fiable;
- Autres en fonction du contexte de l'organisme.

1. CEFRIO, *Le portait numérique des foyers québécois en 2017*. [En ligne], 2017, https://cefrio.qc.ca/netendances/le-portrait-numerique-des-foyers-quebecois-en-2017/. (Consulté le 17 avril 2018.)

Besoins d'affaires des organismes publics

- Disposer d'un réseau sans fil performant qui assure la sécurité des systèmes d'information et la protection des renseignements personnels ou confidentiels;
- Offrir des environnements de travail performants à leur personnel;
- Exploiter les environnements technologiques de façon optimale;
- Mettre en application des technologies dites « branchées » nécessitant le Wi-Fi (Internet des objets, localisation de matériel, etc.);
- Autres en fonction du contexte de l'organisme.

Il devient donc important de bien guider les organismes publics dans l'implantation de technologies pouvant répondre à ces besoins. Le présent guide apporte des recommandations sur l'implantation de l'une d'elles, soit le réseau sans fil de type Wi-Fi.

La première recommandation vise à bien positionner l'apport du réseau sans fil dans l'organisation, tant actuellement que dans l'avenir.

Recommandation 1 – L'implantation du sans fil de type Wi-Fi dans les organismes publics doit être appuyée par une vision des besoins afin que son succès soit assuré.

L'implantation d'un réseau sans fil de type Wi-Fi doit être faite en fonction des besoins existants et à venir. Une vision doit appuyer l'organisme public dans l'analyse de ses besoins, dans l'étude des risques, etc. Cette même vision doit permettre de tirer profit de l'apport des nouvelles technologies de l'information qui dépendent du Wi-Fi, comme les thermostats numériques, les caméras de surveillance, la téléphonie IP, les différents capteurs de présence et de mouvements, etc. Toutes ces technologies reposent sur les services de réseaux majoritairement sans fil de type Wi-Fi. Il faut donc que les organismes publics prévoient l'implantation de leur réseau sans fil en tenant compte de ces nouvelles possibilités.

La section à venir présente différents besoins d'affaires en matière de réseau sans fil appliquant la technologie Wi-Fi. De ceux-ci découlent des recommandations destinées aux organismes publics.

1.1 Les besoins d'affaires du grand public

Le citoyen désire être branché à ses services numériques et il s'attend à ce que son gouvernement lui offre de tels services. D'ailleurs, le gouvernement du Québec a fait des annonces importantes en ce sens, lesquelles annonces sont liées à la Stratégie numérique du Québec[2].

Pour optimiser l'expérience utilisateur, il est requis que des services d'accès sans fil soient mis à la disposition du grand public lorsque le citoyen est présent dans les locaux des organismes publics. À titre d'exemple, les salles d'attente des organismes publics sont des lieux où le citoyen souhaite avoir accès à un réseau sans fil.

Recommandation 2 – Il est recommandé que les organismes publics qui ont des aires d'attente ou des lieux susceptibles de recevoir des citoyens mettent en place des services Wi-Fi sécuritaires de type public avec accès à Internet seulement.

Ces services doivent offrir une performance adéquate pour répondre aux besoins du grand public. Il faut prévoir des technologies qui privilégieront de la bande passante pour certains types d'utilisation et qui bloqueront d'autres utilisations jugées inappropriées. Par exemple, l'accès à du contenu gouvernemental, comme les pages Web d'intérêt pour les citoyens présents sur place, devrait être privilégié par rapport à des sites de diffusion vidéo qui sont de grands consommateurs de bande passante.

Les sites inadéquats (p. ex. : pornographie, propagande haineuse, raciste ou sexiste, violence, etc.) devraient évidemment être inaccessibles, car ils sont jugés inappropriés, tant dans les lieux publics qu'ailleurs.

Les mécanismes de sécurité de l'organisme public doivent être implantés de façon à ce que le réseau local et le trafic de type public/Internet soient isolés. Cette bonne pratique dissocie le réseau de l'organisme public d'éventuelles tentatives d'accès non autorisé venant de la zone Wi-Fi publique. Voir la section 2 sur la sécurité pour obtenir plus de détails.

2. ÉCONOMIE, SCIENCE ET INNOVATION, *Stratégie numérique*. [En ligne], 2018, https://www.economie.gouv.qc.ca/objectifs/ameliorer/strategie-numerique/. (Consulté le 18 avril 2018.)

1.2 Les besoins d'affaires des employés des organismes publics

Comme c'est le cas dans le secteur privé, les environnements de travail des employés de l'administration publique doivent être modernisés. Ces lieux doivent offrir au personnel des outils performants, conviviaux et sécuritaires afin que les tâches soient accomplies de façon adéquate. D'ailleurs, des gestes concrets du gouvernement du Québec vont dans ce sens.

La Société québécoise des infrastructures (SQI) indique, dans son Plan stratégique 2018-2023[3], qu'elle modernise les environnements de travail de l'administration publique.

> Par conséquent, la SQI continuera, de manière toujours plus soutenue, à : […]
>
> – jouer un rôle de premier plan dans la modernisation des environnements de travail de l'administration publique.

Il devient évident que des réseaux Wi-Fi doivent être implantés dans les locaux des organismes publics pour soutenir le travail du personnel. Le numérique favorise la mobilité de l'employé qui participe à des rencontres et qui collabore constamment avec ses pairs. Les outils technologiques font maintenant partie intégrante de notre mode de vie et facilitent les interactions professionnelles et personnelles. Pour cette raison, le travailleur se procure de plus en plus d'appareils mobiles, tels que le cellulaire, la tablette et l'ordinateur portable.

Recommandation 3 – Des services de réseaux sans fil de type Wi-Fi mis à la disposition de l'ensemble du personnel sont implantés dans tous les établissements. Il est primordial d'offrir une couverture complète dans l'ensemble des édifices afin que les employés de l'administration publique puissent collaborer aisément avec leurs pairs.

Ces services doivent répondre aux besoins actuels des employés, notamment en matière de capacité, de disponibilité, de sécurité, de couverture et de convivialité d'utilisation. Cela dit, dès l'analyse de l'implantation de services Wi-Fi, il sera nécessaire d'anticiper une augmentation croissante de la charge associée aux nouveaux besoins. À titre d'exemple, un employé du secteur public peut avoir en sa possession un ordinateur portable, s'il s'agit d'un employé dit « mobile ». Certains peuvent également disposer d'un téléphone mobile. Peuvent aussi s'ajouter les

3. SOCIÉTÉ QUÉBÉCOISE DES INFRASTRUCTURES, *Plan stratégique*. [En ligne], 2018, https://www.sqi.gouv.qc.ca/apropos/Documents/Plan_strat%C3%A9gique_2018-2023.pdf. (Consulté le 23 avril 2018.)

appareils personnels, comme une tablette numérique et un téléphone mobile personnel. On parle ainsi de « BYOD », pour *bring your own device*. Tous ces appareils sont susceptibles d'être reliés à des services Wi-Fi. Dans l'avenir, il est envisageable que l'utilisation de technologies vocales sur *Internet Protocol* (IP) s'ajouterait à la liste des services du réseau sans fil de l'organisme public. Il faut donc prévoir qu'un employé pourrait avoir des besoins d'un réseau sans fil Wi-Fi pour au moins quatre dispositifs sans fil.

Les aménagements de bureaux sont en cours de changement à la suite de la révolution numérique et pour répondre à l'évolution et à la croissance des besoins. Les lieux de travail subiront de grandes transformations dans les prochaines années. Cela exige que le réseau sans fil couvre tous les recoins des édifices dans l'ensemble de l'administration publique. Le type de points d'accès et leur nombre nécessitent des analyses très exhaustives.

Un employé doit pouvoir utiliser le réseau Wi-Fi de façon conviviale, tandis que d'autres aspects primordiaux, comme la sécurité, doivent être pris en compte. Il faut réduire les impacts que ces considérations peuvent entraîner sur le travail des employés. À titre d'exemple, lorsqu'un employé se déplace, l'infrastructure technologique en place doit lui assurer la disponibilité de la connexion sans fil sans qu'il soit obligé de se reconnecter.

La sécurité demeure par ailleurs une priorité lors de l'implantation de tels services sans fil. La sécurité des systèmes d'information, du réseau local, des appareils et de l'information qu'ils contiennent ainsi que celle des utilisateurs doivent faire l'objet d'une évaluation du risque afin que des mesures de mitigation appropriées soient proposées et mises en application. Voir la section 2 sur la sécurité pour obtenir plus de détails.

1.3 Les besoins d'affaires des organismes publics

Les premières recommandations sont associées au type d'utilisateurs des réseaux sans fil. Reste maintenant à couvrir les besoins des organismes publics.

Sans détailler ici l'ensemble des besoins relatifs au réseau Wi-Fi, en voici certains qui méritent notre attention :

- avoir accès à des systèmes d'information protégés;
- offrir des environnements de travail performants aux membres du personnel;
- exploiter ses environnements technologiques de façon optimale;
- pouvoir mettre en place des technologies nécessitant le Wi-Fi (Internet des objets, localisation de matériel, etc.);
- assurer une haute disponibilité du réseau sans fil.

Le premier besoin est directement lié à la sécurité des systèmes d'information. Les menaces à l'égard des organismes, publics ou privés, sont tangibles et en constante augmentation. Elles sont diverses et présentes sur une base quotidienne.

L'administration publique prend très au sérieux la sécurité de ses systèmes d'information et de l'information qu'elle détient. C'est ainsi que l'implantation et l'exploitation quotidienne d'un réseau sans fil doivent être faites selon les meilleures pratiques en matière de sécurité de l'information.

Le matériel et les logiciels doivent être constamment mis à niveau pour que les réseaux sans fil soient performants, disponibles et sécuritaires. L'environnement de travail doit être adapté aux besoins des employés pour que ces derniers puissent exploiter à bon escient la nouvelle technologie disponible.

Recommandation 4 – Les technologies sans fil, les procédures pour les exploiter et les mesures de mitigation des risques sont établies selon la gestion du risque relatif à la nature de l'information qui y circule.

Comme nous l'avons indiqué précédemment, le travailleur d'aujourd'hui a des besoins qui diffèrent de ceux de ses prédécesseurs. Son environnement de travail doit s'adapter à ces besoins. L'organisme public doit faciliter la mise en œuvre de nouvelles façons de travailler. Entre autres, le réseau sans fil doit soutenir l'organisme public qui souhaite aménager de nouveaux locaux, se doter de salles de rencontre et mettre à la disposition de son personnel des outils de travail mobiles et collaboratifs.

Dans le contexte actuel, où la charge de travail des équipes en technologies de l'information est importante, la recherche d'efficience devient une priorité. Les organismes publics doivent donc privilégier les architectures de réseau sans fil qui réduisent les impacts sur la charge de travail sans que des compromis concernant la sécurité et les besoins exprimés soient nécessaires.

Recommandation 5 – On devra choisir des technologies sans fil performantes, évolutives et sécuritaires, qui répondent adéquatement aux besoins et dont l'exploitation nécessite peu de ressources.

À titre d'exemple, il existe des services Wi-Fi qui unissent le matériel physique, la surveillance, l'alertage et les logiciels d'exploitation. Le tout est offert en services infonuagiques de type logiciel, comme le SaaS. L'exploitation est ainsi optimisée et automatisée. Il est aussi possible de confier à un tiers l'établissement du réseau Wi-Fi et son exploitation au quotidien. Il faut considérer l'offre de services partagés parmi les solutions possibles dans un tel cas. Il est important de bien comprendre que la responsabilité demeure celle de l'organisme public dans tous les cas de figure. Le contrat entre l'organisme public et le prestataire de services prend alors une grande importance, surtout en ce qui a trait aux clauses portant sur la responsabilité telle que nous l'avons décrite précédemment.

2. Les aspects de sécurité de la technologie sans fil (Wi-Fi)

Des enjeux de sécurité de l'information sont associés à l'adoption rapide de la technologie sans fil. En effet, une organisation ou une personne malveillante, équipée d'outils qu'il est facile de se procurer, peut capter les renseignements transportés par ces réseaux.

Devant ces importants enjeux de sécurité, il importe que l'administration publique tienne compte des risques associés à l'utilisation des réseaux sans fil dans ses efforts de protection de l'information gouvernementale.

Une première démarche fondamentale consiste à réaliser une catégorisation de l'information qui transitera sur les réseaux sans fil de l'organisme, c'est-à-dire évaluer le niveau de sensibilité de l'information visée. Par la suite, en fonction de la détermination du niveau de sensibilité de l'information constaté et à la suite de l'analyse des risques, les mesures de mitigation (contrôles) de sécurité sont choisies et mises en application.

En prenant exemple sur les pratiques de nombreux pays expérimentés en cette matière, il est essentiel d'appliquer des mesures de sécurité visant à encadrer l'utilisation du sans fil dans l'administration publique.

Par exemple, au Royaume-Uni, le site gouvernemental met à la disposition des organismes publics un ensemble de recommandations relatives au partage des réseaux sans fil sur les lieux de travail[4].

En France, des recommandations pour un usage sécuritaire du Wi-Fi ont été publiées. Elles présentent les faiblesses (vulnérabilités) de cette technologie et les moyens de s'en prémunir[5].

Aux États-Unis, le standard SP 800-153 *Guidelines for Securing Wireless Local Area Networks* (WLANs) du National Institute of Standards and Technology (NIST)[6] propose aux organismes publics gouvernementaux et non gouvernementaux des recommandations pour sécuriser la configuration et pour surveiller leurs réseaux sans fil.

4. UNITED KINGDOM GOVERNMENT, *Sharing workplace wireless networks*. [En ligne], 2016, https://www.gov.uk/guidance/sharing-workplace-wireless-networks. (Consulté le 30 avril 2018.)
5. AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION, *Recommandations de sécurité relatives aux réseaux Wi-Fi.* [En ligne], 2013, https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_WI-FI_NoteTech.pdf. (Consulté le 2 mai 2018.)
6. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Guidelines for Securing Wireless Local Area Networks (WLANs)*. [En ligne], 2012, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf. (Consulté le 2 mai 2018.)

Au Canada, le Centre de la sécurité des télécommunications (CST) du gouvernement fédéral a mis à la disposition du public et du personnel spécialement affecté à l'utilisation du sans-fil et de la mobilité des pratiques exemplaires et des directives en cette matière. Ont également été publiées des recommandations et des orientations concernant la sécurisation des communications sans fil et mobiles au pays.

Tableau 1 : Résumé des publications disponibles dans les différents pays

Pays	Publications
Royaume-Uni	Mesures techniques à appliquer en matière de sécurité du sans fil[7]
France	Note technique *Recommandations de sécurité relatives aux réseaux Wi-Fi*
États-Unis	Recommandations techniques du NIST pour la protection des réseaux sans fil
Canada	Pratiques exemplaires et directives du CST[8] à tous les ministères et organismes du gouvernement du Canada au sujet des différents aspects de la sécurité des réseaux sans fil et mobiles

Public cible

L'information contenue dans cette section du document est à l'usage des personnes responsables de la sécurité des réseaux locaux sans fil (WLAN). Elle devrait également être utile aux ingénieurs réseau et aux personnes responsables de la sécurité ainsi qu'aux administrateurs responsables de la conception, de l'implantation, de la sécurisation et de la maintenance des réseaux sans fil. De même, elle sera utile au responsable organisationnel en sécurité de l'information (ROSI), au dirigeant sectoriel de l'information (DSI) et au dirigeant de l'information (DI) puisque chacun, dans son domaine d'activité, participe à la sécurité de l'information au sein de son organisme.

2.1 Un aperçu de la sécurité du sans fil (Wi-Fi)

Tout comme les réseaux filaires, les réseaux sans fil doivent intégrer les principaux objectifs de la sécurité de l'information que sont la disponibilité, l'intégrité et la confidentialité.

La *disponibilité* donne l'assurance que les ressources de l'infrastructure sans fil peuvent être accessibles et utilisées en tout temps seulement par les personnes autorisées.

7. UNITED KINGDOM GOVERNMENT, *op. cit*. (Consulté le 30 avril 2018.)
8. CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS DU GOUVERNEMENT DU CANADA, *Sans-fil et mobilité*. [En ligne], 2018, https://www.cse-cst.gc.ca/fr/publication/list/Wireless-and-Mobility. (Consulté le 30 avril 2018.)

L'*intégrité* permet de détecter tout changement dans les données lorsqu'elles sont en transit sur le réseau sans fil. Les changements autorisés doivent être permis tandis que les changements non autorisés doivent être bloqués.

La *confidentialité* donne l'assurance que les communications à travers le réseau sans fil ne peuvent pas être portées à la connaissance de personnes non autorisées et que l'information qui y circule n'est consultée que par les personnes qui disposent du droit d'accès.

2.2 Les risques et les menaces inhérents à l'utilisation du sans fil (Wi-Fi)[9]

Les réseaux sans fil Wi-Fi sont exposés à des risques semblables à ceux des réseaux câblés. Cependant, en raison de leur nature, ils sont généralement plus sensibles aux menaces suivantes :

- Écoute du trafic : l'attaquant surveille passivement les communications réseau pour intercepter les données, y compris les renseignements d'authentification.
- Analyse du trafic : l'attaquant surveille passivement les transmissions pour repérer les schémas de communication et les participants.
- Modification de messages : l'attaquant modifie un message légitime en y effectuant des manipulations diverses qui peuvent aller jusqu'à la suppression complète du message.
- Détournement de session : l'attaquant vole ou fait un usage non autorisé d'un service.
- L'homme au milieu : l'attaquant se fait passer pour le client vis-à-vis d'un point d'accès sans-fil et il se fait passer pour un point d'accès sans fil vis-à-vis du client. Cela lui permet d'intercepter les communications entre le point d'accès sans-fil et le client, obtenant ainsi de l'information d'identification et des données d'authentification.
- Mascarade : en utilisant le leurre, l'attaquant emprunte l'identité d'un utilisateur autorisé et obtient certains privilèges pour exploiter le réseau.
- Déni de service : l'attaquant empêche ou limite l'utilisation normale ou la gestion des réseaux ou des périphériques du réseau.
- Rejeu : l'attaquant surveille passivement les transmissions et retransmet les messages en agissant comme s'il était un utilisateur légitime.

9. CHANGHUA, He et John C. MITCHELL. *Security Analysis and Improvements for IEEE 802.11i*, article from Electrical Engineering and Computer Science Departments of Standford University, [En ligne], https://theory.stanford.edu/~jcm/papers/NDSS05.pdf. (Consulté le 17 avril 2018.)

- Points d'accès fictifs : points d'accès sans-fil qui se présentent comme légitimes et qui, en réalité, sont des outils de piratage servant à écouter les communications.

Sécurité de la norme 802.11x

La protection des communications sans fil Wi-Fi figure parmi les préoccupations des institutions prônant la norme. En préconisant la famille des normes 802.11, les enjeux de sécurité sont pris en considération par la Wi-Fi Alliance[10]. Au début, le protocole WEP a été proposé pour le cryptage des échanges sans fil. Très rapidement, ce protocole a démontré ses faiblesses et a été remplacé successivement par les protocoles WPA, puis WPA2[11]. À ce jour, le protocole de sécurité WPA2 est considéré comme la solution la plus sécuritaire pour les échanges sans fil. Cependant, au dernier trimestre de 2017, un groupe de chercheurs y a découvert certains points de vulnérabilité[12] qui ont porté la Wi-Fi Alliance à annoncer la sortie, pour 2018, d'une nouvelle mouture du protocole de sécurité, le WPA3[13].

2.3 La sécurité du sans fil à l'échelle gouvernementale

L'encadrement de la gestion des risques en matière de sécurité de l'information à l'échelle gouvernementale doit dorénavant nécessairement contenir la gestion des infrastructures Wi-Fi. Ainsi, la gestion de la sécurité du sans fil fera partie intégrante de la gestion de la sécurité de l'information dont la responsabilité demeure au niveau des ministères et organismes. Un rappel à l'intention des organismes publics concernant les préoccupations quant à l'utilisation d'un réseau sans fil devrait notamment tenir compte des points suivants :

- L'enregistrement obligatoire des points d'accès Wi-Fi. Ce faisant, dans une organisation, on utilise que des points d'accès légitimes, donc reconnus par l'organisme;
- L'utilisation de technologies approuvées par l'autorité compétente. Cela permet dutiliser que des ressources reconnues et testées par les autorités de l'organisme
- La sécurisation de points physiques qui servent le matériel sans fil. Par leur disposition, cette mesure permet l'accès des équipements seulement aux personnes autorisées de l'organisme;

10. WI-FI ALLIANCE. [En ligne], 2018, https://www.wi-fi.org/discover-wi-fi/security. (Consulté le 25 avril 2018.)
11. WEP (*Wired Equivalent Privacy)* : Un protocole de sécurité pour les réseaux locaux sans fil définis dans la norme IEEE 802.11. Amélioration de la sécurité apportée par le WAP : WPA : *Wi-Fi Protected Access* et par le WPA2 : *Wi-Fi Protected Access* version 2.
12. KEY REINSTALLATION ATTACKS, *Breaking WPA2 by forcing nonce reuse*. [En ligne], 2017, https://www.krackattacks.com/. (Consulté le 25 avril 2018.)
13. WI-FI ALLIANCE, *Wi-Fi Alliance introduces security enhancements*. [En ligne], 2018, https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements. (Consulté le 25 avril 2018.)

- La personnalisation des configurations. Cela évite l'utilisation des configurations par défaut;
- L'authentification obligatoire des utilisateurs. Cette mesure permet l'accès au réseau sans fil uniquement aux utilisateurs autorisés.
- L'utilisation obligatoire d'un portail captif pour accéder au réseau; Cela permet la gestion de l'authentification en forçant l'utilisateur à s'identifier avant d'utiliser les ressources du réseau sans fil.

sans filsans filLes préoccupations et les risques à considérer sont déjà bien connus et documentés. Les bonnes pratiques sont déjà déterminées et elles sont disponibles. Il appartient donc à chaque organisme public de se positionner à propos d'une politique de mise en œuvre et d'utilisation d'un réseau sans fil, ainsi que de la gestion des risques inhérents à ce type de technologie et de la mise en place des mesures de mitigation (contrôles) inhérentes.

Recommandation 6 – L'utilisation de la technologie sans fil Wi-Fi induit de nouveaux risques de sécurité de l'information qu'il importe de mitiger. Chaque organisme public doit s'assurer d'adopter une politique de sécurité de l'information qui prévoit des éléments précis sur les particularités des réseaux sans fil Wi-Fi. La documentation liée à la sécurité des réseaux sans fil doit être révisée régulièrement afin qu'elle suive l'évolution des menaces et des mesures qui s'y rattachent.

Mesures spécifiques

En plus de la politique de sécurité, des mesures techniques spécifiques en cette matière doivent aussi être déterminées et mises en application par les organismes publics. Par exemple, il est recommandé d'utiliser le réseau Wi-Fi en mode *infrastructure* et de rendre obligatoire l'utilisation d'un portail captif.

Utilisation du mode infrastructure

Dans un objectif de sécurité, les infrastructures à déployer à l'échelle gouvernementale doivent répondre aux besoins particuliers des organismes concernés. Ces infrastructures prendront notamment en considération les besoins d'affaires abordés dans les sections précédentes de ce document.

Lors du déploiement des réseaux sans fil Wi-Fi, il est recommandé que soient déployés des points d'accès sans fil configurés de façon telle qu'ils utilisent le mode *infrastructure* plutôt que le mode *ad hoc*. Avec le mode *ad hoc*, deux dispositifs sans fil peuvent communiquer entre eux sans l'intervention d'une autorité de contrôle centralisée. À titre d'exemple, deux ordinateurs peuvent s'échanger de l'information par le réseau Wi-Fi sans passer par un point d'accès. De son côté, le mode

infrastructure exige l'usage d'un point d'accès sans fil et les cartes réseau sans fil des systèmes ne peuvent pas interagir directement entre elles. Le point d'accès sans fil applique alors des restrictions pour l'accès au réseau.

Utilisation d'un portail captif

Un « portail captif » est une technique d'authentification qui redirige un client Web sans fil nouvellement connecté vers une page de contrôle d'accès. La page du portail peut exiger que l'utilisateur saisisse une information d'identification de connexion ou qu'il entre un code d'accès. On utilise aussi un portail captif pour afficher une politique d'utilisation, une politique de confidentialité ou une politique de suivi à l'utilisateur. Ce dernier doit accepter les conditions avant de pouvoir accéder au réseau. Donc, pour répondre aux besoins d'affaires du grand public, les portails captifs devraient être obligatoires pour les utilisateurs invités qui visitent les sites des ministères et organismes du gouvernement.

2.4 Les mesures de sécurité générales concernant le sans fil (Wi-Fi)[14]

Les mesures générales suivantes peuvent servir de guide et devront être prises en considération lors du déploiement d'un réseau Wi-Fi au sein des ministères et organismes. Elles sont mentionnées à titre indicatif seulement et ne prétendent pas être exhaustives. Ces mesures ont pour but de sensibiliser les responsables réseau à propos des points de sécurité à considérer quand on traite du sans fil :

- Effectuer le changement du mot de passe administrateur par défaut;
- Désactiver la diffusion SSID [15] (ne pas afficher l'identification du réseau disponible);
- Changer le SSID pour un nom unique propre à l'organisme;
- Activer la forme la plus élevée d'authentification et de cryptage prise en charge;
- Traiter le réseau sans fil Wi-Fi comme un accès externe et isoler le point d'accès Wi-Fi du réseau filaire en utilisant un dispositif de protection;
- Traiter le réseau sans fil Wi-Fi comme un point d'entrée potentiel pour les attaquants et adopter les mesures de sécurité qui conviennent;
- Exiger que toutes les transmissions entre les clients du réseau sans fil et les points d'accès sans fil soient cryptées;
- Ne donner accès qu'à Internet aux appareils externes de l'organisme public qui sont reliés au réseau sans fil Wi-Fi;

14. (ISC) 2, *CISSP Official Study Guide*, 7th Ed., 2015.
15. Fait référence au nom du réseau (*Service Set Identifier*).

- Ajuster la puissance du signal Wi-Fi afin d'éviter que ce signal soit accessible à l'extérieur des locaux de l'organisme.

Il est important de comprendre que le choix des mesures particulières que chaque organisme doit appliquer sera fait selon son propre environnement et son propre contexte; ces recommandations servant à titre de guides.

En effet, il existe de nombreuses technologies de protection. Il est donc nécessaire que chaque organisme puisse sélectionner la technologie la plus appropriée en fonction de ses façons de faire. De même, il est aussi essentiel que la conception sécurisée du réseau sans fil tienne compte des réseaux sans fil existants déjà présents dans l'organisme (*legacy*) et de l'infrastructure câblée en place.

2.5 Les impacts de l'utilisation du sans fil Wi-Fi sur les technologies émergentes[16]

Avec l'effet grandissant des technologies émergentes au sein du gouvernement, il est important qu'une attention particulière soit portée à l'utilisation du réseau sans fil pour se connecter aux infrastructures existantes et que les mesures de sécurité inhérentes soient mises en place. Citons, à titre d'exemple, le cas d'Internet des objets et le BYOD[17].

L'Office québécois de la langue française définit l'expression « Internet des objets » de la façon suivante : « Ensemble des objets branchés à Internet capables de communiquer avec des humains, mais aussi entre eux, grâce à des systèmes d'identification électronique, pour collecter, transmettre et traiter des données avec ou sans intervention humaine[18]. » L'un des moyens de communication de l'Internet des objets est précisément le réseau sans fil Wi-Fi.

Le développement exponentiel de l'Internet des objets s'accompagne aussi d'enjeux très importants portant sur la sécurité. Ainsi, dans une consultation publique sur la cybersécurité organisée par le gouvernement du Canada en 2016, il a été mentionné qu'en matière d'Internet des objets, « il n'existe actuellement aucune norme clairement établie en ce qui concerne la protection de ces dispositifs et des données qu'ils recueillent[19] ».

Le BYOD est une approche selon laquelle les organismes publics acceptent, par une entente, que les membres de leur personnel utilisent leurs appareils mobiles personnels au travail pour leurs activités tant personnelles que professionnelles. Dans

16. La prise en considération de la sécurité dans l'utilisation du mobile, comprend le BYOD, l'Internet des objets, etc.
17. BYOD signifie « *Bring Your Own Device* » (« Apportez votre propre matériel »).
18. OFFICE QUÉBÉCOIS DE LA LANGUE FRANÇAISE, *Fiche terminologique*. [En ligne], 2015, http://granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=26529845. (Consulté le 1er mai 2018.)
19. SÉCURITÉ PUBLIQUE CANADA, *Sécurité et prospérité dans l'ère numérique : Consultation concernant l'approche adoptée par le Canada en matière de cybersécurité*. [En ligne], 2016, https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2016-scrty-prsprty/index-fr.aspx. (Consulté le 1er mai 2018.)

ce cas, les employés peuvent connecter leur ordinateur portable, leur téléphone intelligent ou leur tablette au réseau sans fil de l'organisme public.

Ces nouvelles pratiques, dont l'adoption tend à s'intensifier et exerce une pression de plus en plus forte sur les organismes publics concernant leur adoption, suscitent leur lot de risques en matière de sécurité de l'information.

Dans le cadre du déploiement du sans fil au sein des organismes publics de la communauté gouvernementale, les enjeux de sécurité et de protection des renseignements personnels qu'entraîne l'utilisation du BYOD doivent être pris en considération dans tout effort de protection de l'information. Cela sera fait notamment par l'adoption de politiques claires sur le sujet et la mise en place des mesures de sécurité appropriées.

Les actions suivantes sont ainsi recommandées :

- Une analyse sur la gestion des risques;
- Un plan d'action pour la mise en application des mesures retenues pour sécuriser le réseau sans fil Wi-Fi;
- L'élaboration ou la mise à jour de la documentation liée à la gestion du changement (guides techniques, guides d'utilisateur, plan de communication, etc.);
- Des audits réguliers de l'environnement du réseau sans fil Wi-Fi mis en place;
- Une veille constante sur les menaces qui visent précisément les réseaux sans fil Wi-Fi.

Secrétariat
du Conseil du trésor
Québec
Au cœur de l'administration publique