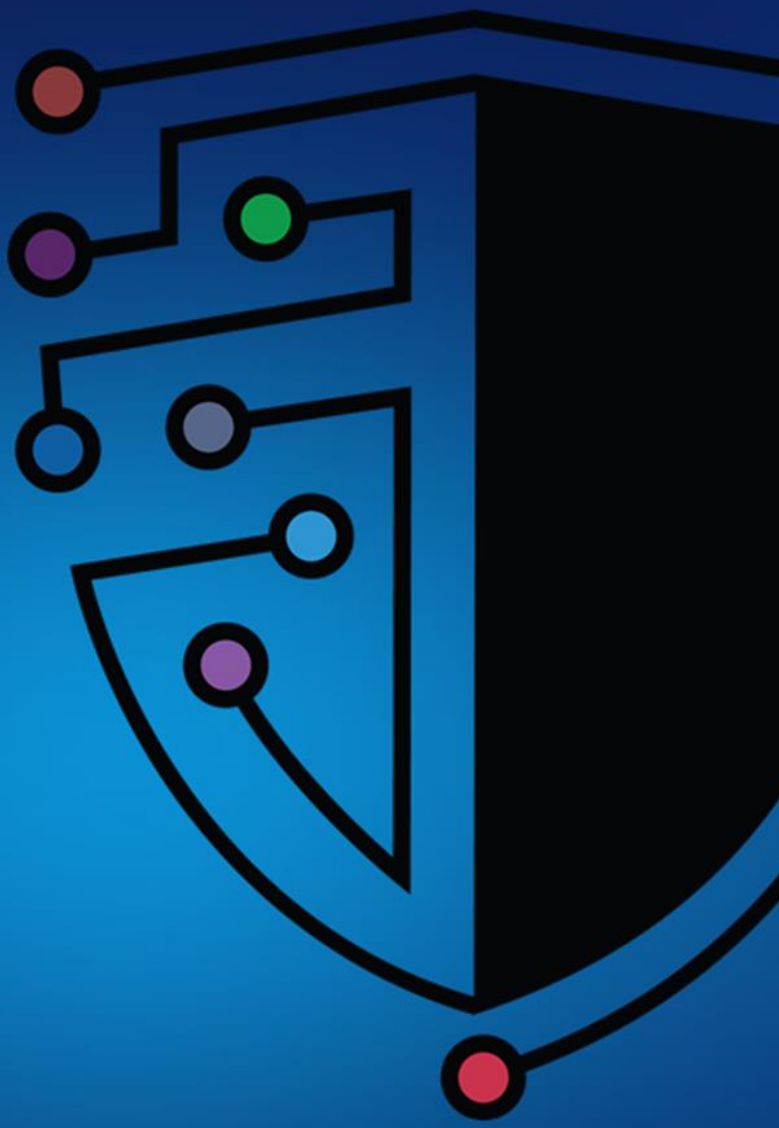
Direction générale adjointe

DE LA CYBERSÉCURITÉ
ET DE L'INFONUAGIQUE (DGACI)

2023-04-13



CYBERSÉCURITÉ

Directive sur la mise en place et l'exploitation sécuritaires de la technologie de réseaux sans fil (Wi-Fi)

MSSS-DIR09

Votre gouvernement

Ministère de la Santé et des Services sociaux
Québec

Table des matières

Préambule

L'exploitation de la technologie des réseaux sans fil (Wi-Fi) fait de plus en plus partie intégrante de la prestation de services dans le domaine de la santé et des services sociaux. Elle permet notamment de répondre à certains besoins :

- **mobilité** de la clientèle en établissement (salles d'attente, familles, visiteurs, soins de courte durée, etc.);
- **mobilité** du personnel, notamment pour l'accès aux actifs informationnels du MSSS et du RSSS;
- utilisation de la **technologie biomédicale** par les professionnels de la santé (électrocardiographe, glucomètre intelligent, armoires à narcotiques, robot pharmacie, etc.);
- utilisation des **technologies de sécurité** des lieux et des personnes (vidéosurveillance, accès aux locaux, bouton d'alarme-agression, etc.);
- exploitation des **technologies du bâtiment** (chauffage, ventilation, ascenseurs, purification d'eau, etc.).

Étant donné sa nature, le Wi-Fi s'avère plus vulnérable qu'un réseau filaire, car ses signaux peuvent se propager à l'extérieur des limites d'une organisation. Étant donné qu'ils doivent être aussi sécuritaires que les réseaux filaires, leur implantation et leur exploitation constituent un enjeu de sécurité dont il faut tenir compte afin de favoriser la disponibilité, l'intégrité et la confidentialité de l'information qui y circule.

Cette directive est complétée par le document Exigences Wi-Fi qui précise les éléments de nature plus technique favorisant la mise en œuvre de cette directive.

Objectifs

Cette directive vise à :

- encadrer l'implantation et l'exploitation des réseaux Wi-Fi afin qu'ils comportent le même niveau de sécurité que celui des réseaux filaires;
- définir les rôles et responsabilités en la matière;
- fournir une assise sur laquelle les CSIO peuvent s'appuyer afin de s'assurer que leurs réseaux Wi-Fi respectent les obligations de la présente directive.

Champs d'application et portée

Cette directive s'applique aux entités suivantes :

- au ministère de la Santé et des Services sociaux (MSSS);
- aux organismes publics visés au paragraphe 5 de l'article 2 de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G 1.03)*, ci-après appelés « établissement et organismes », ci-après appelés RSSS.

Elle englobe toute information détenue par ces organisations, indépendamment de son format ou du support sur lequel elle se trouve (papier, enregistrement sonore ou vidéo, données électroniques ou numériques, etc.) et qui est en lien avec la technologie Wi-Fi.

Cadre légal et administratif

Cette directive fait partie du cadre de gouvernance du MSSS et s'y inscrit, sans s'y limiter, en conformité avec :

- la politique provinciale de la sécurité de l'information - MSSS-POL01;
- le cadre provincial de gestion de la sécurité de l'information - MSSS-CDG01;
- la directive sur la cybersécurité - MSSS-DIR03;
- la règle particulière sur la sécurité organisationnelle.

Obligations

1. Étude de site (« site survey »)

L'étude de site consiste à cartographier les plans des bâtiments ou des étages afin de déterminer l'emplacement optimal des capteurs et des points d'accès dans l'installation.

La planification adéquate de la conception d'un réseau Wi-Fi permettra de bien comprendre :

- l'environnement dans son ensemble;
- la façon dont les ondes se propageront.

Elle permettra également de vérifier l'impact de l'ajout d'un ou de plusieurs points d'accès à l'intérieur d'un réseau déjà existant, ceci afin que cette modification permette de conserver le même niveau de sécurité.

2. Analyse des risques liés à la sécurité de l'information

Une telle analyse doit être menée si l'information qui circulera sur le réseau Wi-Fi est catégorisée à 3 ou à 4 pour au moins l'un des volets suivants : disponibilité, intégrité ou confidentialité.

3. Séparation (ou segmentation)

Chaque réseau Wi-Fi doit être séparé en fonction du contexte dans lequel il est exploité : visiteurs, recherche, CHSLD, travailleur, hors mission, soins à domicile, etc.

4. Connexion d'un dispositif

Un dispositif ne doit être branché qu'à un seul réseau à la fois (soit filaire ou soit sans fil).

5. Protection des données

Les données sensibles qui circulent sur le réseau Wi-Fi (en transit) doivent être protégées en tout temps, par un chiffrement par exemple.

6. Micrologiciels des points d'accès

Les correctifs et les mises à jour des micrologiciel des points d'accès doivent être testés et déployés sur une base régulière.[1]

7. Cartographie (inventaire)

La cartographie du réseau doit être mise à jour sur une base périodique et inclure :

- les points d'accès;
- les dispositifs connectés.

8. Gestion des interférences[2]

La mise en place d'un réseau Wi-Fi doit tenir compte de la nécessité d'éviter les interférences électromagnétiques avec :

- tout autre équipement électronique (médical, téléphonique, domestique, etc.);
- d'autres réseaux déjà existants dans l'organisation.

9. Propagation du signal

Les signaux Wi-Fi peuvent se propager à l'extérieur des limites de l'organisation, ce qui offre aux personnes malveillantes la possibilité de balayer les ondes générées par le Wi-Fi ou d'y obtenir un accès non autorisé. Le réseau Wi-Fi doit donc limiter la propagation du signal au minimum.

10. Surveillance

Le réseau Wi-Fi fait partie intégrante des actifs informationnels. À ce titre, son utilisation doit être surveillée dans le respect des exigences gouvernementales et ministérielles en vigueur.

Obligations des principaux intervenants

Cette section énonce les rôles et responsabilités des principaux intervenants qui doivent participer au déploiement et à l'exploitation d'un réseau Wi-Fi, en complément aux responsabilités déjà incluses dans les documents de la section « *Cadre légal et administratif* ».

Chef délégué de la sécurité de l'information (CDSI)

Le CDSI s'assure de la cohérence des dispositions de la présente directive au regard des exigences gouvernementales et ministérielles.

[1] Conformément au processus gouvernemental de gestion des menaces, des vulnérabilités et des incidents (GMVI).

[2] Les interférences de radiofréquences, également appelées « bruit » du réseau sans fil, peuvent être causées par des appareils électroniques. Bien que certains réseaux soient très puissants et fiables, des appareils électroniques risquent malgré tout d'interférer avec leur signal.

Chef de la sécurité de l'information organisationnelle principal (CSIO)

Le CSIO principal a comme responsabilité :

- d'élaborer et de diffuser la présente directive;
- de soutenir les CSIO afin qu'ils puissent mettre en œuvre et exploiter des réseaux Wi-Fi qui répondent adéquatement aux obligations de cette directive.

Chef de la sécurité de l'information organisationnelle (CSIO)

Le CSIO est responsable du respect de la présente directive dans son organisation. À ce titre, il doit :

- s'assurer de la prise en charge des obligations qui y sont précisées pour tout projet de déploiement ou de modification d'un réseau Wi-Fi;
- voir à mettre en place une veille sur les menaces spécifiques au Wi-Fi;
- s'assurer de la mise à jour en continue de la cartographie de ce réseau.

Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

Le COMSI s'assure de la mise en place effective et de l'adéquation des mesures de protection des installations Wi-Fi, notamment celles :

- recommandées par le ROCD (gouvernementales et ministérielles) ou par le Centre opérationnel de sécurité (COS);
- provenant de la gestion des menaces, des balayages de vulnérabilité, etc.;
- concernant la mise à jour les micrologiciels des points d'accès.

Il s'assure de plus d'intégrer le Wi-Fi à la surveillance et de tenir à jour la cartographie (inventaire) du réseau.

Entrée en vigueur et révision

Cette directive entre en vigueur à la date de son approbation. Elle doit être révisée :

- tous les trois ans;

  ou

- lors de changements organisationnels ou de l'adoption de nouvelles orientations ministérielles en la matière.

Approuvée par le chef délégué de la sécurité de l'information (CDSI) :	Reno Bernier
Date d'approbation :	13 avril 2023