Titre :	**Mise en place et exploitation de la technologie Sans fil (Wi-fi)**		
État :	Approuvé	Effective à partir de :	2023-03-10
		Dernière mise à jour :	2023-03-10

Type :	Exigences		
Code du document :	MSSS-EXI-005	Portée :	MSSS et RSSS
Mots clés :	Sans fil; Wi-fi; Exploitation; Mise en place		

Déclaration :	**Séparer les réseaux Sans fil**
Précisions :	
L'organisation doit séparer physiquement ou logiquement ses réseaux sans fil spécifiques et leur octroyer des noms différents. Cette séparation doit se faire en divisant le trafic de données en différents segments, isolés les uns des autres. Cela exige donc que les équipements Wi-Fi permettent de configurer plusieurs noms de réseau (Service Set identifier (SSID)). Ces équipements doivent être configurés de façon à mettre en place des paramètres qui restreignent le trafic entre les SSID ou les différents segments du réseau.	
Justification :	La séparation des réseaux sans fil contribue à la confidentialité des flux entre les terminaux connectés. Les appareils isolés en fonction du réseau sans fil utilisé permettent une meilleure gestion et le contrôle de ce qui est connecté. Cette séparation contribue à un meilleur partage des ressources, comme sécuriser les systèmes contenant des données sensibles. Cette pratique est une des mesures de mitigation pour contrôler et sécuriser l'information qui y circule, pour protéger les systèmes sensibles, pour améliorer les performances du réseau et pour appliquer une gestion des accès adéquate.
Lien avec :	MSSS-DIR09 - Directive d'utilisation de la technologie sans fil

Déclaration :	**Protéger les données transmises par les réseaux sans fil**
Précisions :	

• Utiliser le plus haut niveau de chiffrement possible pour les protocoles de sécurité sans fil.
• S'assurer que les équipements de réseau sans fil prennent en charge les algorithmes de chiffrement robuste.
• Déployer selon le minimal obligatoire du 802.1x, avec mécanismes d'authentification EAP-TLS et EAP-TTLS.
• **Accès non critique** : déploiement minimal du protocole WPA2 qui génère les clés au moyen du protocole AES (802.11i).
  ○ Favoriser le WPA3 lorsque possible.
• **Accès aux données sensibles** : déployer une infrastructure de certificats d'entreprise.
  ○ Voir modèle d'architecture spécifique	

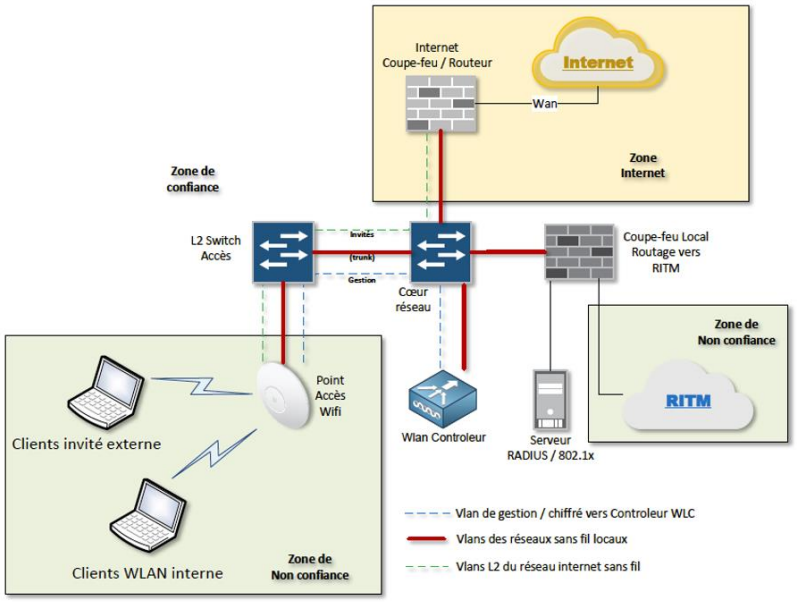
Justification :	Certains réseaux sans fil sont utilisés pour des besoins de mission qui impliquent des actifs informationnels comportant des informations sensibles. L'organisation doit protéger les données en transit sur les ondes des radios fréquences (RF).

Déclaration :	Utiliser un modèle d'architecture spécifique

Précisions :

Tous les réseaux sans fil doivent être installés sur un modèle d'architecture qui possède minimalement les caractéristique suivantes :

- le réseau invité et de gestion doivent être isolés de la zone de confiance;
- tout trafic qui circule sur le réseau Wi-Fi invité doit demeurer local (hors réseau RITM) avant d'accéder à un fournisseur Internet;
- utiliser le protocole 802.1x afin de protéger les données qui circulent sur ce réseau.



Déclaration :	**Disposer d'outils de prévention et de détection pour les composantes du réseau sans fil**
Précisions :	
Des systèmes de détection et prévention d'intrusion sans fil WIDS* et WIPS** doivent être incorporés au système sans fil. * (Wireless Intrusion Detection System) **(Wireless Intrusion Prevention System)	
Justification :	La liste suivante identifie quelques menaces de la technologie sans fil : • Point d'accès indésirable et Rogue accès point • Découverte et cartographie des AP (War-driving) • KRACK • Déni de services • Evil Twin (AP espion) Afin de prévenir ces attaques, les WIPS sont utilisés. Ce sont des systèmes permettant l'écoute radio et la reconnaissance de modèles d'attaques afin d'alerter l'administrateur du système de la menace. Les systèmes WIDS sont conçus pour détecter et atténuer les attaques actives qui sont menées en exploitant des radios fréquences (RF) émises.

Déclaration :	**Implanter un système de supervision et de surveillance du réseau sans fil**
Précisions :	
• Tout réseau sans fil doit être surveillé en temps réel par un système ayant des fonctionnalités intégrées d'interrogation sans fil et de surveillance du réseau. • Les équipements sans fil doivent pouvoir être surveillés par un système de gestion centralisé (ex. : SIEM). Une personne ou un groupe de personnes doivent être désignés pour réaliser cette tâche. • Les appels d'offres visant à se doter d'un réseau Wi-Fi doivent inclure une clause prévoyant des audits de sécurité.	

Déclaration :	**Gérer les accès au réseau sans fil**
Précisions :	
• Appliquer le principe du moindre privilège. • Déployer un outil de gestion d'identité du réseau sans fil et l'intégrer dans le processus de contrôle d'accès. • Des politiques d'accès utilisateurs et des appareils doivent être indiqués clairement et spécifiés pour chaque contexte d'utilisation (invité, biomédical, technologie de sécurité des bâtiments, etc.). • Masquer le SSID corporatif. • La politique de filtrage Web de l'organisation doit s'appliquer. • Tout accès d'un utilisateur invité doit être unique, authentifiable, révocable et avoir une durée d'utilisation limitée.	
Justification :	Le MSSS et le RSSS qui ont des aires d'attente ou des lieux susceptibles de recevoir des citoyens doivent mettre en place des services de réseau sans fil sécuritaires de type public avec accès à Internet seulement.
Lien avec :	• MSSS-EXI-001 Accès réseau confiance zéro (ZTNA)

Déclaration :	**L'utilisation obligatoire d'un portail captif pour l'accès au réseau sans fil par la population**
Précisions :	
• Utiliser un portail captif pour les utilisateurs invités qui visitent les sites des ministères et organismes du gouvernement (établissement de santé en tant que visiteur ou séjour de courte durée). • Doter le portail captif d'une validation des conditions d'utilisation avant que l'utilisateur ne puisse accéder au réseau.	
Lien avec :	• L'architecture d'entreprise gouvernementale (AEG), version 3.3, SCT 2018

Déclaration :	**Gestion du système de réseau sans fil**
Précisions :	
• Gérer le réseau sans fil sur un réseau dédié et sécurisé tout au long du cycle de vie du réseau avec un protocole de chiffrement sécuritaire. • Limiter et contrôler les accès au système de type administrateur. • Former les ressources TI sur la gestion et l'exploitation de ce système.	
Justification :	L'administration d'un point d'accès sans fil doit être réalisée depuis le réseau filaire, de préférence à partir d'un réseau d'administration logiquement séparé et en utilisant exclusivement des protocoles sécurisés.

Déclaration :	**Développer des processus d'audit de sécurité sans fil**
Précisions :	
• Auditer périodiquement l'environnement du réseau sans fil. • Sécuriser adéquatement le serveur d'audit afin de protéger l'intégrité des données d'audit précédemment enregistrées. • S'assurer que les événements d'audit incluent, au minimum, les tentatives d'authentification et de connexion, que ces tentatives soient réussies ou non.	
Justification :	L'élaboration d'un processus d'audit sur le réseau sans fil permettra de : • s'assurer que l'organisation a respecté les exigences de sécurité; • détecter les comportements non autorisés et les failles de sécurité. Les points d'accès et les systèmes d'accès doivent envoyer des données d'événement à un serveur d'audit sécurisé en temps réel, afin que l'intégrité des données soit garantie.

Déclaration :	Implémenter la journalisation des accès au système sans fil
Précisions :	
• Mettre en place de la journalisation afin d'assurer une traçabilité des accès des utilisateurs habilités à accéder au Wi-Fi. • La journalisation doit être conservée dans le respect des exigences gouvernementales pour fins de monitoring et d'enquête.	

Déclaration :	Couverture des réseaux sans fil
Précisions :	
• Faire une analyse de site (site survey) préalable au déploiement et la mettre à jour périodiquement. • Rendre disponibles des services de réseau sans fil à l'ensemble du personnel, en s'assurant du respect des zones de couverture qui doivent être circonscrites aux espaces de travail.	
Justification :	Le réseau Wi-Fi doit limiter la propagation du signal afin qu'il ne dépasse pas les limites de contrôle physique des installations de l'organisation. L'analyse de site permet notamment de planifier le déploiement du réseau, de prévoir les comportements des ondes RF pour le site accueillant ce réseau et de mieux comprendre la façon dont les ondes se propageront en validant les points suivants : • la réflexion (onde rebondie); • la réfraction (vapeur d'eau, pression d'air, température); • le dispersement (ex. : une boule disco); • la diffraction (ex. : une vague qui frappe un rocher); • l'absorption (matériaux qui absorbent l'énergie); • la distance. Le positionnement des points d'accès pour une couverture optimale afin de répondre aux besoins des utilisateurs et des secteurs d'activité. Il est primordial d'offrir une couverture adéquate et sécuritaire dans l'ensemble des édifices afin que les employés puissent collaborer aisément avec leurs pairs.

Déclaration :	Filtrage Web pour le réseau hors mission
Précisions :	
Le réseau sans fil hors mission doit être intégré à l'outil de filtrage Web afin de bloquer l'accès du personnel et des invités aux sites web dont la consultation est interdite aux mineurs, ou dont le contenu est illégal ou malicieux.	

Déclaration :	**Sécurité physique des composantes sans fil**
Précisions :	
Les points d'accès doivent être situés dans des zones physiquement sécurisées pour empêcher le vol de matériel ou toute intrusion.	

Déclaration :	**Installation et configuration d'un point d'accès Wi-Fi**
Précisions :	
Une procédure d'installation et de sécurisation des points d'accès doit être élaborée et mise en œuvre à chaque installation d'un nouvel équipement d'accès. Seul le personnel désigné par le Coordonnateur organisationnel des mesures de sécurité (COMSI) ou les administrateurs des réseaux informatiques peuvent mettre en place et gérer un tel point d'accès. Des contrôles doivent être menés régulièrement pour s'assurer que les réseaux informatiques de l'organisation n'accueillent pas de bornes Wi-Fi non gérées (bornes « pirates »). Le certificat du serveur qui est présenté par le point d'accès Wi-Fi configuré en WPA2-Entreprise doit être signé par une autorité de certification de confiance reconnue par les postes clients.	