

**Consignes de sécurité**

**Mise en place d’un WiFi**

**Sécurité de l’information**

**Informations générales**

Version : 0.7

État document : Draft

Classification : Publique

Sujet traité : Mise en place d’un WiFi

Document : Consignes de sécurité – Sécurité de l’information

Date : 11/12/2019

Représentant :

Table des matières

[1 Avertissement relatif aux conseils et consignes de sécurité de ce document 2](#_Toc334688850)

[2 Consignes de sécurité pour l’implémentation d’un Wifi 3](#_Toc334688851)

[2.1 Risques identifiés 3](#_Toc334688852)

[2.2 Réduction de l’exposition aux risques 3](#_Toc334688853)

[2.2.1 Responsabiliser l’utilisateur 3](#_Toc334688854)

[2.2.2 Nom du point d’accès et procédure de connexion 5](#_Toc334688855)

[2.2.3 Dissocier les réseaux et protéger son propre réseau interne 5](#_Toc334688856)

[2.2.4 Réduire le service au minimum de sa raison d’être 5](#_Toc334688857)

[2.2.5 Réduire les ayants droit au service 6](#_Toc334688858)

[2.2.6 Contrôler les accès logique et physique à la borne Wifi 6](#_Toc334688859)

[2.2.7 Ajouter toutes les protections supplémentaires et nécessaires 6](#_Toc334688860)

[2.2.8 Chiffrer les transmissions Wifi 6](#_Toc334688861)

# Avertissement relatif aux conseils et consignes de sécurité de ce document

Les consignes et propositions incluses dans ce document ont été réalisées de bonne foi et par des experts travaillant en relation avec la plateforme « [www.nc3.lu](http://www.nc3.lu) ». Toutefois, ces consignes ne sauraient se substituer à une analyse circonstentielle et critique issue d’un cabinet de conseil juridique. La mise en œuvre des conseils inclus dans ce document constitue une première étape de sécurisation, mais elle n’est pas forcément suffisante. Quoi qu’il en soit, la diversité des cas d’application (ainsi que leur mise en œuvre) des conseils inclus dans ce document ne peut entraîner la responsabilité de leur auteur.



# Consignes de sécurité pour l’implémentation d’un Wifi

Dans le cadre de services associés à vos activités, vous offrez gratuitement et/ou librement un accès à Internet à vos clients ou à vos usagers via la technologie sans fil (WiFi).

Des utilisateurs vont se connecter à Internet, via une infrastructure dont vous avez la gestion, il y a donc des risques associés qui entraînent votre responsabilité, il s’agit donc d’identifier ces risques.

## Risques identifiés

Les risques les plus probables sont les suivants :

1. Une personne utilise votre connectivité, donc votre identité pour perpétrer des délits avec l’aide d’outils informatiques. Exemple : Attaque de sites internet (accès aux données, mise hors servie), vols et manipulation d’information (déchargement illégal, atteinte aux droits d’auteur, contenus pédophiles, etc.).
2. Une personne est victime d’une attaque alors qu’elle utilise votre connectivité (vol de mot de passe ou d’information, infection virale).
3. Une personne malintentionnée utilise votre connectivité pour s’infiltrer dans votre réseau interne.

Ces différents risques peuvent avoir divers impacts, notamment :

* La dégradation de votre image ou de votre réputation.
* Des pertes financières dues à des poursuites juridiques incertaines en l’absence de jurisprudence.
* La perte de données, la divulgation d’informations confidentielles ou l’indisponibilité de services dont l’impact est difficilement quantifiable.

Note : Des risques spécifiques à votre contexte peuvent s’ajouter à la liste ci-dessus, vous devez vous même procéder à leur recherche pour pouvoir les traiter.

## Réduction de l’exposition aux risques

En mettant en œuvre de tels services, vous ne pouvez vous dégager de toutes responsabilités. Vous pouvez toutefois réduire votre exposition aux risques.

La première étape consiste en une réflexion relative à la raison d’être du service : quels sont les usages que vous souhaitez autoriser ? Veuillez noter que l’environnement va fortement impacter la réponse à cette question fondamentale (proximité ou non d’une école, …).

Les conseils suivants constituent plusieurs pistes pour vous permettre de gérer au mieux votre exposition aux risques.

### Responsabiliser l’utilisateur

#### Généralité

Il est conseillé de demander à l’utilisateur de valider une page qui l’informe formellement de ses droits, risques et interdits. Ce sont les « Conditions générales d'utilisation (CGU) ». Voir ci-dessous un exemple de CGU.

#### Exemple de Conditions générales d'utilisation (CGU)

**[**

Vous êtes sur le point d'accéder à Internet via un réseau d'accès Internet sans fil (le «Service») exploité par **XXXXXXXX**. La finalité du service est de fournir un accès public gratuit à Internet sans fil aux visiteurs de **XXXXXXXX**. Vous pouvez utiliser le Service uniquement si vous acceptez les conditions suivantes du service, et ce chaque fois que vous y accédez.

Conditions générales d'utilisation (CGU)

L'accès au réseau WiFi.

Le Service est gratuit et fourni par **XXXXXXXX**. Votre accès au Service est entièrement à la discrétion de **XXXXXXXX**, et votre accès au Service peut être bloqué, suspendu ou résilié à tout moment pour n'importe quelle raison, y compris, mais sans limitation, la violation du présent Accord, ou toute action pouvant entraîner une responsabilité pour **XXXXXXXX**, telles que (mais non limitativement), la perturbation de l'accès à d'autres utilisateurs ou réseaux, ou toute violation des lois ou règlements applicables. **XXXXXXXX** peut réviser les conditions d'utilisation à tout moment. Vous devez accepter cet accord, et ce à chaque fois que vous utilisez le Service et il est de votre responsabilité de le revoir pour tout changement à chaque fois. Il s'agit d'un réseau sans fil ouvert, et de ce fait, vous reconnaissez qu'aucune communication réseau par ce biais ne peut être totalement sécurisée.

En utilisant le Service, vous acceptez que l'ensemble de vos communications sur le réseau ne soient PAS considérées comme privées ou protégées. Toutes les communications via le Service sont potentiellement soumises à une surveillance, et ce afin de protéger et sécuriser le Service. **XXXXXXXX** se réserve le droit de réduire le débit ou l'accès tant que de besoins. STRICTEMENT DANS CETTE FINALITÉ DE PROTECTION DU SERVICE, ET EN UTILISANT CE SERVICE, VOUS AUTORISEZ **XXXXXXXX** À ÉTUDIER TOUS LES LOGS ET INFORMATIONS DE CONNEXION ET D'USAGE SE RATTACHANT A VOTRE USAGE DU SERVICE.

Règles d'utilisation acceptable du Service.

Votre utilisation du Service et toute autre activité réalisée en ligne par l'intermédiaire du Service ne doivent violer aucune loi ou réglementation applicable. **XXXXXXXX** ne peut accepter aucune responsabilité pour tout dommage ou perte découlant de contenus inexacts, inappropriés, offensants ou autres auxquels vous auriez eu accès via le Service.

Avertissement.

Vous reconnaissez (i) que le service peut ne pas être ininterrompu ou sans erreur (ii) que des virus ou d'autres applications nuisibles peuvent être téléchargées à votre insu via le Service (il est de votre responsabilité de vous protéger via les logiciels adéquats), et plus généralement (iii) que **XXXXXXXX** ne garantit pas la sécurité du Service.

LE SERVICE EST FOURNI TEL QUEL, selon la disponibilité et SANS GARANTIE D'AUCUNE SORTE.

Pas de dommages indirects.

EN AUCUN CAS **XXXXXXXX**, ses fournisseurs ou concédants, OU LEURS DIRIGEANTS, ADMINISTRATEURS, EMPLOYÉS, AGENTS ET AFFILIES NE SERONT TENUS RESPONSABLES DE DOMMAGES CONSÉCUTIFS, OU INDIRECTS ISSUS DE l'USAGE DE CE SERVICE.

L'UTILISATION DU SERVICE POUR LES ACTIVITÉS SUIVANTES EST INTERDITE:

Le spam et l'invasion de la vie privée d'autrui.

La violation du droit de la propriété intellectuelle.

La transmission de contenus obscènes, indécents, diffamatoires, injurieux ou racistes.

La distribution de virus Internet, vers, chevaux de Troie ou toutes autres activités destructrices.

**]**

### Nom du point d’accès et procédure de connexion

Il est préférable de fournir une information accessible à tous les utilisateurs du service sur le nom du point d’accès (SSID), la zone géographique couverte et la procédure de connexion, ceci afin d’éviter que les utilisateurs ne se trompent de réseau.

Note : le spoofing de votre réseau ne peut pas être empêché.

### Dissocier les réseaux et protéger son propre réseau interne

Le point d’accès Wifi (public) ne doit en aucun cas donner un accès à votre réseau interne (privé). Vous devez mettre en place une architecture indépendante ou les moyens de protection nécessaire pour vous protéger (ce point fait partie des risques spécifiques que vous devez analyser vous-même).

### Réduire le service au minimum de sa raison d’être

Si le service consiste à mettre à disposition Internet et le courrier électronique, alors n’autorisez que les protocoles et ports correspondants (filtrer les FTP, peer2peer, jeux, paris en ligne, etc.).

Si l’accès n’est pas complètement ouvert, filtrer les accès par le biais de « black list » et/ou « White list » (une méthode parmi d’autres permettant la limitation des accès aux contenus illicites comme notamment les contenus pédopornographiques, racistes, révisionnistes couverts par les articles 384, 385bis et 454 du Code pénal).

### Réduire les ayants droit au service

Sauf, si vous voulez offrir un service à tout le monde sans restriction, vous devez gérer les accès à votre service de façon à ce que seuls les ayants droit puissent se connecter.

Dans le cas d’un accès limité, vous devez mettre en place une méthode de gestion des autorisations adéquates qui permet de contrôler la diffusion de la clé, son changement régulier ou son changement rapide en cas de suspicion de compromission.

### Contrôler les accès logique et physique à la borne Wifi

La puissance d’émission doit être réglée au minimum nécessaire de la zone de couverture que vous voulez adresser.

Le point d’accès doit être sécurisé de manière à ce qu’il ne puisse pas facilement être détourné par une personne malintentionnée (être transformé en point d’accès « rogue »). Le mot de passe administrateur doit être fort et gérer dans l’état de l’art (stockage et diffusion).

L’accès physique au matériel de gestion du Wifi doit être contrôlé pour éviter la manipulation frauduleuse de la configuration.

### Ajouter toutes les protections supplémentaires et nécessaires

Selon le service mis à disposition, des dispositifs spécifiques peuvent être ajoutés pour scanner les pages Web et fichiers transmis afin de détecter les virus ou malwares éventuels.

### Chiffrer les transmissions Wifi

Les transmissions Wifi doivent être chiffrées, de minimum en WPA2.