

**Safety instructions**

**Setting up an accessible WiFi**

**Information security**

**Informations générales**

Version: 0.7

Document state: Draft

Classification: Public

Subject: Setting up an accessible WiFi

Document: Safety instructions - Information security

Date: 08/04/2019

Representative:

Table of Contents

[1 Warning for the advice and safety instructions in this document 2](#_Toc26775224)

[2 Safety instructions for implementing a Wifi 3](#_Toc26775225)

[2.1 Identified risks 3](#_Toc26775226)

[2.2 Reduction of risk exposure 3](#_Toc26775227)

[2.2.1 Empower the user 3](#_Toc26775228)

[2.2.2 Access point name and connection procedure 5](#_Toc26775229)

[2.2.3 Dissociate networks and protect one's own internal network 5](#_Toc26775230)

[2.2.4 Reduce the service to the minimum required 5](#_Toc26775231)

[2.2.5 Reducing the beneficiaries of the service 5](#_Toc26775232)

[2.2.6 Controlling logical and physical access to the Wifi terminal 6](#_Toc26775233)

[2.2.7 Add all additional and necessary protections 6](#_Toc26775234)

[2.2.8 Encrypting Wifi transmissions 6](#_Toc26775235)

# Warning for the advice and safety instructions in this document

The instructions and proposals included in this document were made in good faith and by experts working in connection with the "www.nc3.lu" platform. However, these instructions cannot replace a cautious and critical analysis from a law firm. The implementation of the advice included in this document is a first step of security, but it is not necessarily sufficient. In any case, the diversity of the application cases (as well as their implementation) of the advice included in this document cannot entail the responsibility of their author.



# Safety instructions for implementing a Wifi

As part of services associated with your activities, you offer free and / or open Internet access to your customers or users via wireless technology (WiFi).

Users will connect to the Internet, through an infrastructure that you manage, so there are associated risks that lead to your liability, so it is about identifying those risks.

## Identified risks

The most likely risks are:

1. A person uses your connectivity, so your identity to perpetrate crimes with the help of computer tools. Example: Attack of websites (access to data, disablement), theft and manipulation of information (unlawful copying, infringement of copyrights, paedophile content, etc.).
2. A person is attacked while using your connectivity (password or information theft, virus infection).
3. A malicious person uses your connectivity to infiltrate your internal network

These different risks can have various impacts, including:

* The degradation of your image or your reputation.
* Financial losses due to uncertain legal proceedings in the absence of jurisprudence.
* The loss of data, the disclosure of confidential information or the unavailability of services whose impact is difficult to quantify.

Note: Risks specific to your context may be added to the list above; you must even search for them before you are able to treat them.

## Reduction of risk exposure

By implementing such services, you cannot relieve yourself of all responsibilities. You can, however, reduce your risk exposure.

The first step is a reflection on the purpose of the service: what are the use cases that you want to allow? Please note that the environment will strongly impact the answer to this fundamental question (ex. proximity or not of a school, ...).

The following tips are several ways to help you better manage your risk exposure.

### Empower the user

#### In General

It is advisable to ask the user to validate a page which informs him formally of his rights, risks and prohibited. These are the "Terms of Use (ToU)". See below for an example of a UGC.

#### Example of General Terms of Use (ToU)

**[**

You are about to access the Internet via a wireless Internet access network (the "Service") operated by XXXXXXXX. The purpose of the service is to provide free public wireless internet access to XXXXXXXX visitors. You may use the Service only if you agree to the following terms of service each time you access it.

General conditions of use (GCU)

Access to the WiFi network.

The Service is free and provided by XXXXXXXX. Your access to the Service is entirely at the discretion of XXXXXXXX, and your access to the Service may be blocked, suspended or terminated at any time for any reason, including, but not limited to, breach of this Agreement, or any action may result in liability for XXXXXXXX, such as (but not limited to) disruption of access to other users or networks, or any violation of applicable laws or regulations. XXXXXXXX may revise the terms of use at any time. You must accept them agreement each time you use the Service. It is your responsibility to review them each time you connect to confirm that you accept even if changes have occurred. This is an open wireless network, so you recognize that no network communication through this network can be completely secure.

By using the Service, you agree that all your communications on the network are NOT considered private or protected. All communications via the Service are potentially subject to surveillance in order to protect and secure the Service. XXXXXXXX reserves the right to reduce throughput or access as needed. STRICTLY IN THIS SERVICE PROTECTION PURPOSE, AND BY USING THIS SERVICE, YOU AUTHORIZE XXXXXXXX TO STUDY ALL LOGS AND CONNECTION INFORMATION IN RELATION OF YOUR USE OF THE SERVICE.

Rules of acceptable use of the Service.

Your use of the Service and any other activity performed online through the Service shall not violate any applicable law or regulation. XXXXXXXX can not accept any responsibility for any damage or loss arising from inaccurate, inappropriate, offensive or other content to which you would have accessed via the Service.

Warning.

You acknowledge (i) that the service may not be uninterrupted or error free (ii) that viruses or other harmful applications may be downloaded without your knowledge via the Service (it is your responsibility to protect yourself via the appropriate software ), and more generally (iii) that XXXXXXXX does not guarantee the security of the Service.

THE SERVICE IS PROVIDED AS IS, AS AVAILABLE AND WITHOUT WARRANTY OF ANY KIND.

No indirect damage.

IN NO EVENT SHALL XXXXXXXX, its suppliers or licensors, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, AND AFFILIATES, BE LIABLE FOR ANY CONSEQUENTIAL OR INCIDENTAL DAMAGES RESULTING FROM THE USE OF THIS SERVICE.

USE OF THE SERVICE FOR THE FOLLOWING ACTIVITIES IS PROHIBITED:

Spam and invasion of the privacy of others.

Infringement of intellectual property rights.

The transmission of obscene, indecent, defamatory, abusive or racist content.

The distribution of Internet viruses, worms, Trojan horses or any other destructive activities.

**]**

### Access point name and connection procedure

It is preferable to provide information accessible to all users of the service on the access point name (SSID), the geographical area covered and the connection procedure, in order to prevent users from mistakenly connect to the wrong network.

Note: The spoofing of your network cannot be prevented.

### Dissociate networks and protect one's own internal network

The Wifi point (public) must not give access to your internal network (private). You need to put in place an independent architecture or the means of protection necessary to protect yourself (this point is one of the specific risks that you have to analyse yourself).

### Reduce the service to the minimum required

If the service is to provide Internet and email, then only allow the corresponding protocols and ports (filter FTP, peer2peer, games, online betting, etc.).

If the access is not completely open, filter the accesses through "black list" and / or "White list" (one method among others allowing the limitation of the accesses to the illicit contents like in particular the paedopornographic contents, racists, revisionists covered by Articles 384, 385bis and 454 of the Criminal Code).

### Reducing the beneficiaries of the service

Except, if you want to offer a service to everyone without restriction, you must manage access to your service so that only rights holders can connect.

In the case of limited access, you must implement an appropriate authorization management method that allows you to control the distribution of the key, its regular change or its rapid change in case of suspicion of compromise.

### Controlling logical and physical access to the Wifi terminal

The transmit power must be set to the minimum necessary for the coverage area you want to address.

The access point must be secure so that it cannot easily be hijacked by a malicious person (ex. transformed into a "rogue" access point). The administrator password must be strong and managed respecting the state of the art (storage and distribution).

Physical access to Wifi management equipment must be controlled to prevent fraudulent manipulation of the configuration.

### Add all additional and necessary protections

Depending on the service provided, specific devices can be added to scan Web pages and transmitted files to detect possible viruses or malware.

### Encrypting Wifi transmissions

Wifi transmissions must be encrypted, using WPA2 as a minimum.