SOFTWARE SECURITY INFORMATION

FCC ID: PNB-LB1ZM
IC: 3919A- LB1ZM

Pursuant to:
FCC Part 15E 15.407(I) and KDB 594280 D02 UNII Device Security v01r03 / IC RSS-247 issue 2 article 6.4(4).

The information within this section is to show compliance against the SW Security Requirements laid out within KDB 594280 D02 U-NII Device Security v01r03. The information below describes how to maintain the overall security measures and systems so that only:

1. **Authenticated software is loaded and operating on the device.**
2. **The device is not easily modified to operate with RF parameters outside of the authorization.**

SOFTWARE SECURITY DESCRIPTION		
	Requirement	**Answer**
General Description	1. Describe how any software/firmware updates for elements than can affect the device's RF parameters will be obtained, downloaded, validated and installed. For software that is accessed through manufacturer's website or device's management system, describe the different levels of security as appropriate.	The RF parameters are stored in the Axis firmware which can be downloaded from Axis website. The device utilizes "secure boot", meaning that the entire Axis firmware is signed cryptographically with a key and the device cannot boot firmwares that are not signed by Axis.
	2. Describe the RF parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited such that any other software/firmware changes will not allow the device to exceed the authorized RF characteristics?	The RF parameters are tied to the country code which is set in factory. The Axis firmware uses the country code to load the correct RF parameters.
	3. Describe in detail the authentication protocols that are in place to ensure that the source of the RF-related software/firmware is valid. Describe in detail how the RF-related software is protected against modification.	The Axis firmware sets the RF parameters by loading a binary file that matches the country code set in factory. These binary files have been received from NXP and are included in the Axis firmware. The user cannot change them.
	4. Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware.	Only firmwares signed by Axis can be used on the device, see point 1.
	5. For a device that can be configured as a master and client (with active or passive scanning), explain how the device ensures compliance for each mode? In particular if the device acts as master in some band of operation and client in another; how is compliance ensured in each band of operation?	The device can act as master only on channels 1-11 in the 2.4GHz band. It can only act as client in 5GHz band. This behaviour is enforced by the Axis firmware and cannot be controlled by the user. It uses the same country code in master mode to ensure compliance.

	Requirement	Answer
Third Party Access Control	1. Explain if any third parties have the capability to operate a U.S./Canada - sold device on any other regulatory domain, frequencies, or in any manner that may allow the device to operate in violation of the device's authorization if activated in the U.S./Canada.	The regulatory domain is set in factory and cannot be controlled by any third parties.
	2. Describe, if the device permits third-party software or firmware installation, what mechanisms are provided by the manufacturer to permit integration of such functions while ensuring that the RF parameters of the device cannot be operated outside its authorization for operation in the U.S./Canada. In the description include what controls and/or agreements are in place with providers of third-party functionality to ensure the devices' underlying RF parameters are unchanged and how the manufacturer verifies the functionality.	It is not possible to install third-party software or firmware on the device.
	3. For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers fully comply with these software security requirements for U-NII devices. If the module is controlled through driver software loaded in the host, describe how the drivers are controlled and managed such that the modular transmitter RF parameters are not modified outside the grant of authorization.	Not applicable.

This section is required for devices which have a "User Interface" (UI) to configure the device in a manner that may impact the operational parameter. The operation description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 D01 v02r01

SOFTWARE CONFIGURATION DESCRIPTION		
	Requirement	**Answer**
ER CONFIGURATION GUIDE	1. Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences.	The device's UI does not support configuration of RF parameters.
	a) What parameters are viewable and configurable by different parties?	Not applicable.
	b) What parameters are accessible or modifiable by the professional installer or system integrators?	Not applicable.

	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?	Not applicable.
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S./Canada?	Not applicable.
	c) What parameters are accessible or modifiable by the end-user?	Not applicable.
	(1) Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized?	Not applicable.
	(2) What controls exist so that the user cannot operate the device outside its authorization in the U.S./Canada?	Not applicable.
	d) Is the country code factory set? Can it be changed in the UI?	The country code is set in factory and cannot be changed in the UI.
	(1) If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S./Canada?	Not applicable.
	e) What are the default parameters when the device is restarted?	The default parameters follow regulations in all countries, U.S. and Canada included.
	2. Can the radio be configured in bridge or mesh mode? If yes, an attestation may be required. Further information is available in KDB Publication 905462 D02.	No.
	3. For a device that can be configured as a master and client (with active or passive scanning), if this is user configurable, describe what controls exist, within the UI, to ensure compliance for each mode. If the device acts as a master in some bands and client in others, how is this configured to ensure compliance?	The device can act as master only on channels 1-11 in the 2.4GHz band. It can only act as client in 5GHz. This behaviour is enforced by the Axis firmware and cannot be controlled by the user. It uses the same country code in master mode to ensure compliance.
	4. For a device that can be configured as different types of access points, such as point-to-point or point-to-multipoint, and use different types of antennas, describe what controls exist to ensure compliance with applicable limits and the proper antenna is used for each mode of operation. (See Section 15.407(a)).	Not applicable.

Name and surname of applicant (or authorized representative):

_____

Date: _____ **Signature:** _____

Revision Record Sheet:

Revision	Section number	Page number	Date	Remark(s)	issued by
6		1	28-12-2022	History sheet added	WJJ

Issued/modified by : Willem Jan Jong
Function : Team Lead
Revision : 6
Date : 28-12-2022

Verified by : Axel Gase
Function : Quality Manager
Date : 28-12-2022

Released by : Axel Gase
Function : Manager Quality Assurance
Date of release: : 28-12-2022