NextFlex

NextFlex AirGuardian

Hardware Version: A25 Rev. A
Firmware Version: 1.4

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 0.4

Prepared for:	**Prepared by:**
NextFlex 2244 Blach Place, Suite 150 San Jose, CA, 95131 United States of America Phone: +1 408 797 2244 www.nextflex.us	**Corsec Security, Inc.** 13921 Park Center Road, Suite 460 Herndon, VA 20171 United States of America Phone: +1 703 267 6050 www.corsec.com

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the NextFlex AirGuardian from NextFlex. This Security Policy describes how the NextFlex AirGuardian meets the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S.[1] and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the Cryptographic Module Validation Program (CMVP) website, which is maintained by National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS).

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module. The NextFlex AirGuardian is referred to in this document as AirGuardian, crypto module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The NextFlex website (https://www.nextflex.us/) contains information on the full line of products from NextFlex.
- The search page on the CMVP[2] website (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search) can be used to locate and obtain vendor contact information for technical or sales-related questions about the module.

1.3 Document Organization

The Security Policy document is organized into two primary sections. Section 2 provides an overview of the validated module. This includes a general description of the capabilities and the use of cryptography, as well as a presentation of the validation level achieved in each applicable functional area of the FIPS standard. It also provides high-level descriptions of how the module meets FIPS requirements in each functional area. Section 3 documents the guidance needed for the secure use of the module, including initial setup instructions and management methods and policies.

[1] U.S. – United States

[2] CMVP – Cryptographic Module Validation Program

2. NextFlex AirGuardian

2.1 Overview

The NextFlex AirGuardian, or AirGuardian, provides real-time monitoring of health and safety metrics, as defined by the Occupational Safety and Health Administration (OSHA) for maintainers working in confined spaces. The AirGuardian (see Figure 1) employs a network of off-the-shelf physiological sensors with custom-designed flexible hybrid electronic (FHE) environmental sensors for monitoring oxygen levels, temperature, and humidity as the maintainer works. The sensor network is held in an armband and worn by the maintainer.

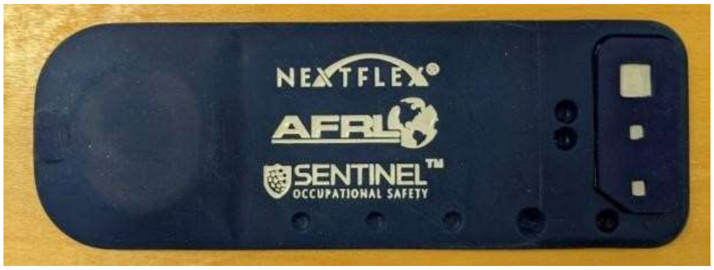

Figure 1 – NextFlex AirGuardian

The AirGuardian transmits this sensor data via Bluetooth Low Energy (BLE) connection to a paired smart device in the maintainer's possession that is monitored by attendants at remote locations. The module first secures the sensor data using 128-bit AES[3]-CTR[4] encryption prior to export. The module then exports the encrypted data over a BLE connection via an onboard nRF5280 Bluetooth SoC[5] developed by Nordic Semiconductor that provides both general processing (via a 32-bit ARM Cortex-M4 CPU[6]) and BLE service functionalities. The AES key is pre-loaded at the factory prior to module deployment.

The AirGuardian also includes LEDs[7] to warn the maintainer if unsafe conditions have been detected.

The AirGuardian is validated at the FIPS 140-2 Section levels shown in Table 1.

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	1

[3] AES – Advanced Encryption Standard
[4] CTR – Counter
[5] SoC – System on a Chip
[6] CPU – Central Processing Unit
[7] LED – Light Emitting Diode

Section	Section Title	Level
6	Operational Environment	N/A[8]
7	Cryptographic Key Management	1
8	EMI/EMC[9]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The AirGuardian is a hardware module with a multiple-chip standalone embodiment. The overall security level of the module is 1. The cryptographic boundary of the AirGuardian is defined by the physical enclosure of the device, which surrounds all hardware, software, and firmware components of the module.

2.2.1 Modes of Operation

When configured and operated according to the guidance provided in section 3.1, the module only supports an Approved mode of operation.

2.2.2 Algorithm Implementations

The module implements the FIPS-Approved algorithms listed in Table 2.

Table 2 – FIPS-Approved Algorithm Implementations

Certificate Number	Algorithm	Standard	Mode/Method	Key Lengths, Curves, or Moduli	Use
A2056	AES	FIPS PUB[10] 197	CTR	128	Encryption/decryption *Decryption is not used by the module.*

Additional algorithms are provided by the onboard Nordic SoC in support of the module's Bluetooth services. These algorithms are considered non-compliant (as they are untested by the CAVP[11]):

- AES-CCM[12] (non-compliant)
- AES-CMAC[13] (non-compliant)
- DRBG[14] (non-compliant)

[8] N/A – Not Applicable
[9] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[10] PUB – Publication
[11] CAVP – Cryptographic Algorithm Validation Program
[12] CCM – Counter with Cipher-block chaining Message Authentication Mode
[13] CMAC – Cipher-based Message Authentication Code

- Elliptic Curve Diffie-Hellman (non-compliant)
- Elliptic Curve Digital Signature Algorithm (non-compliant)
- HMAC[15] (non-compliant)
- SHA2[16]-256 (non-compliant)

Use of these non-compliant algorithms in the Approved mode of operation follows example scenario #2 from *FIPS 140-2 Implementation Guidance* (IG) section 1.23. Since the module uses its validated AES algorithm to encrypt all output data prior to the establishment of the Bluetooth connection, use of these algorithms to further secure the BLE communications is considered redundant; thus, no security is claimed on the functions that use these algorithms, and their use is allowed.

2.3 Module Interfaces

The module's design separates the physical connections into four logically distinct and isolated categories. They are as follows:

- Data Input
- Data Output
- Control Input
- Status Output
- Power Interface

The module monitors and collects data from the maintainer's environment using three sensors (humidity/temperature, oxygen, and gas). the module can export the collected data, send status output (in the form of error messages), and receive commands over the BLE connection to an application running on a paired smart device.

The module also includes the following LEDs:

- The Alert LED
- The Connect LED
- The Reserved LED (disabled)

Table 3 – AirGuardian LEDs

Physical Port/Interface	Quantity	Color	Action	Purpose
Alert LED	5	Red	Solid on	Unsafe condition detected
Connect LED	1	Red/Green/Blue	Blue	BLE advertisement initiated. Waiting on a connection
			Green	Connection established over BLE
			Red solid on	Self-test or integrity test fails
			Red two blinks	Fuel Gauge Initialization failure (start-up only)

[14] DRBG – Deterministic Random Bit Generator
[15] HMAC – Hash-based Message Authentication Code
[16] SHA – Secure Hash Algorithm

Physical Port/Interface	Quantity	Color	Action	Purpose
			Red three blinks	Gas Sensor Initialization failure (start-up only)
			Red four blinks	I2C[17] to SPI[18] Bridge initialization failure (start-up only)
			Red five blinks	ADC[19] initialization failure (start-up only)
Reserved LED	1	Green	N/A	Disabled

The physical interfaces for the AirGuardian are described in Table 4 below.

Table 4 – FIPS 140-2 Logical Interface Mappings

Physical Port/Interface	Quantity	FIPS 140-2 Interface
BLE Antenna	1	• Data Output • Control Input • Status Output
Humidity/Temperature Sensor	1	• Data Input
O2[20] Sensor	1	• Data Input
Gas Sensor	1	• Data Input
LED (Green)	1	• Reserved for future use
Connect LED (RGB)	1	• Status Output
Alert LED (Red)	5	• Status Output
Wireless Power Receiver	1	• Power Input

2.4 Roles, Services, and Authentication

The sections below describe the module's authorized roles, services, and operator authentication methods.

2.4.1 Authorized Roles

The module supports two roles in the module (as required by FIPS 140-2) that operators may assume: Cryptographic Officer (CO) role and User role. The module does not support multiple concurrent operators.

2.4.2 Operator Services

Descriptions of the services available are provided in Table 5 below. The module's services are invoked through commands sent from an application on the smart device. Please note that the keys and Critical Security Parameters (CSPs) listed in the table indicate the type of access required using the following notation:

[17] I2C – Inter-Integrated Circuit

[18] SPI – Serial Peripheral Interface

[19] ADC- Analog to digital converter

[20] O2 – Oxygen

- R – Read: The CSP is read.
- W – Write: The CSP is established, generated, or modified.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.
- Z – Zeroize: The CSP is zeroized.

Table 5 – Mapping of Module Services to Roles, CSPs, and Type of Access

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Reset MCU[21]	✓		Reset MCU. Can be used for on-demand self-tests	Command	Status	None
Read firmware version	✓		Read firmware version for: • module firmware • Nordic firmware • bootloader	Command	Status	None
Set sensor notify period	✓		Sets the number of seconds, between 1 – 255, between notifications from sensors	Command	None	None
Set sensor parameters	✓		Sets the following: • high current • PWM[22] duty cycle • Power mode (high, low, or off)	Command	None	None
Send sensor data		✓	Immediately send data from module sensors	Command	Response	Session Key – X
Read enumerated state status		✓	Read sensing state of module: • idle • sensing • locating	Command	Response	Session Key – X
Read power-up bit status		✓	Sensor status on startup	Command	Response	Session Key – X
Read continuous bit status		✓	Sensor status that runs continuously	Command	Response	Session Key - X
Read battery state of charge		✓	Read percent of charge remaining in battery	Command	Response	Session Key – X
Read temperature		✓	Read temperature in Fahrenheit from -500 to 500	Command	Response	Session Key – X

[21] MCU – Microcontroller Unit
[22] PWM – Pulse Width Modulation

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Read humidity		✓	Read humidity in g/m3[23] from 0 to 40	Command	Response	Session Key – X
Read oxygen level		✓	Read detected oxygen level in mg/l[24] from 1 to 20	Command	Response	Session Key – X
Read VOC[25] level		✓	Reads the detected VOC level in mg/l from 0 to 100	Command	Response	Session Key – X
Read LEL[26] level		✓	Reads detected LEL level	Command	Status	Session Key – X
AES status check	✓		Read status to verify successful power-up self-tests	Command	Status	Session Key – X
AES zeroize	✓		Zeroize the stored AES key	Command	None	Session Key – Z
Send AES toggle (Enable)	✓		Sets the encryption mode as on	Command	Status	Session Key – X
Boot-Soft	✓		Runs system check on boot and BLE stack	Command	Status	None
App CRC16 check	✓		Reads result of integrity test on firmware application	Command	Status	None

2.4.3 Authentication

The module does not support authentication mechanisms; operators implicitly assume their role based upon the service selected for execution.

2.5 Physical Security

The AirGuardian is a multiple-chip standalone cryptographic module. The module consists of production-grade enclosure and components that include standard passivation techniques.

[23] g/m^3 – grams per cubic meter
[24] mg/l – milligram per liter
[25] VOC – Volatile Organic Compounds
[26] LEL – Lower Explosive Limit

2.6 Operational Environment

The module employs a non-modifiable operating environment and therefore does not provide the module operator with access to a general-purpose operating system. The module's firmware executes on the 32-bit ARM Cortex-M4 CPU on the Nordic nRF5280 SoC. Only the module's image can be run on the device.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 6.

Table 6 – Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Session key	128-bit AES-CTR key	Pre-loaded at factory	Never output	Stored in plaintext in non-volatile memory	By Zeroization command	Encrypt sensor data prior to transmitting to paired smart device over BLE

2.8 EMI / EMC

The AirGuardian is classified as a radio and therefore, per FIPS 140-2 is excluded from all EMI/EMC requirements. The module was independently tested by TBD (accredited by the A2LA[27] under certificate number 0803.01) and was awarded FCC[28] ID[29] TBD.

2.9 Self-Tests

Cryptographic self-tests are performed by the module when the module is first powered up. The following sections list the self-tests performed by the module, their expected error status, and the error resolutions.

2.9.1 Power-Up Self-Tests

The AirGuardian performs the following self-tests at power-up:

- Firmware integrity check (16-bit CRC[30])
- AES-CTR encrypt KAT[31] (128-bit)

2.9.2 Conditional Self-Tests

No conditional self-tests or critical function tests are performed by the module.

2.9.3 Critical Functions Self-Tests

No critical function tests are performed by the module during power-up or conditionally.

2.9.4 Self-Test Failure Handling

If either power-up self-test fails, the module will enter a critical error state, and the Connect LED will turn on solid red to indicate the failure. While in this state, the module inhibits all data output from the BLE interface.

To recover from the error state, the module must be returned to NextFlex for further assistance.

2.10 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 Level 1 requirements for this validation.

[27] A2LA – American Association for Laboratory Accreditation
[28] FCC – Federal Communication Commission
[29] ID – Identification
[30] CRC – Cyclic Redundancy Check
[31] KAT – Known Answer Test

3. Secure Operation

The sections below describe how to place and keep the NextFlex AirGuardian in the FIPS-Approved mode of operation. **Operating the module without following the guidance herein (including the use of undocumented services) will result in non-compliant behavior and is outside the scope of this Security Policy**.

3.1 Module Setup

The module must be fully charged and placed into an armband sleeve. As soon as the module is powered on and completes the boot process and self-tests, a fast-advertising interval is started to make a connection to the maintainer's smart device. The Connect LED is lit blue during the advertisement. When the BLE connection is established, the Connect LED turns green. The smart device will report a "Connected" status while the BLE link is in operation. Once the connection is complete, the module enters an uninitialized state. From the uninitialized state, the module will initialize its environmental sensors and components to include:

- Fuel Gauge
- Gas sensor
- Humidity/Temperature sensor
- I^{2}C to SPI bridge
- ADC
- Oxygen sensor voltage

Once the sensor/component initialization is complete, the CO must immediately issue the "set encryption mode" command to enable encryption. Once encryption mode is enabled, the module is considered fully initialized and will be in FIPS mode of operation.

If any sensor or component fails to initialize, the Connect LED will blink red to indicate the failure. If this occurs, the module should not be put into use, and the CO should contact NextFlex.

3.2 Crypto Officer Guidance

The CO is responsible for ensuring that the module is operating in the FIPS-Approved mode of operation. The "set encryption mode" shall not be disabled while operating the module. Disabling this mode takes the module out of its approved mode of operation and will result in non-compliant behavior.

3.2.1 On-Demand Self-Tests

Both the firmware integrity test and the AES self-test can be run on demand using the "Reset MCU" command. This command will reset the MCU can cause the module to run through boot procedures and run self-tests. The "AES Status Check" can be used to query the status of a successful test. The module will enter an error state and the red Connect LED will turn on if a self-test fails.

3.2.2 Monitoring Status

At any point in time, the status of the module (i.e., FIPS mode status) can be determined by sending the “Read encryption mode” command via the paired smart device. This will return “1” if FIPS encryption is enabled or “0” if FIPS encryption is not enabled.

3.2.3 Zeroization

To zeroize the session key, the “Zeroize” command must be sent. Once the session key has been zeroized, the module is rendered inoperable and must be returned to NextFlex to load a new session key.

3.3 User Guidance

The User does not have the ability to modify configuration of the module but should notify the CO if any irregular activity is noted.

4. Acronyms and Abbreviations

Table 7 provides definitions for the acronyms and abbreviations used in this document.

Table 7 – Acronyms and Abbreviations

Acronym	Definition
A2LA	American Association for Laboratory Accreditation
AES	Advanced Encryption Standard
BLE	Bluetooth Low Energy
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CCM	Counter with Cipher-Block Chaining Message Authentication Code
CMAC	Cipher-Based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CO	Cryptographic Officer
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
CTR	Counter
DRBG	Deterministic Random Bit Generator
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
FHE	Flexible Hybrid Electronic
FIPS	Federal Information Processing Standard
g/m3	Grams per Cubic Meter
HMAC	Hash-based Message Authentication Code
ID	Identification
IG	Implementation Guidance
KAT	Known Answer Test
LED	Light Emitting Diode
MCU	Microcontroller Unit
mg/l	Milligram per Liter
NIST	National Institute of Standards and Technology

Acronym	Definition
N/A	Not Applicable
O2	Oxygen
OSHA	Occupational Safety and Health Administration
PUB	Publication
PWM	Pulse Width Modulation
SHA	Secure Hash Algorithm
SoC	System on a Chip
SP	Special Publication
U.S.	United States

Prepared by:
Corsec Security, Inc.

Corsec

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com