

# High Sec Labs FI11H-M, FI11D-M, FI11PH-M Firmware Version 44404- E7E7 Peripheral Sharing Devices Common Criteria Guidance Supplement

*Doc No. 2149-001-D105A2B*

*Version: 1.5*

*13 March 2024*



*High Sec Labs Ltd.  
29 HaEshel St  
Caesarea,  
Israel 3079510*

## **Prepared by:**

*EWA-Canada, An Intertek Company  
1223 Michael Street North, Suite 200  
Ottawa, Ontario, Canada  
K1J 7T2*



## CONTENTS

<b>1</b>	<b>PREPARATION OF THE OPERATIONAL ENVIRONMENT.....</b>	<b>1</b>
1.1	OPERATIONAL ENVIRONMENT .....	1
1.2	REFERENCES .....	1
<b>2</b>	<b>SECURE ACCEPTANCE PROCEDURES .....</b>	<b>2</b>
<b>3</b>	<b>SECURE INSTALLATION PROCEDURES .....</b>	<b>3</b>
3.1	SECURE INSTALLATION.....	3
<b>4</b>	<b>SECURE OPERATION .....</b>	<b>4</b>
4.1	SELF TESTS.....	4
4.2	NUMBER OF SUPPORTED DISPLAYS.....	4

## LIST OF TABLES

Table 1 – Procedure to Initiate a Self Test.....	4
--	---

# 1 PREPARATION OF THE OPERATIONAL ENVIRONMENT

## 1.1 OPERATIONAL ENVIRONMENT

For secure operation, users are required to ensure the following conditions are met in the operational environment:

- TEMPEST approved equipment may not be used with the secure peripheral sharing device
- The operational environment must provide physical security, commensurate with the value of the peripheral sharing device and the data that transits it
- Wireless keyboards, mice, audio, user authentication, or video devices may not be used with the secure peripheral sharing device
- Peripheral sharing device Administrators and users are trusted individuals who are appropriately trained
- Administrators configuring the peripheral sharing device and its operational environment follow the applicable security configuration guidance
- Special analog data collection cards or peripherals such as analog to digital interface, high performance audio interface, or a component with digital signal processing or analog video capture functions may not be used with the secure peripheral sharing device

## 1.2 REFERENCES

The documents listed below are applicable to all of the models covered by this guidance document:

- HSL QUICK SETUP GUIDE Secure KVM Isolators, HDC19412 Rev. 2.2
- Guidance may be downloaded from the High Sec Labs website (<https://highseclabs.com/quick-start-guides/>) in .pdf format.

## 2 SECURE ACCEPTANCE PROCEDURES

High Sec Labs (HSL) peripheral sharing devices may be purchased directly from HSL, or through distributors and resellers / integrators.

Upon receipt of the HSL peripheral sharing device, the customer can verify the configuration and revision by comparing the part number and revision on the packing list with the label on the back of the hardware unit. The nameplate includes the product part number (CGA) which is linked directly to the revision of the hardware components and firmware. Verification of the part number provides assurance that the correct product has been received.

The customer must download product documentation from the HSL website in Adobe Acrobat Portable Document Format (PDF). The customer can confirm that the documentation matches the purchased model.

Customers are instructed to check all delivered products for package container seals, and to verify that product tampering evident labels are intact. If an issue is discovered, the customer is instructed to return the product immediately.

## **3 SECURE INSTALLATION PROCEDURES**

This section describes the steps necessary for secure installation and configuration.

### **3.1 SECURE INSTALLATION**

Instructions for secure installation may be found in the Quick Installation Guides.

## 4 SECURE OPERATION

This section describes the steps necessary for the secure operation of the HSL Peripheral Sharing Devices.

### 4.1 SELF TESTS

A self test is performed at power up. Self test failures may be caused by an unexpected input at power up, or by a failure in the device integrity. A self test failure may also be an indication that the device has been tampered with.

A user may initiate a self test by following the procedures outlined in Table 1. In the case of a self test failure, users are directed to contact HSL Technical Support.

Device Type	Procedure
FI11H-M FI11D-M FI11PH-M	<ol style="list-style-type: none"><li data-bbox="500 772 1416 898">1. To enter self-test mode, ensure the display is disconnected from the unit. Power on the unit for at least five seconds. The HID device's LED will start blinking and the keyboard/mouse and video are disabled.</li><li data-bbox="500 898 1073 930">2. To exit self test mode, cycle the power.</li></ol>

**Table 1 – Procedure to Initiate a Self Test**

### 4.2 NUMBER OF SUPPORTED DISPLAYS

HSL KVM Isolators support a single display.