# FarmerMind AI — Device Security Policy

Effective Date: April 30, 2026 | Last Updated: April 30, 2026 | Version: 1.0

## 1. Purpose and Scope

This Device Security Policy (**"Policy"**) describes the security architecture of the FarmerMind AI Cube and related hardware (the **"Device"**), the security controls implemented by **FarmerMind AI LLC** (**"FarmerMind," "we," "us,"** or **"our"**), and the security responsibilities of users (each, a **"User"**).

This Policy is incorporated by reference into the FarmerMind **Terms of Use** and **End User License Agreement**. Capitalized terms not defined here have the meanings given to them in those documents.

## 2. Security Architecture Overview

The Device is engineered as an **offline-first, hardened agricultural appliance**. Its security model is built on the following principles:

- **Data stays on the Device.** Farm data, diagnostics, images, and user-generated content are processed and stored locally on the Device. No continuous cloud connection is required for the Device to operate.
- **Least surface area.** Unused interfaces, remote access, and interactive shells are disabled by default in the shipped configuration.
- **Signed, controlled updates.** Software updates are delivered only through cryptographically signed, FarmerMind-verified USB updates.
- **Encryption at rest.** The Device's root filesystem is protected by full-disk encryption.
- **Kiosk execution.** The Device boots directly into a restricted, application-focused user interface.

## 3. Device-Side Security Controls

As of the Effective Date, the shipped Device configuration includes the following controls. FarmerMind may modify these controls in future firmware releases to maintain or improve the Device's security posture.

## 3.1 Full-Disk Encryption

The Device's root filesystem is encrypted using **Linux Unified Key Setup (LUKS)**. The keyfile required to unlock the root filesystem is stored in the initial RAM filesystem (*initramfs*). This configuration protects user data against offline extraction of Device storage media.

## 3.2 Disabled Interactive Access

**TTY consoles and SSH** are disabled in the shipped configuration. The Device does not accept remote interactive logins and does not expose a local shell through attached keyboards or serial consoles.

## 3.3 Kiosk Boot Mode

The Device boots into **kiosk mode**, loading directly into the FarmerMind user interface. Users do not have access to the underlying desktop environment, package manager, or system utilities through the normal user experience.

## 3.4 Verified USB Updates Only

Software, firmware, and content updates are installed exclusively through a **FarmerMind-verified USB update**. Each update bundle is **cryptographically signed** by FarmerMind. The Device validates the signature at install time and rejects unsigned, modified, or third-party update payloads.

Attempting to load unsigned or modified updates will (a) be rejected by the Device, (b) be treated as a tamper event for the purposes of Section 7, and (c) may render the Device inoperable.

## 3.5 Peripheral and USB Control

The Device is designed to accept only the following peripherals:

- A FarmerMind-verified USB update stick, connected only during an update;
- A Micro HDMI cable to the Device's display;
- The FarmerMind-supplied 45W USB-C power adapter;
- Input peripherals (keyboard, mouse, or touch input) supported by the shipped configuration.

Connecting unauthorized peripherals, mass-storage devices, or communications radios is **prohibited** under the Terms of Use and may be rejected by the Device.

### 3.6 Boot Integrity

The Device performs integrity checks on its boot chain at startup. Attempts to modify the bootloader, kernel, or initramfs will prevent the Device from booting into the FarmerMind user interface.

## 4. Ships-Without-Battery Design

The Device ships **without an internal battery**. Power is supplied via the FarmerMind-supplied 45W USB-C power adapter or an equivalent regulated supply meeting the Device's published specifications. This design reduces fire and transport risks and simplifies compliance with hazardous-materials shipping regulations.

## 5. Data Protection on the Device

User-generated data on the Device is protected by the full-disk encryption described in Section 3.1. Access to this data is controlled by the kiosk user interface. FarmerMind does not maintain, and is unable to recover, any key or credential that would allow FarmerMind to access the contents of your Device remotely.

For details on information we collect when you affirmatively share it with us (such as through opt-in analytics sharing or a support request), see our **Privacy Policy**.

## 6. User Security Responsibilities

The Device's security posture depends on proper handling by the User. You agree to:

- **Physically secure the Device** against unauthorized access, theft, and environmental damage (dust, moisture, temperature extremes, direct sunlight, and power surges);
- **Use only the supplied or specified power adapter** and cabling. Unregulated or counterfeit power supplies may damage the Device and void the Warranty;
- **Do not connect** unauthorized USB devices, mass storage, radios, or networking peripherals to the Device;
- **Do not attempt** to modify, tamper with, bypass, or reverse engineer any security control described in this Policy;
- **Apply FarmerMind-verified updates** promptly when they are made available, to receive security fixes;
- **Protect any access credentials** you set (such as passcodes on the kiosk interface, where applicable);
- **Report suspected security issues** under Section 8 below.

Failure to meet these responsibilities may void the Warranty, terminate the license granted in the EULA, and result in suspension of the Services.

## 7. Tamper Events and Consequences

A **“Tamper Event”** includes, without limitation:

- Any attempt to bypass full-disk encryption, kiosk mode, boot integrity, or update verification;
- Loading or attempting to load unsigned, modified, or third-party firmware, software, or content onto the Device;
- Physical disassembly or modification of the Device beyond what is permitted by the Warranty Policy;
- Connecting unauthorized peripherals in a manner designed to gain shell, filesystem, or memory access;
- Use of tools, exploits, or techniques intended to defeat the Device’s security controls.

A Tamper Event:

- Is a **material breach** of the Terms of Use and EULA;
- **Voids the Warranty** as described in the Warranty Policy;
- **Automatically terminates** the license to the Software granted in Section 2 of the EULA;
- May constitute a violation of the **U.S. Digital Millennium Copyright Act**, the **Computer Fraud and Abuse Act**, or equivalent foreign law; and
- May render the Device permanently inoperable. FarmerMind is not responsible for repair or replacement of a Device affected by a Tamper Event.

## 8. Reporting Security Issues

If you believe you have identified a security vulnerability, a suspected compromise of your Device, or a counterfeit FarmerMind product, please contact us at **info@farmermind.ai** with:

- A description of the issue and its potential impact;
- Steps to reproduce, if applicable;
- The Device serial number (if you are the registered owner);
- Your contact information for follow-up.

FarmerMind will acknowledge receipt within a reasonable period and investigate the report. We ask that reporters **give us a reasonable period to remediate** before publicly disclosing a vulnerability, and that reporters do not conduct testing that degrades service for other users, accesses data not belonging to the reporter, or violates applicable law.

FarmerMind does not currently operate a paid bug-bounty program. We appreciate and will acknowledge good-faith security research.

## 9. Security Updates

FarmerMind may issue security updates that modify, disable, or replace vulnerable components in the Software or firmware. By applying any FarmerMind-verified USB update, you consent to the installation of such updates, as described in Section 5 of the EULA.

FarmerMind has no obligation to provide security updates for any particular period. Security-update availability may vary across Device generations and product lines.

## 10. Counterfeit and Tampered Devices

Genuine Devices are identified by the markings applied at manufacture, including the FarmerMind product sticker (bearing, at minimum, the product identifier **FMIA-001**, a Patent Pending notice, the FCC ID, and an Assembled in USA mark). Devices without these markings, or with evidence of tampered or replaced markings, are not genuine and are not covered by the Warranty.

Purchases should be made through **farmermind.ai** or an authorized reseller. If you believe you have received a counterfeit Device, please report it under Section 8.

## 11. Policy Updates

FarmerMind may update this Policy from time to time. Material changes will be notified consistent with Section 19 of the Terms of Use. The “Last Updated” date at the top of this Policy indicates when it was most recently revised.

## 12. How to Contact Us

**FarmerMind AI LLC**

Email: **info@farmermind.ai**