

# AV Device Security Guidelines

---

Document Version: 1.0

Prepared by: OpenAVCloud Technical Working Group

Date: October 2, 2025

## Table of Contents

Table of Contents.....	2
Document History and Change Log.....	3
1. Purpose.....	4
2. Security Requirements .....	5
2.1 Firmware Integrity and Secure Boot .....	5
2.2 Secure Communications (Data in Transit) .....	5
2.3 Network Authentication and Access Control .....	5
2.4 Secure Storage (Data at Rest).....	5
2.1 Device Provisioning and Identity .....	6
2.2 Lifecycle Security and Vulnerability Management.....	6
3. Additional Considerations .....	7
3.1 Password Management.....	7
3.2 Secure Development and Supply Chain Practices.....	7
3.3 Incident Response and Logging.....	7
3.4 Application Security .....	7
4. Compliance and Auditing .....	7
4.1 Security Audits .....	7
5. References.....	8

## Document History and Change Log

This section captures the history of changes made to this document.

Version	Date	Reason for Change
1.0	2025-10-02	Initial release of AV Device Security Guidelines.

## **1. Purpose**

This document outlines the minimum security guidelines required for Audio/Video (AV) devices developed, deployed, or integrated by members of the OpenAVCloud initiative.

## **2. Security Requirements**

### **2.1 Firmware Integrity and Secure Boot**

- 2.1.1 Devices must implement an irrevocable hardware Secure Boot process.
- 2.1.2 Secure Boot must be enabled by default.
- 2.1.3 Devices must prevent unauthorized and unauthenticated software from being loaded. If permitted, it must run in a sandboxed or limited-permission environment.
- 2.1.4 Remote software updates must be digitally signed by a trusted authority.
- 2.1.5 Devices must verify the digital signature and certificate chain before updates.

### **2.2 Secure Communications (Data in Transit)**

- 2.2.1 Devices must use certificate pinning or equivalent for TCP/IP or UDP/IP communication.
- 2.2.2 TCP protocols (e.g., MQTT) must be protected by TLS.
- 2.2.3 UDP protocols (e.g., CoAP) must be protected by DTLS.
- 2.2.4 Cryptographic suites must be validated against NIST 800-131A or OWASP. Unsecure suites must be removed.

### **2.3 Network Authentication and Access Control**

- 2.3.1 Devices must support a secure network authentication method such as 802.1X.
- 2.3.2 All unused ports must be closed by default.
- 2.3.3 Treat auto-discovery conservatively by default and restrict its scope to intended domains and purposes
- 2.3.4 Debug interfaces must be disabled or protected via a best practice authentication or access control mechanism.
- 2.3.5 Debug interfaces that are physical ports should be physically protected by the device.
- 2.3.6 Resilience should be built into the device, taking into account the possibility of outages of data networks and power.

### **2.4 Secure Storage (Data at Rest)**

- 2.4.1 Devices must not contain hardcoded credentials.
- 2.4.2 Network communication keys must be stored securely.

- 2.4.3 Passwords must be stored using industry-standard cryptographic algorithms.
- 2.4.4 Users must be provided with functionality such that all their user data can be erased from the consumer IoT device in a simple manner (factory reset).

## **2.1 Device Provisioning and Identity**

- 2.1.1 Devices must have a unique and tamper-resistant identifier.
- 2.1.2 Secure provisioning must include unique generation, distribution, update, revocation, and destruction of keys.

## **2.2 Lifecycle Security and Vulnerability Management**

- 2.2.1 Vulnerability assessments must be conducted before launch and periodically thereafter.
- 2.2.2 The manufacturer must make a vulnerability disclosure policy publicly available. This policy must include, at a minimum:
  - 2.2.2.1 contact information for the reporting of issues; and
  - 2.2.2.2 timelines for initial acknowledgement of receipt of a vulnerability report; and
  - 2.2.2.3 timelines for when the person who reported the issue will receive status updates until the resolution of the reported issues.
- 2.2.3 The manufacturer must publish, in an accessible way that is clear and transparent to the user, the defined support period.

### **3. Additional Considerations**

#### **3.1 Password Management**

- 3.1.1 Enforce strong password policies including complexity, rotation, and secure recovery.
- 3.1.2 Avoid default passwords and ensure initial credentials are changed at first use
- 3.1.3 Establish mutual trust for device-to-device and device-to-gateway communications, with credentials managed for expiration and revocation

#### **3.2 Secure Development and Supply Chain Practices**

- 3.2.1 Follow secure coding practices, code signing, and vulnerability scanning.
- 3.2.2 Ensure vendors comply with supply chain security standards including SBOM transparency.

#### **3.3 Incident Response and Logging**

- 3.3.1 Support event logging for security actions.
- 3.3.2 Maintain a documented incident response plan including detection, containment, and remediation.

#### **3.4 Application Security**

- 3.4.1 All applications running on the device, including third-party apps, must follow secure development practices.

### **4. Compliance and Auditing**

#### **4.1 Security Audits**

5.

- 4.1.1 All AV devices must undergo regular security audits and demonstrate compliance with this standard.

## **5. References**

- 1 NIST SP 800-131A
- 2 OWASP IoT Top 10
- 3 ISO/IEC 27001
- 4 IEEE 802.1X