@demotoprod · EDGE

Edge AI security checklist

On 17 Sep 2026 a group reported unbolting one licence-plate-reader camera and finding the encryption key next to the recorded media: about 1.6 million images and 27,321 clips from roughly 21 days, from a device whose vendor had said footage is only briefly stored. A device that scores frames locally must decrypt them locally, so "encrypted at rest" protects a dead disk, not a working device.

1 Pull one unit off the wall and count what is on it

The claim was "briefly stored"; the device held about 21 days of media, and nobody knew because nobody had taken a unit down and counted. Retention on the edge is a claim until someone counts, and the count is what a thief gets.

- **Once a quarter, image one deployed device per hardware revision and list every file with its age.**
- **Put the counted retention in the questionnaire; set the on-device window in minutes and alert past it.**

2 Keep keys in a secure element the board cannot read as a file

The stolen camera's media partition carried the key that unlocked the media, so on-device encryption changed nothing for whoever held it. The consumer IoT baseline standard says sensitive security parameters shall be stored securely and a per-device identity shall resist physical, electrical and software tampering.

- **Per-device keys in a secure element or TEE, generated on the device, never on flash; no shared fleet key.**
- **The cloud accepts a device only after attestation; "encrypted at rest" is true only when the device is off.**

3 Store the result, not the frame

The model needed each frame for milliseconds; the device kept it for weeks. About 50,200 vehicles and 11 people were in the extracted media because raw frames stayed after the inference that used them. The NIST core baseline makes data protection a capability of the device itself.

- **Write the inference output (class, count, score) and at most a thumbnail; drop the frame after scoring.**
- **Anything waiting for upload is encrypted with a key the device does not hold; delete on acknowledgement.**

4 Sign the model and the firmware, and refuse anything unsigned

A device nobody guards can be opened, re-flashed and put back, so the model and the firmware must prove where they came from. The baseline standard asks for secure boot and updatable software; UK law for consumer connectable products (in force 29 April 2024) requires a published minimum security-update period.

- **Secure boot with anti-rollback; the model is signed with a key that never lives on the device, and an unsigned model does not load.**
- **Signed over-the-air updates with a tested rollback; publish the support period per hardware revision.**

5 Rehearse losing the box

One unit gave up 21 days of media; with a shared key it would have been the fleet. The NIST baseline asks that each device be uniquely identifiable and report its own state, which helps only if revoking one has been rehearsed.

- **Per-device identity and certificate, and a "reported stolen" runbook that revokes it within minutes.**
- **Remote wipe on next contact; rehearse the runbook on a real unit twice a year.**

Nitish Gautam · indica-tech.com · hello@indica-tech.com

INDICA TECH · @DEMOTOPROD

Nitish Gautam

Founder-led AI engineering. Demo to production, under NDA, in regulated industries, on fixed scope.

Where this list comes from

Ten-plus years taking products from zero to one across seven sectors, including defence, fintech, medical and telecom, with AI shipped into regulated and air-gapped environments. The @demotoprod channel takes one production AI failure apart each day. These checklists are the same work written down: every item is a dated failure or a documented default, with the control that stops it and the primary source.

If this list found a gap

1. **Your demo works and production is stuck.**
   Production Readiness Audit. Fixed price, two weeks. A five-dimension scorecard, cost and failure analysis, and a 90-day execution roadmap.

2. **You need senior AI judgement without a full-time hire.**
   Fractional AI Lead. Monthly, 30-day notice either side. Weekly 1:1 with the founder or CTO, architecture and code review, technical hiring support, investor-ready due diligence.

3. **An AI feature has to work, by a date.**
   AI Build Sprint. Fixed price, four to eight weeks. Scope signed off up front, weekly demos, CI/CD and observability included, 30-day production warranty.

4. **A regulator, an auditor or a customer's security team is asking.**
   AI Governance & Compliance. Fixed price, four weeks. ISO 27001 / SOC 2-aligned controls, a model risk framework, human-in-the-loop and audit logging, regulator-ready documentation.

BOOK A CALL
indica-tech.com/#contact

EMAIL
hello@indica-tech.com

WEBSITE
indica-tech.com

ALL CHECKLISTS
indica-tech.com/checklists/

YOUTUBE
youtube.com/@demotoprod

LINKEDIN
linkedin.com/in/startup-founderx

INSTAGRAM
instagram.com/demotoprod

TIKTOK
tiktok.com/@demotoprod

Free to share. The live list, with every source link: indica-tech.com/checklists/#edge-ai-security