IoT Security Checklist for Production

A practical sign-off document for product makers

v1.1 · September 2026

Six controls. Clear priorities. Evidence before shipment.

Designed by Nastrotek · nastrotek.com

Contents and reviewer qualifications

This checklist is a production-readiness aid, not a replacement for a security audit or penetration test. Mark every item, attach evidence, and assign an owner for anything that is not ready.

Reviewer qualifications

ROLE	MINIMUM EXPECTATION
Security reviewer	Security engineer or reviewer familiar with OWASP IoT Top 10 and abuse-case testing.
Firmware lead	Confirms boot chain, signing, storage, OTA behavior, and production configuration.
Product owner	Accepts residual risk only with a documented mitigation, owner, and target date.
Independence	The code author should not be the sole reviewer of their own security control.

Release gate

A critical failure blocks shipment unless the product owner records a formal risk decision. A deferred item needs a mitigation, owner, target date, and evidence plan.

GATE CHECK	STATUS / OWNER / NOTES
No CRITICAL item is open without a documented decision.	[ ] Pass [ ] Fail Owner: _____
Production firmware, hardware revision, and configuration are uniquely identified.	[ ] Pass [ ] Fail Owner: _____
Debug and factory access are disabled or controlled.	[ ] Pass [ ] Fail Owner: _____
Test evidence is stored with the release record.	[ ] Pass [ ] Fail Owner: _____

Priority legend

LABEL	SHIPMENT MEANING
CRITICAL	Blocker by default: compromise, unauthorized code, or fleet-wide impact.
HIGH	Must be fixed or explicitly accepted before release.
MEDIUM	Track and schedule; assess impact in the product threat model.
LOW	Useful hardening; defer only with a recorded reason.

1. TLS/SSL and transport security

Unencrypted traffic can expose credentials and user data to interception or tampering. This section proves plaintext fallback is rejected, not merely discouraged.

PRIORITY	CHECK	EVIDENCE GUIDANCE	RESULT / OWNER
CRITICAL	All cloud and API traffic uses TLS; plaintext endpoints are disabled.	[ ] Packet capture showing 100% HTTPS; endpoint inventory; CI negative test for HTTP fallback.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
CRITICAL	The device validates server certificate and hostname.	[ ] Negative test with expired, wrong-host, and self-signed certificates; approved TLS configuration.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
HIGH	Secrets are absent from source, firmware artifacts, and logs.	[ ] Secret-scanner output; firmware strings review; sanitized log export.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
MEDIUM	Certificate, key, and endpoint rotation has a tested process.	[ ] Rotation runbook; staging rotation result; owner and expiry alert.	[ ] Pass [ ] Fail [ ] N/A Owner: _____

2. Password and credential storage

A shared password turns one exposed device into a fleet-wide incident. Credentials should be unique, protected at rest, revocable, and removed by reset.

PRIORITY	CHECK	EVIDENCE GUIDANCE	RESULT / OWNER
CRITICAL	Each device has a unique identity or credential; no universal default password.	[ ] Provisioning record for sample devices; uniqueness query; factory-default test.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
CRITICAL	Passwords and tokens are never stored as plaintext.	[ ] Flash/storage inspection; code review; secret scan of logs and crash reports.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
HIGH	A lost or compromised device can be revoked individually.	[ ] Revocation test showing only one device loses access; backend audit log.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
HIGH	Factory reset removes credentials, bonds, and account linkage as intended.	[ ] Before/after reset test; backend state check; data-deletion evidence.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
HIGH	Brute-force attempts are rate-limited or locked out.	[ ] Abuse-case test with threshold and recovery behavior recorded.	[ ] Pass [ ] Fail [ ] N/A Owner: _____

3. Secure Boot

Physical access can turn an unprotected boot path into a way to run modified code. Secure Boot establishes the device-side gate before application logic starts.

PRIORITY	CHECK	EVIDENCE GUIDANCE	RESULT / OWNER
CRITICAL	Boot verification is enabled in the production configuration.	[ ] Production fuse/configuration export; boot log from a release device.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
CRITICAL	Unsigned or modified firmware is rejected before execution.	[ ] Tamper test with changed image; captured rejection result.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
HIGH	Recovery behavior does not create an unauthenticated bypass.	[ ] Recovery-mode test; documented RMA authorization flow.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
HIGH	Production provisioning steps and security settings are access-controlled.	[ ] Manufacturing SOP; access list; sample provisioning record.	[ ] Pass [ ] Fail [ ] N/A Owner: _____

4. Firmware signing

Signing protects the release boundary: only an image approved by the product team should be installable. The signing key itself is a production asset and needs custody rules.

PRIORITY	CHECK	EVIDENCE GUIDANCE	RESULT / OWNER
CRITICAL	Every production image is signed by a controlled release process.	[ ] Signed artifact, firmware hash, CI/CD release log, and approver.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
CRITICAL	The device verifies signature, version, and target before install.	[ ] Wrong-key, wrong-target, and malformed-image negative tests.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
HIGH	Signing keys are separate from source code and developer laptops.	[ ] Key custody record; CI secret configuration; access review.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
MEDIUM	A key-compromise response plan exists.	[ ] Rotation/revocation runbook; named owner; tabletop exercise result.	[ ] Pass [ ] Fail [ ] N/A Owner: _____

5. OTA security

An OTA package can be validly signed and still break the device. Safe updates need authentication, version policy, power-loss recovery, health checks, and rollback.

PRIORITY	CHECK	EVIDENCE GUIDANCE	RESULT / OWNER
CRITICAL	OTA packages are authenticated, not only checksum-checked.	[ ] Signed OTA test; invalid-signature rejection log; release manifest.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
CRITICAL	The device prevents downgrade to a vulnerable version.	[ ] Downgrade test; minimum security version configuration.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
HIGH	Interrupted updates recover to a known-good image.	[ ] Power-loss matrix during download/write/boot; recovery result.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
HIGH	Rollout, authorization, health check, and rollback are observable.	[ ] OTA dashboard/logs; staged rollout record; rollback drill.	[ ] Pass [ ] Fail [ ] N/A Owner: _____

6. Data encryption and privacy

Encryption reduces exposure, but data minimization reduces the blast radius. The team should know what is collected, where keys live, how long data stays, and how it is deleted.

PRIORITY	CHECK	EVIDENCE GUIDANCE	RESULT / OWNER
CRITICAL	Sensitive data is encrypted in transit and at rest where appropriate.	[ ] Traffic capture; storage configuration; key-management evidence.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
HIGH	Encryption keys are isolated from protected data and can be rotated.	[ ] Key lifecycle document; rotation test; access-control review.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
HIGH	Logs avoid passwords, tokens, personal data, and raw secrets.	[ ] Production log sample; automated log scan; redaction test.	[ ] Pass [ ] Fail [ ] N/A Owner: _____
MEDIUM	Data retention and deletion behavior is documented and tested.	[ ] Data map; deletion test; retention configuration and owner.	[ ] Pass [ ] Fail [ ] N/A Owner: _____

Remediation tracker

Complete one row for every item marked FAIL. The first row is an example; replace it with your own issue. A useful entry says what failed, why it failed, what engineering will change, and who owns the date.

FAILED CHECK / PRIORITY	ROOT CAUSE	FIX PLAN	TARGET DATE / OWNER
Example: TLS plaintext fallback / CRITICAL	Legacy provisioning path still accepts HTTP.	Remove HTTP path; add negative test; release firmware v1.2.	30 Sep 2026 / Linh
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Risk acceptance record

Deferred risk and mitigation: _____

Accepted by: _____ Date: _____ Review date: _____

Compliance scoring summary

Use the totals from the six section tables. A pass rate is a navigation aid, not a substitute for severity: one open CRITICAL item can block shipment even when the percentage looks high.

METRIC	VALUE
Total checks	26
Passed	_____
Failed	_____
N/A	_____
Pass rate	_____ %
Highest open priority	[ ] CRITICAL [ ] HIGH [ ] MEDIUM [ ] LOW
Overall status	[ ] READY [ ] CONDITIONAL [ ] BLOCKED

Scoring notes

A CONDITIONAL approval should name every accepted risk. Recalculate when firmware, hardware, cloud endpoints, provisioning, or OTA policy changes.

Final sign-off and approval workflow

STAGE	SIGN-OFF ACTION	OWNER / DATE
1	Security lead reviews checks and evidence.	_____
2	Engineering lead confirms remediation plans.	_____
3	Product owner accepts residual risk.	_____
4	CTO or delegated approver signs CONDITIONAL approval.	_____

Final decision

FIELD	RECORD
Decision	[ ] Ready to ship [ ] Conditional approval [ ] Blocked
Open items	_____ _____
Approved by	_____
Date	_____

Keep this review with the release evidence and repeat it when the product, firmware, cloud endpoint, or provisioning flow changes.

References and changelog

Use these sources to deepen a specific control or plan a separate security assessment.

REFERENCE	USE
OWASP IoT Security Testing Guide	Practical test ideas for device, interface, and backend review.
NIST IR 8259A	Core baseline capabilities for IoT device cybersecurity.
ESP-IDF security examples	Reference flows for Secure Boot, storage protection, and security configuration.
ESP-IDF OTA examples	Reference implementation patterns for update and rollback testing.
CWE / OWASP IoT Top 10	Shared language for weaknesses and threat prioritization.

Changelog

VERSION	CHANGE
v1.1 · Sep 2026	Added priority levels, expanded evidence guidance, reviewer qualifications, remediation tracker, scoring summary, approval workflow, and changelog.
v1.0 · Sep 2026	Initial Nastrotek IoT production security checklist.

Designed by Nastrotek · nastrotek.com
For educational and production-readiness review purposes.