



# AF 9100:2026

## Aerospace Quality Management System

POLICY

### **Trusted Evidence, Confidentiality and Digital Integrity Policy**

**AF-PL-9100-003**

FIRST EDITION

30 September 2026 | English master text

# Publication identity and application

| Control                    | Publication value                                                                                                            |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Title                      | Trusted Evidence, Confidentiality and Digital Integrity Policy                                                               |
| Document code              | AF-PL-9100-003                                                                                                               |
| Edition / language         | FIRST EDITION / English master text                                                                                          |
| Companion edition identity | 30 September 2026                                                                                                            |
| Controlling source         | AF 9100:2026 — FIRST EDITION — 29 September 2026                                                                             |
| Responsible owner function | Accountable executive                                                                                                        |
| Primary source anchors     | 7.9, 7.11, 7.12, 12.7, 13, D, O, AJ.7                                                                                        |
| Delivery status            | Prepared implementation companion. Actual approval, adoption, effectivity and operational decisions are recorded separately. |

## Use and document-control boundary

This companion implements the supplied AF 9100 requirement basis without changing the original standard. Its process allocation, examples, checklists and record design are authored implementation material. Actual mission or product limits, specialist procedures, permissions and genuine observations must be completed before consequential use. Applicable source minima and independent decision conditions cannot be reduced by this companion.

The printed edition date identifies the companion series; it is not evidence that later preparation, review or operational decisions occurred on that date. New support codes in this set are proposed allocations for controlled registration. Established AF-IG-9100-001, AF-FAQ-9100-001 and AF-TR-9100-001 identities are retained; earlier files, the corporate master list and ASTRA codes are not overwritten.

Equivalent combined or digital records are permitted when all required fields, relationships, authority and history remain intact. A completed PDF field or typed name is not evidence of an authenticated approval. Blank records in this delivery contain no invented applicant, signature, event or result.

# Contents and reading route

|                                                      |    |
|------------------------------------------------------|----|
| Publication identity and application                 | 2  |
| Contents and reading route                           | 3  |
| 1 Scope, responsibility and source priority          | 4  |
| 2 Policy commitments and prohibited conduct          | 4  |
| 3 Responsibilities, implementation and review        | 5  |
| 4 Implementation instruments                         | 5  |
| Appendix A — Controlling source and evidence         | 6  |
| Source tables — complete field and decision payloads | 10 |
| Appendix B — Local implementation and release        | 12 |

Select actual scope → complete application criteria → use the applicable procedure and technical book → capture authentic evidence → evaluate every applicable condition → obtain the required independent decision. Document availability does not establish implementation or conformity.

# 1 Scope, responsibility and source priority

Applies to the responsible function and exact evaluated object selected from the source. Use only the duties triggered by actual activity and retained responsibility.

| Boundary         | Required implementation decision                                                                                                                 |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Object and route | Identify ORG, PRD, SVC, PRC, PER, SUB or CAB separately. Combined records do not merge outcomes.                                                 |
| Activity         | Apply source technical modules by performed or retained responsibility, including relevant outsourced work.                                      |
| Authority        | Technical release, employer task permission, independent attestation and statutory authorization remain distinct.                                |
| Source priority  | AF 9100:2026 and all compatible binding obligations control. This companion does not import ASTRA programme rules or external normative schemes. |

# 2 Policy commitments and prohibited conduct

## 2.1 Document, Record and Publication Control

The responsible function maintains document, record and publication control within its actual scope. A missing applicable instruction, inaccessible essential evidence or unapproved technical amendment prevents dependent use.

Policy application: Separate requirements, operating instructions, blank templates, completed records and public extracts. Assign an owner and a unique identifier; record the source edition and the object that may rely on it. Remove obsolete copies from unintended use, retain their historical decision links and notify recipients of material corrections. Verify cached, translated and remote copies; source availability alone does not establish local implementation.

## 2.2 Technical Tools, Data Integrity and Evidence Portability

The responsible function maintains technical tools, data integrity and evidence portability within its actual scope. Failure of an essential known-answer, authority or relationship check blocks consequential use of the affected tool.

Policy application: Identify the decision, consequence, algorithm, data model, units, interfaces, user roles and functions capable of creating or hiding a defect. Record actual local acceptance, remaining restrictions, trained users and revalidation triggers. Transfer usable records and accepted custody before cutover; PDFs are record artifacts, not a deployed database.

## 2.3 Continuity, Emergency Interfaces and Assured Recovery

The responsible function maintains continuity, emergency interfaces and assured recovery within its actual scope. Availability restored without required integrity or protective evidence does not authorize assured use.

Policy application: Record critical functions, maximum tolerable interruptions under the real profile, recovery objectives, alternate sources and common failures. The technical authority approves bounded return only after required checks. Independently update any scheme status, assess prior outputs, repeat failures and verify improvements.

## 2.4 Software, AI, Models and Trusted Updates

The responsible function maintains software, ai, models and trusted updates within its actual scope. Unknown target configuration, invalid evaluation or failed essential protection blocks consequential deployment.

Policy application: Identify requirements, criticality, architecture, domain, users, permitted and prohibited actions, interfaces and recovery. Assess whether the proposed tool is necessary and sufficiently verifiable.

Define drift, changed exposure, unavailable inputs and response authority. Reassess adaptation outside the approved envelope; preserve source/build access, records and support beyond supplier or platform exit.

## 3 Responsibilities, implementation and review

| Function                     | Policy responsibility                                                                                                    |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Accountable executive        | Provide resources, protect independence, approve policy application and respond to systemic adverse evidence.            |
| Technical and process owners | Translate commitments into applicable controls, prospective criteria and genuine records.                                |
| Independent assurance        | Challenge unsupported decisions and report unresolved threats through an uninvolved authority.                           |
| All relevant personnel       | Use current instructions, report actual observations, preserve adverse evidence and stop unsupported consequential work. |

Explain this policy in forms and language understood at the actual point of use. Evaluate application through decisions and records rather than attendance alone. Review after material change, serious concern and the applicable management review; do not invent an additional universal review calendar.

## 4 Implementation instruments

| Procedure code | Operating instrument                                     |
|----------------|----------------------------------------------------------|
| AF-PR-9100-001 | Document, Record and Publication Control                 |
| AF-PR-9100-010 | Technical Tools, Data Integrity and Evidence Portability |
| AF-PR-9100-026 | Continuity, Emergency Interfaces and Assured Recovery    |
| AF-PR-9100-027 | Software, AI, Models and Trusted Updates                 |

# Appendix A — Controlling source and evidence

Source: AF 9100:2026, Aerospace Quality Management System, FIRST EDITION, 29 September 2026; supplied 131-page PDF. Source page references below locate the original publication. These excerpts are read with the complete applicable standard; local implementation sequences do not replace it.

## 7.9 Communication and controlled information exchange

### **SOURCE p. 19 | Normative when applicable**

7.9(a) The organization shall define what information is communicated, by whom, to whom, when and through which controlled channels. Urgent information affecting released products shall have an escalation path and acknowledgement mechanism. Supplier and customer changes shall reach the functions that use the affected data.

7.9(b) Sensitive, proprietary, personal or controlled technical information shall be shared only through authorized arrangements. Meeting attendance or federation membership shall not itself grant access. Communication restrictions shall be reconciled with required hazard and conformity reporting through an approved process.

**Required evidence:** Communication matrix; notification and acknowledgement logs; approved information-sharing arrangements.

## 7.11 Record integrity, retention and long-life readability

### **SOURCE p. 19 | Normative when applicable**

7.11(a) Records shall preserve the identity of the subject, performer, reviewer and applicable configuration, together with time, results, units and disposition. Changes to recorded evidence shall retain the original value, reason, author and approval where relevant. Electronic signatures and acceptance media shall be individual, protected and revocable.

7.11(b) Retention periods shall consider law, contract, product life, latent defects, liability, material traceability and long- duration missions. No universal short retention period is prescribed. Digital preservation shall address format obsolescence, cryptographic validity, migration verification, backup, recovery and readable access after supplier or platform failure.

7.11(c) The organization shall test retrieval of selected legacy and current records, including restoration from backup. Destruction shall be authorized, recorded and suspended when subject to a relevant investigation, claim or preservation obligation.

**Required evidence:** Retention schedule; signature controls; audit trails; migration and restore tests; authorized disposal records.

## 7.12 Technical software, spreadsheets and decision tools

### **SOURCE p. 19 | Normative when applicable**

7.12(a) Software, scripts, spreadsheets and computational tools that influence design, inspection, acceptance or assurance decisions shall be identified and controlled. Validation shall be proportionate to the consequence of an undetected error and shall include known-answer tests, boundary conditions, unit consistency and independent review where required.

7.12(b) Inputs, algorithms, dependencies, versions and output interpretation shall be documented. Formula cells and approved parameters shall be protected where appropriate. An AI-generated calculation or report shall undergo competent review; fluent language or successful execution shall not constitute verification of technical correctness.

**Required evidence:** Tool inventory; validation plan and known-answer tests; version records; review and revalidation triggers.

## 12.7 Generative AI and engineering evidence

### **SOURCE p. 30 | Normative when applicable**

12.7(a) Generative AI used in engineering, procurement, inspection, coding or technical documentation shall have controlled inputs, access and review requirements. Generated claims, citations, calculations and design details shall be verified by competent personnel before becoming controlled evidence.

12.7(b) The organization shall prevent unauthorized disclosure of proprietary or controlled technical data to external services. Prompt history or a generated explanation shall not substitute for a validated calculation,

traceable test or approved design rationale. The human or organizational approval responsibility shall remain identifiable.

**Required evidence:** Approved use cases; data-access rules; review records; verified calculations and references.

### 13.1 Security scope and integrated risk assessment

#### **SOURCE p. 31 | Normative when applicable**

13.1(a) The organization shall identify digital assets, trust boundaries, dependencies, users and interfaces affecting assured outcomes. Threat scenarios shall be evaluated together with safety and mission consequences, including loss of integrity, availability, authenticity and confidentiality.

13.1(b) Security assumptions shall be reviewed across suppliers, remote services, maintenance access and physical access. The organization shall identify where a security measure could impair emergency operation or safety and resolve the conflict through a joint technical decision.

**Required evidence:** Asset and trust-boundary inventory; threat assessment; safety-security interface decisions.

### 13.2 Identity, access and privileged actions

#### **SOURCE p. 31 | Normative when applicable**

13.2(a) Access shall be based on verified identity, least necessary privilege and approved roles. Privileged access, remote maintenance and release-authority actions shall have strengthened authentication and traceable authorization appropriate to risk.

13.2(b) Access shall be removed or changed promptly when responsibilities end or change. Shared credentials shall not obscure accountability. Emergency access shall be controlled, logged, time-bounded and reviewed after use. Service accounts and machine identities shall be governed as well as human accounts.

**Required evidence:** Access matrix; privileged approvals; identity lifecycle; emergency-access reviews.

### 13.3 Secure development and supply-chain integrity

#### **SOURCE p. 31 | Normative when applicable**

13.3(a) Security requirements shall be integrated into development, procurement and maintenance. The organization shall assess dependency provenance, vulnerability exposure, secure configuration, supported versions and mechanisms for receiving security information.

13.3(b) A software bill of materials or equivalent controlled inventory shall identify relevant components and dependencies. Vulnerability disposition shall consider exploitability, exposure, safety consequences and available mitigations. Presence of a component in an inventory shall not itself demonstrate that it is secure.

**Required evidence:** Secure-development plan; SBOM; dependency reviews; vulnerability decisions and mitigations.

### 13.4 OT and connected-production safeguards

#### **SOURCE p. 31 | Normative when applicable**

13.4(a) Industrial networks and connected equipment shall be designed to limit unauthorized changes and propagation of failures. Appropriate segmentation, access control, backup, monitoring and safe degraded operation shall be established based on the process risk.

13.4(b) Patches, remote connections and security tools shall be evaluated for compatibility with timing, availability and safety. Where immediate patching is inappropriate, a time-bounded compensating-control decision shall be documented. Production data and machine-program integrity shall remain verifiable.

**Required evidence:** OT architecture; authorized connections; patch assessments; compensating controls; restoration tests.

### 13.5 Secure updates, rollback and cryptographic agility

#### **SOURCE p. 31 | Normative when applicable**

13.5(a) Updates shall verify origin, integrity, compatibility, authorization and intended target configuration before installation. The organization shall define interruption handling, recovery, anti-rollback needs and conditions for safe rollback without reintroducing an unacceptable vulnerability.

13.5(b) Cryptographic dependencies shall be inventoried and reviewed for supported algorithms, key management, certificate validity and migration capability. Future algorithm replacement shall be planned according to product life and threat exposure; this standard does not mandate a particular algorithm or claim

universal post-quantum readiness.

**Required evidence:** Update architecture; signed release manifest; interruption and rollback tests; cryptographic inventory and migration plan.

## 13.6 Security testing and vulnerability handling

### SOURCE p. 31 | Normative when applicable

13.6(a) Security testing shall have documented authorization, boundaries, safety precautions, data handling and restoration requirements. Methods shall be selected for the architecture and threat model. Test-induced operational or physical hazards shall be assessed before execution.

13.6(b) The organization shall provide a channel for vulnerability reports, assess credibility and impact, track remediation and communicate relevant actions to affected parties. Security findings shall remain connected to product configuration and safety assessment; closure shall require evidence, not only a changed status field.

**Required evidence:** Authorized test plans; results; vulnerability register; remediation verification; customer communication.

## 13.7 Incident response and recovery assurance

### SOURCE p. 32 | Normative when applicable

13.7(a) The organization shall establish incident triage, containment, evidence preservation, technical escalation, communication and recovery responsibilities. Plans shall consider compromised engineering records, manufacturing programs, product updates and supplier credentials, not only office systems.

13.7(b) Recovery shall verify authenticity and consistency of restored data and configurations. A system shall not be returned to assured service solely because it is operational. Exercises shall demonstrate recovery time, recoverable data age and product-impact assessment under representative conditions.

**Required evidence:** Incident plan; exercise records; RTO/RPO basis; integrity verification; return-to-service decision.

## D.1 Requirement-record integrity

### SOURCE p. 55 | Normative when applicable

D.1(a) Every controlled product or service requirement shall have an identifier, statement, source, owner, revision, rationale, applicability, verification method and acceptance criteria. Derived and safety-related requirements shall include their parent link and approving authority.

D.1(b) The organization shall maintain traceability through allocation, implementation, verification, anomaly resolution and release. Traceability completeness shall be evaluated for meaning and validity, not only the presence of hyperlinks. Broken or circular links shall be investigated.

## D.2 Identifiers, versioning and time

### SOURCE p. 55 | Normative when applicable

D.2(a) Identifiers shall remain unique within the defined repository and resolvable after migration. Revision and status shall be distinct; an approved obsolete version shall not appear current. Time records shall identify the relevant time basis and sequence sufficient to reconstruct events.

D.2(b) Units, coordinate systems, reference frames and data encodings shall be explicit where misinterpretation could affect conformity. Imported supplier data shall be checked for mapping errors, truncated precision and semantic differences. Automated exchange shall retain validation results.

## D.3 Evidence provenance and tamper indication

### SOURCE p. 55 | Normative when applicable

D.3(a) An evidence record shall identify the source system or person, acquisition method, processing, transformations and approvals. Cryptographic hashes or signatures may support integrity but shall not be treated as proof that the original observation was correct.

D.3(b) Corrections shall preserve the prior evidence and explain why it changed. Access and modification logs shall be protected in accordance with consequence and obligations. Migration shall verify relationships as well as files; a readable PDF without its underlying configuration links may be insufficient. The filled chain demonstrates structure only. It deliberately does not supply a universal stopping-time value, load or speed; those values require a valid system-specific safety basis.

## O.1 Security evidence baseline

### SOURCE p. 77 | Normative when applicable

O.1(a) The organization shall maintain the records in Table O-1 for the relevant scope. Evidence shall be versioned and linked to the product, service or infrastructure configuration. Confidential security information shall have controlled access without losing authorized auditability.

O.1(b) The security review shall identify unresolved dependencies and limitations. A security certification or penetration-test report for a different scope shall not establish assurance of the actual deployed system.

## O.2 Update release checklist

### SOURCE p. 77 | Normative when applicable

O.2(a) Before update deployment, the organization shall verify the approved build, target compatibility, cryptographic origin/integrity, regression evidence, hazard/security impact and required authorization. The deployment plan shall include interrupted installation and loss-of-power scenarios where relevant.

O.2(b) After installation, the actual version, configuration and protective functions shall be verified. Failed or partial deployment shall remain visible in fleet or asset status. Rollback shall be evaluated for compatibility and vulnerability consequences rather than assumed always safe.

## O.3 Incident-to-product linkage

### SOURCE p. 77 | Normative when applicable

O.3(a) When an incident could affect engineering data, process programs, test records or released products, the organization shall assess the affected technical population. Cyber response and product-quality response shall share a controlled evidence trail.

O.3(b) Return to operation shall require both operational restoration and justified integrity. The authority making that decision shall understand remaining uncertainty. Unverified records shall not be silently reclassified as authentic because the server has been restored.

## O.4 Filled illustrative recovery evaluation

### SOURCE p. 77 | Definition, explanation or informative example; no new universal limit

O.4(a) Example recovery objectives are RTO=4 hours and RPO=1 hour for a technical-record service. An exercise restores service in 3.2 hours from a backup 45 minutes old. These two objectives are met in the example, but one configuration-link integrity check fails.

O.4(b) The exercise outcome is therefore “service restored; assured use held pending integrity correction”. Passing time objectives does not establish trustworthy evidence. The record retains the failed check, affected records, corrective action and successful repeat verification.

## AJ.7 Digital implementation and record export

### SOURCE p. 131 | Normative when applicable

AJ.7(a) A digital workflow shall implement required state transitions, approvals and access controls and shall be tested against permitted and prohibited cases. Tests shall include open critical findings, expired competence, unavailable evidence, mismatched configurations, suspended status and an attempted unauthorized approval.

AJ.7(b) An export shall preserve readable decisions, identities, configurations, requirements, actual results and relationships to supporting evidence. A summary PDF without the necessary source evidence shall not be described as a complete transferable dossier. Migration and restoration shall verify records and relationships, not merely file counts.

**Required evidence:** Workflow validation; prohibited-case tests; attributable approvals; complete exports; relationship and recovery verification.

# Source tables — complete field and decision payloads

**Table D-1 — Required lifecycle data entities**

Source p. 55 | Required structure when applicable

| Entity                    | Minimum fields                                                                                       | Required relationships                                                             |
|---------------------------|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Requirement               | ID; revision; statement; source; rationale; criticality; owner; acceptance criterion; status.        | Parent need; allocated item/function; verification case; applicable obligation.    |
| Configuration item        | ID; type; revision; physical/software identity; owner; baseline; approved use.                       | Requirements; BOM; interfaces; change history; as-built or deployed instances.     |
| Material or component lot | Source; manufacturer; lot/batch; quantity; condition; certificate; received date.                    | Incoming verification; process route; consumed serials; split/merge history.       |
| Verification case         | ID; method; requirement; configuration; procedure; environment; uncertainty; acceptance rule.        | Test article; equipment; raw data; result; anomaly and disposition.                |
| Process execution         | Route revision; operation; performer; date/time; equipment; parameters; material; result.            | Lot/serial; qualified procedure; inspection; nonconformity; next authorized step.  |
| Change                    | ID; reason; baseline before/after; impact; approvals; effectivity; verification.                     | Affected requirements/items; delivered population; suppliers; support information. |
| Hazard or risk            | ID; scenario; consequence; likelihood basis; exposure; controls; owner; residual decision.           | Requirements; mitigations; verification evidence; operational limitations.         |
| Release                   | ID; configuration; scope; acceptance evidence; concessions; restrictions; authorized identity; date. | Requirements baseline; product serial/lot; delivery dossier; service-life status.  |
| Digital artifact          | Artifact ID; version; source/build; dependencies; hash; signature; provenance; access class.         | Requirements; verification; release; deployment instances; vulnerabilities.        |
| Retirement                | Asset identity; condition; hazardous inventory; reuse restrictions; disposition; verifier.           | Life history; disposal evidence; retained records; remaining obligations.          |

**Table D-2 — Filled illustrative trace chain**

Source p. 55, 56 | Illustrative or explanatory source table

| Record        | Example value                                                                                | Connection                                     |
|---------------|----------------------------------------------------------------------------------------------|------------------------------------------------|
| Need          | NEED-GSC-01: controlled motion during payload handling.                                      | Allocated to SYS-GSC-R12.                      |
| Requirement   | SYS-GSC-R12 rev B: stop response within a program-defined limit under stated load and speed. | Hazard H-GSC-02; verification V-GSC-12.        |
| Configuration | Controller CTRL-07 rev C; firmware 2.4.1; cart serial GSC-004.                               | Build manifest BM-241; interface ICD-09 rev D. |

| Record       | Example value                                                          | Connection                                                                       |
|--------------|------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Verification | V-GSC-12 rev 3; test article GSC-004; report TR-012.                   | Raw records RAW-012;<br>calibrated timer TM-08;<br>approved decision rule DR-03. |
| Disposition  | Anomaly AN-04 closed after independent retest.                         | NCR-026; verified corrective<br>action CA-026.                                   |
| Release      | REL-GSC-004 rev 1; approved operating- domain<br>restriction attached. | Release authority RA-02;<br>receiving acknowledgement<br>ACK-004.                |

## Table O-1 — Required security and integrity records

Source p. 77 | Required structure when applicable

| Record                       | Minimum content                                                                                                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Asset/trust model            | Assets, identities, interfaces, zones, data flows, dependencies and trust assumptions.                                   |
| Threat and impact assessment | Credible threats, exposure, safety/mission consequences, controls and residual decisions.                                |
| Access record                | Role, identity, privileges, approver, start/end, emergency use and periodic review.                                      |
| SBOM and dependencies        | Components, versions, provenance, known exposure, support status and disposition.                                        |
| Vulnerability record         | Report source, affected versions, severity basis, exploitability context, mitigation, deadline and verification.         |
| Update manifest              | Target identity, old/new configuration, origin/integrity evidence, compatibility, authorization and rollback conditions. |
| Incident record              | Timeline, evidence preservation, affected population, containment, communication, root cause and recovery approval.      |
| Recovery test                | RTO/RPO basis, backup identity, restoration duration, integrity checks, configuration reconciliation and result.         |
| Crypto-agility record        | Algorithms, keys/certificates, support horizon, dependencies, migration needs and verification.                          |
| Supplier interface           | Access conditions, notification duties, update responsibilities, evidence rights and termination controls.               |

## Appendix B — Local implementation and release

| Readiness condition          | Evidence before consequential use                                                                                                                     |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authority and responsibility | Actual legal operator, owner, competent technical authority, independent reviewer and permitted result class are recorded.                            |
| Scope and criteria           | Object, configuration, site, period, trigger, every technical value or observable attribute, units and prospective approval are complete.             |
| Evidence and methods         | Original accessible evidence, representative observations, valid methods, uncertainty, adverse cases and limitations support the intended conclusion. |
| People and independence      | Competence is current for each task; genuine conflicts, relevant prior work and needed separation have been checked.                                  |
| Records and tools            | Field meanings, unique IDs, original history, access, retention, recovery and actual deployed workflows have passed local validation.                 |
| Decision and public use      | All relevant blockers are resolved; required independent decision and written permissions precede the exact public claim.                             |
| Continuity and handover      | Receiving custody, unresolved duties, corrections and historical decisions survive transfer, retirement or provider closure.                          |

Record the completed local readiness and actual authorization in AF-FR-9100-032 or an equivalent controlled record. Preserve the unchanged source standard and each earlier decision basis. A blocked activity may continue only within a genuinely permitted development boundary, not as a provisional conformity certificate.