NAICAS Technical Requirements Overview

Public technical requirements supporting certification workflows and registry publication
Version 1.0 - Effective December 1, 2025

Document type	Public Technical Requirements Overview (Non-Rulebook; Non-Amending)
Applies to	Systems and workflows submitted for NAICAS certification; NAICAS portal and registry operations
Authority	Program requirements are governed by the NAICAS Rulebook
Effective date	December 1, 2025
Version	1.0
Contact	info@naicas.org

1. Authority and conflict

This document defines minimum technical capabilities that support NAICAS certification workflows and public registry publication. It does not create, amend, supersede, or reinterpret the NAICAS Rulebook. Where any conflict exists, the Rulebook governs.

2. Purpose

- Bind every non-public action to an authenticated actor role and subject identity.
- Enforce least-privilege access controls with fail-closed behavior by default.
- Produce audit-ready, tamper-evident records that support traceability and review.
- Preserve evidence integrity (hashing, versioning, and immutability after submission).
- Support reproducible certification outcomes from stored artifacts and decision records.
- Expose a safe public registry interface that contains only public-safe fields.

3. Normative language

MUST / SHALL: mandatory requirement.
MUST NOT / SHALL NOT: prohibited.
SHOULD: recommended.
MAY: permitted.

4. Identity, access control, and context

- Protected operations MUST be bound to an authenticated actor role and subject identity.
- Authorization MUST be enforced at the data access layer (database or equivalent) and MUST fail closed for protected data.
- Public access MUST be limited to registry endpoints and explicitly allowed public fields.

5. Auditability and traceability

- Every material action MUST be recorded with who performed it, what occurred, and when it occurred.
- Audit records MUST be append-only or equivalently tamper-evident.
- Each request SHOULD carry a correlation identifier that is recorded on audit and workflow records for end-to-end traceability.

Certification decisions MUST be reproducible from stored records, including: application scope, evidence inventory (including hashes), decision record, status progression, and any deficiency or appeal records applicable to the application.

6. Evidence handling

- Evidence MUST be stored with a content hash (for example, SHA-256) and timestamps.
- Evidence SHOULD preserve historical versions and prevent silent overwrite.
- After submission, declared scope and system identifiers SHOULD be immutable except via a defined change process with an audit trail.

7. Public registry requirements

- Registry results MUST expose only public-safe fields (for example: display name, certification level, scope summary, status, and dates).
- Registry endpoints MUST NOT expose evidence links unless intentionally designated as public.
- Registry endpoints SHOULD implement stable ordering, pagination, and rate limits appropriate to public access.

8. Change control

This document is versioned. Changes require a documented proposal, review and approval, and a published effective date. The NAICAS Rulebook governs program authority.

Contact: info@naicas.org