MOROCCAN YOUTH COUNCIL

FOR DIPLOMATIC AND INTERNATIONAL COOPERATION

DIGITAL RESPONSIBILITY FRAMEWORK

Digital Trust & Information Governance

A practical model for records, identity, access, privacy and verification.

PUBLICATION CODE

MYC-PUB-202611-9E0B9D7177

EDITION

NOVEMBER 2026

DOCUMENT FAMILY

PLATFORM

STATUS

PUBLIC REFERENCE EDITION

CURRENT RECORD AND DOCUMENT HISTORY

mycdic.org/documents/records/digital-trust-framework/

Historical signed PDFs are retained without alteration.

About this edition

Digital Trust & Information Governance

A practical model for records, identity, access, privacy and verification.

This revised reference explains the Council's public operating approach as of 4 November 2026. It is not a legal amendment, appointment instrument, government accreditation, audit certification, or a replacement for an independently authenticated source. Earlier digitally signed files remain available as historical editions.

SECTION 01

Trust begins with a reliable record

A credible public claim should be traceable to the office and system that authorised it. MYCDIC uses publication records, member references, appointment records and document fingerprints for different purposes; no one control substitutes for the others.

- A reference proves a record can be located; it does not by itself prove that an appointment or document is current.
- An integrity hash detects file changes when compared against a trusted record.
- An institutional signature should be shown as valid only after the relevant verification check succeeds.

SECTION 02

Access and accountability

Administrative access should match the staff member's remit, not simply their title. Permissions for publishing, editing members, signing documents and inspecting sensitive submissions must be separate and reviewable.

- Require individual accounts and explicit permissions for privileged actions.
- Record sensitive changes with actor, time, object and outcome.
- Revoke or adjust access promptly after reassignment or departure.
- Apply additional authentication to privileged operations where supported.

SECTION 03

Personal data and retention

The Council processes personal information for defined activities, including membership administration and applications. The relevant team should request only information necessary for that activity and retain it for an approved purpose.

- Avoid placing identity documents, personal photographs, private correspondence or case evidence in public directories.
- Separate public member profiles from application evidence and internal screening notes.
- Define retention, deletion and incident response according to applicable law and documented policy.

SECTION 04

Document authenticity and versioning

A PDF can be edited after publication, and a QR code alone is not a digital signature. The document register must distinguish the public information page, the current file, the historical file and an actual signed verification result.

- Keep original signed editions intact when publishing a new editorial edition.
- Use immutable publication references and display revision dates.
- Do not label a newly revised file cryptographically signed before the authorised system has recorded and checked it.

SECTION 05

Security operations and incident handling

A technical incident should have a defined report, triage and follow-up path. Incident content must be restricted to those performing containment, correction or lawful notification.

- Capture time, affected system, symptoms, evidence and immediate response without exposing secrets.
- Prioritise prevention of further harm and accurate records over public assurances.
- Separate vulnerability reporting from general correspondence and publish only validated outcomes.

SECTION 06

Accessibility and responsible automation

Digital services should remain usable across languages, devices and assistive technologies. Automation can support routing, summarising and document processing but should not silently replace accountable human decisions.

- Provide clear labels, keyboard access and readable error states on public forms.
- Check language direction for Arabic content and avoid unreadable fallback PDFs.
- Review automated decisions, protect submitted information and explain material limitations.

Document control and use

Record	/documents/records/digital-trust-framework/
Related page	/trust-center.aspx
Current edition	2026.11 | 4 November 2026
Prior edition	The earlier secured PDF is retained as an archival version.
Integrity	SHA-256 is provided in the downloadable sidecar. A digest is not a digital signature.

For binding legal texts, verified appointments, safeguarding decisions or current regional listings, consult the relevant official record and competent issuing office. Public descriptions should not be read as conferring government, consular or diplomatic authority.