MOROCCAN YOUTH COUNCIL FOR DIPLOMATIC AND INTERNATIONAL COOPERATION

GENERAL SECRETARIAT - OFFICIAL DOCUMENT REPOSITORY

Digital Trust Framework

INSTITUTIONAL PLATFORM AND PROGRAMME BRIEF

OFFICIAL DOCUMENT REFERENCE

DOC-AE8E4F13A302

Repository path: documents/platform/MYCDIC_Digital_Trust_Framework.pdf

Original content fingerprint: 9EB67CBEC1F453494150BAD2B25E637F7D2BA2AA...

DOCUMENT PURPOSE AND STATUS

This cover identifies the attached publication as a document distributed through the official MYCDIC institutional repository. The original document begins on the following page and has been preserved without changing its substantive text, page order, or visual content.

WHAT THIS RECORD CONFIRMS

- The enclosed file was present in the MYCDIC institutional document repository when this cover was generated.
- The visible SHA-256 fingerprint can be used to detect changes to the original enclosed file.
- The QR code opens the official online location assigned to this publication.

LIMITATION AND USE

Unless the enclosed publication expressly states otherwise, this file does not create diplomatic status, public authority, appointment, accreditation, membership, funding commitment, contractual obligation, or permission to represent MYCDIC. Current validity should be checked through the official website.

SCAN TO OPEN OFFICIAL FILE

INSTITUTIONAL DIGITAL VALIDATION

General Secretariat of MYCDIC

Signature ID: GS-DD4690C8D0E2120B

Validation: HMAC-SHA256

Fingerprint: SHA-256

DD4690C8D0E2120B093FD92848DE4004F4A4BBD227875B6770F91A85374392EB

MOROCCAN YOUTH COUNCIL FOR DIPLOMATIC AND INTERNATIONAL COOPERATION

Trust, Security and Digital Responsibility

Public overview of MYCDIC privacy, retention, application security, vulnerability disclosure, service continuity, responsible AI, and accessibility responsibilities.

Public portal	/trust-center.html
Security contact	contact@mycdic.org
Version date	1 August 2026

Implementation references

- W3C Web Content Accessibility Guidelines 2.2
- OWASP Application Security Verification Standard 5.0

Important qualification

These standards are implementation references. This document is not a certification or claim of complete conformity.

Identity information

Identity information submitted through official application processes is not published and should be accessed only by authorized reviewers for defined purposes.

Fields marked as coming soon or to be published are not yet available as validated public data. This file does not create legal authority, accreditation, or representation rights.

MYCDIC CONTROLLED DIGITAL RECORD | MYC-PDF-MYCDIC-DIGITAL-TRUST-918FE2C9 | SIG RSA-D2B5CFFCE7DA986E4B
SHA-256 FINGERPRINT A36576C5C0184DBFA3C63233011611A936099F5E6DDB6BAB333ABB8ADAB8DD2B
2/4
SCAN TO VERIFY

Institutional Application Annex

DOCUMENT

Digital Trust Framework

INSTITUTIONAL USE NOTE

This annex expands how the existing controlled document should be applied within MYCDIC. It does not silently replace the core text. Where the underlying document contains legal, statutory, registration, appointment or other authoritative wording, that original wording remains controlling unless a separately approved instrument expressly amends it.

Operational principles

Authority & scope

Use the document only within the mandate, office, programme or activity to which it actually applies. No publication or title may be read as conferring diplomatic, governmental or legal authority that MYCDIC does not possess.

Decision records

Material approvals, delegations, exceptions and risk decisions should be traceable to an authorized office, a dated record and an identifiable institutional reference.

Integrity & safeguarding

Apply conflict-of-interest, confidentiality, dignity, anti-harassment, data minimization and safeguarding standards proportionately to the activity and the people involved.

Public communication

External statements, branding, media activity and partner references should be accurate, reviewable and consistent with approved institutional positions and published records.

Category-specific implementation expectations

- Define the programme or platform purpose, owner, intended users, data boundaries and approval model before adding features or collecting information.
- Use role-based access and data minimization so participants see only what is needed for their legitimate task.
- Keep public evidence, internal operations and confidential personal information in appropriately separated records.
- Build verification, auditability and clear source-of-truth rules into workflows that create certificates, appointments, applications or public claims.
- Track outcomes with evidence and methodology; do not substitute invented impact figures or unverified claims for measured results.
- Maintain continuity plans for dependencies, credentials, backups, owners and external services so a programme does not depend on one individual account.

Control, Review & Digital Validation

Governance lifecycle

1

Apply

Use the document in the approved institutional context and identify the responsible office or role.

2

Record

Keep proportionate evidence of significant approvals, decisions, incidents, exceptions and outcomes.

3

Review

Reassess the document when law, institutional structure, risk, technology, mandate or operating practice materially changes.

4

Publish

Where publication is appropriate, expose only the public version and keep sensitive operational records separated.

Evidence and institutional recordkeeping

A controlled MYCDIC record should identify the applicable document version, decision owner where relevant, date, affected programme or office, and any evidence necessary to demonstrate responsible implementation. Public records must not disclose confidential personal data, private applicant material, security credentials, or information whose publication would create unnecessary risk.

DIGITAL VALIDATION RECORD

REFERENCE	MYC-PDF-MYCDIC-DIGITAL-TRUST-918FE2C9
SIGNATURE ID	RSA-D2B5CFFCE7DA986E4B
PUBLIC KEY	MYCDIC-RSA-E8A93889B01EEB70
SOURCE SHA-256	918FE2C9468E1AB38AAD3431A67B3DB2 7713406D25089E9F9B28202908CB515F
TEXT FINGERPRINT	EFED2F228C3FEEA3F75572E54A52F564 308B42E947F11169F5456771EAC681BF
RSA SIGNATURE	RR/2Qftv/XJYLS8Mef+v/5lSVMHAzYZI1mMYAlWLpeJKubGLSdUXXY06qcWsyH2aTQYdjV WXpXPL4vHv7/1NamSuQpDwK2L+xpEY8mLrHOR54IWgsuMBmr1ejxYxuRuvZ9AWcF5wret/ wLZiVCFdNY7OCi3KVTsFOVtLDMj5XYN7zof1lA9VD2QBpk+SShbuIi7dLgSlTlpMTRJNhb diQqGMwxGFFgGfuW3reUOC3YRTYjFGVMPde8BKS8NXlUQ2vKzMlFCnN0BLIMs5SyIl0YKc

SCAN TO VERIFY LIVE