MOROCCAN YOUTH COUNCIL FOR DIPLOMATIC AND INTERNATIONAL COOPERATION

GENERAL SECRETARIAT - OFFICIAL DOCUMENT REPOSITORY

Integrity Ethics Safeguarding Framework

INSTITUTIONAL PLATFORM AND PROGRAMME BRIEF

OFFICIAL DOCUMENT REFERENCE

DOC-1427DA693488

Repository path: documents/platform/MYCDIC_Integrity_Ethics_Safeguarding_Framework.pdf

Original content fingerprint: E8CBC0343D40383C0F82994677B3AA8F4D7EF34B...

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-5974029A731AA4E2

Validation: HMAC-SHA256

Fingerprint: SHA-256

5974029A731AA4E2BBFBF24AC3876D98747043CD13281B9368EC80195145C8F7

MOROCCAN YOUTH COUNCIL FOR DIPLOMATIC AND INTERNATIONAL COOPERATION

Integrity, Ethics and Safeguarding Framework

Public reporting framework for misconduct, safeguarding, harassment, discrimination, conflicts of interest, fraud, impersonation, unauthorized fundraising, and data protection incidents.

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

Reporting routes

- General complaints through the Submit a Complaint page
- Confidential or anonymous reports through the Integrity Center
- Private case tracking using a reference and tracking code

Review principles

- Need-to-know access
- Conflict-of-interest routing
- Good-faith non-retaliation commitment
- Protection of unnecessary personal data

Public limitations

Operational investigation procedures and sensitive security details are not published.

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-INTEGRITY-ETHICS-E593DE85 | SIG RSA-BC62146A6648583950

2/4

SHA-256 FINGERPRINT 9442DB49C233DE289124B63F462D30C5D66EA1837240440D670196ACF1DF9EAB

SCAN TO VERIFY

Institutional Application Annex

DOCUMENT

Integrity Ethics Safeguarding 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-INTEGRITY-ETHICS-E593DE85
SIGNATURE ID	RSA-BC62146A6648583950
PUBLIC KEY	MYCDIC-RSA-E8A93889B01EEB70
SOURCE SHA-256	E593DE85368BFBE6830B5FF8BCCBD710 7DFC9A4EE08D2C0260EC6CEC5DDFCE40
TEXT FINGERPRINT	7DDB396C6A204ED52FF7028E44221544 46855E7BC94EA8D40DCD009C1AEE3C17
RSA SIGNATURE	fbC9OZT1iiVfp2f8T8teP+AUuU0y1wcLOp8DvW+syxysxkJF3rQSeU6inhUKjfiqdsanhL WCqaYp1gYERPApxD3XbhA2E3Qiazrmj1jk2RNWyUtZ1IBctLj46J6JJnREO58WIHxXdMQJ My/2JvM/2j7G2rpf13Cp4YFxUuXhCEBhfIm6uyzb1udEzvT/xpIbEqBm6wjK14xbKb4wzW yDcbN2Mjksflk43CDnhNbER/SvNv9qK9uw8OWE58bsW14H4TZ7sWp8NLmWI6ttsPFFQuMG

SCAN TO VERIFY LIVE