Controlled institutional document

Compliance and Enforcement Policy

DOCUMENT REFERENCE

MYC-DOC-2026-1C3FFD7F796A

ISSUED / SECURED

2026-08-07T16:40:15 UTC

SOURCE SHA-256

2346373DCEC12D17440EC0DD7C667FCFC32956B4846B17C6430145CB3D5F32DD

SIGNATURE ID

GS-EB08E31490826EB3

Scan to verify this controlled document against the MYCDIC integrity register.

DIGITAL VALIDATION SIGNATURE (HMAC-SHA256)

EB08E31490826EB33B2E52476FC3396C
516EA0BD8004CB2BE9367128FCAB978E

How to validate this file

The SHA-256 shown on this page identifies the original uploaded evidence before this security page was attached. The MYCDIC register also stores the SHA-256 of the final secured PDF. A file is authentic only when the live verification service confirms the final hash and signature record.

CONTROL NOTICE

Do not rely on screenshots, extracted pages or renamed copies as proof of authenticity. Verify the complete PDF through the official MYCDIC register.

General Secretariat of MYCDIC · Institutional digital validation

MOROCCAN YOUTH COUNCIL FOR DIPLOMATIC AND INTERNATIONAL COOPERATION

GENERAL SECRETARIAT / CONTROLLED PUBLIC POLICY

Compliance and Enforcement Policy

INSTITUTIONAL POLICY AND GOVERNANCE DOCUMENT

Effective date	27 April 2025
Document status	In force / controlled public edition
Institutional owner	General Secretariat of MYCDIC
Reference note	Official 2025 institutional edition - controlled maintenance

Institutional effect. This document governs conduct and internal institutional practice within its scope. It does not create diplomatic status, public authority, employment, contractual rights, or authority to bind MYCDIC unless a separate approved instrument expressly provides otherwise.

MYCDIC CONTROLLED DIGITAL RECORD | MYC-PDF-COMPLIANCE-ENFORCEMENT-CB58AF82 | SIG RSA-C1ABCB682D964D195B
SHA-256 FINGERPRINT CF2663E1A9240E2E11A7E3C12DD5368B2958D37962D2DD83893CE8E3636D72B5

1. Purpose and institutional scope

This Compliance and Enforcement Policy sets the minimum standards applicable to MYCDIC members, Youth Ambassadors, office-holders, staff, volunteers, delegates, authorized account users and other persons acting under the Council's name within the scope described in this document.

The policy protects both the Council and the individuals who serve it by clarifying authority, expected conduct, decision controls, evidence standards and the separation between institutional roles and personal activity.

2. Existing policy framework

1 Introduction

The Moroccan Youth Council for Diplomatic and International Cooperation (MYCDIC) is dedicated to fostering excellence, integrity, and professionalism in youth diplomacy and international cooperation. To uphold these values, MYCDIC enforces strict compliance with its policies, including the Code of Conduct, Diplomatic Protocols, Membership Guidelines, Event Protocols, and Social Media Policy. This Compliance and Enforcement Policy outlines the processes for monitoring adherence, reporting violations, investigating allegations, and implementing disciplinary actions.

This policy ensures that all MYCDIC members, MYCDIC Youth Ambassadors, staff, volunteers, and affiliates (collectively referred to as “Representatives”) maintain the organization’s standards, protecting its reputation and mission. It promotes a transparent, fair, and confidential approach to compliance and enforcement.

2 Scope and Application

This policy applies to:

All MYCDIC Representatives, including those involved in events, programs, or online activities.

Violations of MYCDIC policies, including but not limited to:

Code of Conduct (https://mycdic.org/documents/code-of-conduct.pdf).

Diplomatic Protocols (https://mycdic.org/documents/diplomatic-protocols.pdf).

Membership Guidelines (https://mycdic.org/documents/membership-guidelines.pdf).

Event Protocols (https://mycdic.org/documents/event-protocols.pdf).

Social Media Policy (https://mycdic.org/documents/social-media-policy.pdf).

The policy covers activities conducted in-person, virtually, or online, whether in Morocco or internationally, that are associated with MYCDIC.

3 Objectives

The Compliance and Enforcement Policy aims to:

MYCDIC CONTROLLED DIGITAL RECORD | MYC-PDF-COMPLIANCE-ENFORCEMENT-CB58AF82 | SIG RSA-C1ABCB682D964D195B
SHA-256 FINGERPRINT CF2663E1A9240E2E11A7E3C12DD5368B2958D37962D2DD83893CE8E3636D72B5

SCAN TO VERIFY

Ensure adherence to MYCDIC's policies and ethical standards.

Provide a fair and transparent process for reporting and addressing violations.

Protect MYCDIC's reputation and the well-being of its community.

Foster accountability and continuous improvement among Representatives.

4 General Principles

Compliance and enforcement activities are guided by the following principles:

Fairness: Investigations and disciplinary actions are conducted impartially, with respect for all parties.

Confidentiality: Reports and investigations are handled discreetly to protect privacy.

Non-Retaliation: MYCDIC prohibits retaliation against individuals reporting violations in good faith.

Transparency: Processes and outcomes are communicated clearly, subject to confidentiality requirements.

Proportionality: Disciplinary actions are commensurate with the severity of the violation.

5 Compliance Monitoring

5.1 Oversight

Compliance Committee: A dedicated MYCDIC Compliance Committee, appointed by the Leadership Council, oversees policy adherence. The Committee includes representatives from membership, communications, and leadership teams.

Regular Audits: The Committee conducts periodic reviews of events, social media, and member activities to ensure compliance.

Training: All Representatives must complete mandatory training on MYCDIC policies, with refresher courses annually or as needed.

5.2 Proactive Measures

Policy Accessibility: All policies are available at https://mycdic.org/documents and provided during onboarding.

Monitoring Tools: The Communications Team monitors official social media accounts and public references to MYCDIC.

Feedback Channels: Representatives are encouraged to provide feedback on policies via compliance@mycdic.org to improve compliance.

6 Reporting Violations

6.1 Reporting Process

How to Report: Submit concerns via:

MYCDIC CONTROLLED DIGITAL RECORD | MYC-PDF-COMPLIANCE-ENFORCEMENT-CB58AF82 | SIG RSA-C1ABCB682D964D195B
SHA-256 FINGERPRINT CF2663E1A9240E2E11A7E3C12DD5368B2958D37962D2DD83893CE8E3636D72B5
4/11
SCAN TO VERIFY

Email to compliance@mycdic.org.

Confidential online form at https://www.mycdic.org/contact.html.

Required Information: Include:

Description of the violation (e.g., policy breached, date, location).

Names of individuals involved (if known).

Supporting evidence (e.g., screenshots, documents, witness statements).

Anonymity: Anonymous reports are accepted, though providing contact details may aid investigations.

Confidentiality: Reporter identities and report details are protected, shared only with the Compliance Committee and necessary investigators.

6.2 Non-Retaliation

MYCDIC strictly prohibits retaliation (e.g., harassment, exclusion) against individuals reporting violations or participating in investigations. Retaliation is itself a violation and subject to disciplinary action.

6.3 Timeliness

Reports should be submitted as soon as possible, ideally within 30 days of the incident, to ensure effective investigation.

7 Investigation Process

7.1 Initiation

Receipt: The Compliance Committee acknowledges receipt of reports within 48 hours via email or the reporting platform.

Preliminary Review: The Committee assesses the report to determine if it warrants investigation, based on credibility and relevance to MYCDIC policies.

7.2 Investigation

Assignment: The Committee assigns an impartial investigator or panel, excluding individuals with conflicts of interest.

Evidence Collection: Investigators gather evidence, including interviews with the reporter, accused, and witnesses, and review of documents or media.

Timeline: Investigations are completed within 30 days, unless complex cases require extension (notified to relevant parties).

Confidentiality: All parties are required to maintain confidentiality during the investigation.

MYCDIC CONTROLLED DIGITAL RECORD | MYC-PDF-COMPLIANCE-ENFORCEMENT-CB58AF82 | SIG RSA-C1ABCB682D964D195B
SHA-256 FINGERPRINT CF2663E1A9240E2E11A7E3C12DD5368B2958D37962D2DD83893CE8E3636D72B5

SCAN TO VERIFY

7.3 Findings

Report: Investigators submit a report to the Compliance Committee, detailing findings and recommended actions.

Determination: The Committee determines whether a violation occurred, based on a preponderance of evidence.

8 Disciplinary Actions

If a violation is confirmed, the Compliance Committee recommends actions proportionate to the severity of the offense, including:

Verbal Warning: For minor infractions, with guidance on corrective behavior.

Written Warning: Formal documentation of the violation, with a compliance plan.

Mandatory Retraining: Completion of additional training on relevant policies.

Suspension: Temporary removal from MYCDIC activities or membership (e.g., 1–6 months).

Termination: Permanent revocation of membership or affiliation for serious or repeated violations.

Legal Referral: Referral to authorities for criminal or severe violations (e.g., harassment, fraud).

Disciplinary actions are communicated in writing to the individual, with reasons and appeal options.

9 Appeals Process

Eligibility: Individuals subject to disciplinary actions may appeal within 14 days of notification.

Submission: Submit a written appeal to compliance@mycdic.org, detailing grounds for the appeal (e.g., procedural errors, new evidence).

Review: An independent Appeals Panel, appointed by the Leadership Council, reviews the case within 30 days.

Outcome: The panel may uphold, modify, or overturn the decision. Outcomes are final and communicated in writing.

10 Documentation and Reporting

Records: All reports, investigations, and outcomes are documented securely, with access restricted to the Compliance Committee and Leadership Council.

Annual Report: The Committee publishes an anonymized summary of compliance activities (e.g., number of reports, types of violations) to promote transparency, available at https://www.mycdic.org/regulations.html.

Data Protection: Personal data is handled in accordance with MYCDIC's Privacy Policy and applicable laws.

MYCDIC CONTROLLED DIGITAL RECORD | MYC-PDF-COMPLIANCE-ENFORCEMENT-CB58AF82 | SIG RSA-C1ABCB682D964D195B
SHA-256 FINGERPRINT CF2663E1A9240E2E11A7E3C12DD5368B2958D37962D2DD83893CE8E3636D72B5
6/11
SCAN TO VERIFY

11 Training and Support

Compliance Training: Included in onboarding and annual refreshers, covering reporting procedures and policy adherence.

Support Resources: Access guidance via https://www.mycdic.org/documents.html or contact compliance@mycdic.org for assistance.

Whistleblower Support: MYCDIC provides resources for reporters facing retaliation or distress, including confidential counseling referrals.

12 Amendments

This Compliance and Enforcement Policy may be updated to reflect changes in MYCDIC's operations or legal requirements. Representatives will be notified via email and the MYCDIC website. The latest version is available at https://mycdic.org/documents/compliance-enforcement.pdf.

13 Acknowledgment

By participating in MYCDIC activities, Representatives acknowledge their responsibility to adhere to this policy and report violations. Non-compliance may result in disciplinary measures, as outlined herein.

Contact Information

For inquiries about compliance or to report violations, contact:
Moroccan Youth Council for Diplomatic and International Cooperation (MYCDIC)

Email: contact@mycdic.org

Phone: +34 6 14 14 48 14

Website: https://mycdic.org

Headquarters: Madrid, Spain | National Coordinating Office: Rabat, Morocco | International Office: Brussels, Belgium | Spanish NIF: G75872663

Approved by the MYCDIC Leadership Council on April 27, 2025.

Enhanced institutional safeguards

The following provisions strengthen the operational reading of this policy and apply together with the preceding rules.

Authority and representation controls

No member, ambassador, office-holder, volunteer, partner or contractor may bind MYCDIC, make commitments in its name, issue credentials, promise funding, accept legal obligations, or present personal views as an institutional position unless the authority is documented and current.

MYCDIC CONTROLLED DIGITAL RECORD | MYC-PDF-COMPLIANCE-ENFORCEMENT-CB58AF82 | SIG RSA-C1ABCB682D964D195B
SHA-256 FINGERPRINT CF2663E1A9240E2E11A7E3C12DD5368B2958D37962D2DD83893CE8E3636D72B5

SCAN TO VERIFY

Titles, badges, cards, email addresses and public profiles evidence only the status shown in the live MYCDIC record. They must not be used to imply diplomatic immunity, governmental authority, consular powers, state accreditation or any status not expressly granted by the competent authority.

Conflict of interest, gifts and improper advantage

Covered persons must disclose actual, potential and perceived conflicts before participating in a decision, procurement, selection, partnership, evaluation, disciplinary matter or financial transaction.

Bribes, facilitation payments, secret commissions, kickbacks and any improper advantage are prohibited. Gifts or hospitality that could reasonably influence judgment must be declined or declared under the applicable approval process.

Information security and institutional records

Confidential, personal, financial, security, credential, investigation and unpublished strategic information must be handled only through approved systems and shared on a need-to-know basis.

Official records must not be altered, fabricated, backdated, selectively deleted or moved to personal accounts to evade oversight. Where a controlled register exists, the live register prevails over screenshots, forwarded files or private copies.

Safeguarding and non-retaliation

Harassment, intimidation, exploitation, coercion, discrimination, sexual misconduct, abuse of authority and retaliation against a person who raises a concern in good faith are prohibited.

Where safety, safeguarding, evidence preservation or institutional integrity requires it, MYCDIC may apply proportionate interim measures without treating those measures as a final finding.

Interpretation and hierarchy

This policy must be read with the statutes, internal regulations, approved decisions, privacy rules, safeguarding controls and other applicable MYCDIC instruments. Applicable law always prevails where it imposes a higher or mandatory standard.

If two internal rules conflict, the competent governance body determines the controlling rule, taking account of legal hierarchy, date, scope and the specific decision involved.

Risk-based case intake

Reports are triaged by urgency, safeguarding risk, evidence volatility, conflict of interest and potential institutional impact. Immediate safety and evidence-preservation measures may precede a full investigation.

MYCDIC CONTROLLED DIGITAL RECORD | MYC-PDF-COMPLIANCE-ENFORCEMENT-CB58AF82 | SIG RSA-C1ABCB682D964D195B
SHA-256 FINGERPRINT CF2663E1A9240E2E11A7E3C12DD5368B2958D37962D2DD83893CE8E3636D72B5

SCAN TO VERIFY

Investigation safeguards

Investigators must be sufficiently independent from the matter, disclose conflicts, distinguish facts from allegations, preserve source material, document interviews and give affected persons a fair opportunity to respond where this is safe and appropriate.

Evidence and standard of decision

Administrative decisions should rely on the totality of reasonably reliable evidence. Anonymous or indirect information may trigger review but should not, without corroboration, be treated as conclusive proof of serious misconduct.

Sanctions, reasons and appeal

Final decisions should identify the applicable rule, material findings, outcome and any review route. Appeals may correct material procedural error, significant new evidence, conflict of interest or a clearly disproportionate outcome; they are not automatic rehearings.

Accountability, records and continuing obligations

A person who leaves a role remains responsible for confidentiality, return of Council property, non-misuse of credentials and cooperation with legitimate record-preservation or investigation requirements concerning activity during their mandate.

MYCDIC may amend procedures, forms and technical controls without changing the underlying effective date of this institutional edition, provided that substantive policy amendments are approved through the competent governance process.

Acknowledgement

Participation in MYCDIC activities constitutes a duty to read and comply with the instruments applicable to the relevant role. Where acknowledgement is required, electronic acceptance, signed forms, onboarding records or controlled administrative logs may be used as evidence of receipt.

MYCDIC CONTROLLED DIGITAL RECORD | MYC-PDF-COMPLIANCE-ENFORCEMENT-CB58AF82 | SIG RSA-C1ABCB682D964D195B
SHA-256 FINGERPRINT CF2663E1A9240E2E11A7E3C12DD5368B2958D37962D2DD83893CE8E3636D72B5

SCAN TO VERIFY

Institutional Application Annex

DOCUMENT

Compliance Enforcement

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

- Concerns should be triaged by seriousness, safeguarding impact, legal sensitivity, conflicts of interest and immediate risk rather than by seniority or visibility.
- Fact-finding should distinguish allegation, evidence, response and decision, while limiting disclosure to people with a legitimate need to know.
- Interim safeguards may be used where proportionate, but should not be presented as final findings before review is complete.
- Decisions should identify the applicable rule, relevant evidence, reasoning, authorized decision-maker and any corrective or follow-up action.
- Retaliation against good-faith reporting or participation in review processes should be treated as an integrity concern in its own right.
- Records should support accountability while respecting confidentiality, data minimization and the rights of affected persons.

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-COMPLIANCE-ENFORCEMENT-CB58AF82
SIGNATURE ID	RSA-C1ABCB682D964D195B
PUBLIC KEY	MYCDIC-RSA-E8A93889B01EEB70
SOURCE SHA-256	CB58AF82AAA8A3685E20FF78C67D696B EA66CB7E6F5A2D80B0103FCDC9E34B6D
TEXT FINGERPRINT	29DC28C71456073851DB39616CFBD1DE BAAA8B3C804E747433640494BE4C2A53
RSA SIGNATURE	NS46XbpfuAghp2Ioig0Pci/u1+BLV0422gUqp0BsM09WQFsPu1lqVVCzm1baV9in87ZgNm JEXmT9w81W+RS3zfl5HC5MebgGsNolgunIni4B8h/q6XI4KTCfbiAKj3A9rJKnTePmTJam SSVidnS7O7yp7HSJyWljzgLwTvYu6WN2d8+a/k5CSy20wPvFuN2JTMe8lxTj9J3SadTDxF K8iA2UyQHJqD+8KWehkrKdDGoHFJ510U9V2xuI6kiDfol+kSbVZuITdCh5vIoYxTYiiuam

SCAN TO VERIFY LIVE