



VERIFICATION AND TRUST FRAMEWORK POLICY

Effective Year: 2026

1. Introduction

This Verification and Trust Framework Policy establishes the principles, procedures, standards, and governance mechanisms used by the MDOI Foundation to verify users, organisations, prefixes, identifiers, metadata records, and digital objects. The policy is designed to strengthen trust, credibility, transparency, accountability, and reliability across the MDOI ecosystem.

2. Purpose of the Policy

The purpose of this policy is to ensure that information associated with MDOI records can be trusted, verified, and authenticated while maintaining the integrity of identifier services, metadata quality, organisational participation, and digital knowledge stewardship.

3. Scope

This policy applies to all MDOI users, members, organisations, repositories, publishers, institutions, metadata editors, administrators, technical partners, and any entity seeking verification or trust recognition within the MDOI system.

4. Trust Framework Principles

The MDOI Trust Framework shall be guided by the principles of transparency, accountability, authenticity, integrity, traceability, fairness, consistency, interoperability, evidence-based verification, and continuous improvement.

5. Verification Objectives

Verification activities are intended to:

- Increase confidence in registered records.
- Improve metadata reliability.

- Strengthen organisational credibility.
- Reduce fraud and impersonation.
- Support trustworthy scholarly and institutional communication.
- Enhance confidence in persistent identifier services.

6. Verification Categories

The MDOI Foundation may provide verification for:

- Individual Members
- Organisations and Institutions
- Publishers and Journals
- Research Repositories
- Metadata Records
- Digital Objects
- Assigned Prefixes
- API Integrations
- Trusted Partners

Each category may have different verification requirements and review procedures.

7. User Verification

Individual users may undergo verification to confirm identity, institutional affiliation, professional role, or authorised participation within the MDOI ecosystem. Verification may require supporting evidence or documentation.

8. Organisation Verification

Organisations seeking verification may be required to provide evidence of legal existence, institutional affiliation, operational legitimacy, official contact information, website ownership, and authorised representation.

9. Prefix Verification

Assigned MDOI prefixes may be verified to confirm that the prefix holder is authorised to manage identifier registrations under that namespace. Verification may include organisational review, governance assessment, and operational validation.

10. Metadata Verification

Metadata records may be reviewed for completeness, consistency, accuracy, authorship, ownership, publication information, resource descriptions, and compliance with MDOI metadata standards. Verified metadata records may receive enhanced trust indicators.

11. Digital Object Verification

Digital objects may be assessed to confirm their existence, accessibility, ownership, legitimacy, and relationship to submitted metadata. Verification does not necessarily constitute peer review, endorsement, or quality certification.

12. Verification Badges and Indicators

The MDOI platform may display verification badges, trust indicators, status labels, or confidence markers to communicate verification status. Such indicators help users identify records that have undergone verification procedures.

13. Evidence-Based Assessment

Verification decisions shall be based on evidence, documentation, metadata review, technical validation, organisational confirmation, public records, repository information, or other credible sources of verification.

14. Trust Scoring and Quality Indicators

MDOI may implement trust indicators or quality measures based on factors such as metadata completeness, active resolution status, verified ownership, organisational verification, preservation status, and record maintenance history.

15. Ongoing Monitoring

Verification status may be periodically reviewed to ensure continued compliance with MDOI standards. Changes in ownership, affiliation, metadata quality, operational status, or trustworthiness may trigger re-evaluation.

16. Misrepresentation and Fraud Prevention

Any attempt to obtain verification through false information, forged documents, impersonation, misleading metadata, fraudulent claims, or deceptive conduct may result in rejection, suspension, or revocation of verification status.

17. Verification Suspension and Revocation

Verification status may be suspended or revoked where evidence indicates fraud, policy violations, metadata manipulation, organisational misrepresentation, harmful activity, prolonged inactivity, or failure to maintain required standards.

18. Appeals and Reassessment

Users and organisations may request review or reconsideration of verification decisions. Appeals should include relevant evidence, corrections, supporting documentation, or clarification necessary for reassessment.

19. Trust and Transparency

The Foundation shall seek to maintain transparent verification procedures while protecting sensitive information. Public trust indicators should communicate verification outcomes without unnecessarily exposing confidential data.

20. Relationship to Other Policies

This policy operates alongside the Metadata Policy, Governance and Ethics Policy, Information Security Policy, Privacy and Data Protection Policy, Identifier Resolution Policy, and Content Moderation and Misuse Policy.

21. Compliance Requirements

Verified entities must continue complying with all applicable MDOI policies, ethical requirements, metadata standards, legal obligations, and operational responsibilities. Verification does not exempt a user or organisation from compliance obligations.

22. Enforcement

The Foundation may investigate misuse of verification status, fraudulent trust claims, unauthorised use of badges, false representation, or attempts to undermine trust mechanisms. Appropriate sanctions may be applied where necessary.

23. Policy Review and Updates

This policy shall be reviewed periodically to reflect technological developments, governance improvements, trust infrastructure enhancements, user feedback, international best practices, and evolving verification requirements.

24. Conclusion

The Verification and Trust Framework Policy strengthens confidence in the MDOI ecosystem by promoting authenticity, accountability, transparency, and responsible participation. Through rigorous verification and trust mechanisms, the Foundation

supports a reliable and credible digital knowledge infrastructure for researchers, institutions, publishers, repositories, and global communities.