INFORMATION SECURITY POLICY

Effective Year: 2026

1. Introduction

This Information Security Policy establishes the rules, responsibilities, and security controls required to protect the MDOI Foundation's digital infrastructure, dashboard platform, metadata registry, identifier resolution system, user accounts, organisational records, uploaded files, API services, and related information assets.

2. Purpose of the Policy

The purpose of this policy is to ensure the confidentiality, integrity, availability, reliability, and resilience of the MDOI system. It provides a framework for preventing unauthorised access, data loss, misuse, cyber threats, service disruption, and compromise of trusted identifier infrastructure.

3. Scope

This policy applies to all MDOI users, staff, administrators, developers, metadata editors, organisation administrators, viewers, auditors, technical partners, and third-party service providers who access or manage MDOI systems, data, metadata, files, APIs, dashboards, or infrastructure.

4. Information Security Principles

MDOI shall be guided by the following security principles: confidentiality, integrity, availability, accountability, least privilege, secure-by-design, privacy-by-design, auditability, resilience, and continuous improvement.

5. User Account Security

All users must protect their login credentials and must not share account access with unauthorised persons. Passwords must be encrypted, securely stored, and managed

according to platform security standards. Users must report suspected account compromise, unusual activity, or unauthorised access immediately.

6. Access Control

MDOI shall use role-based access control to ensure that users only access the functions and records necessary for their assigned roles. Permissions shall be assigned based on user category, such as individual user, organisation administrator, metadata editor, viewer, auditor, or system administrator.

7. Authentication and Login Protection

The platform shall implement secure authentication measures, including encrypted passwords, secure session management, login monitoring, and, where applicable, two-factor authentication. Suspicious login attempts may be blocked, logged, reviewed, or escalated.

8. Data and Metadata Protection

All user data, organisational records, identifier records, metadata, uploaded files, logs, and system records must be protected from unauthorised access, alteration, disclosure, deletion, or misuse. Security controls shall be applied to preserve metadata accuracy, identifier trust, and platform reliability.

9. File Upload Security

Uploaded files shall be subject to reasonable security checks, including file type validation, size limits, malware scanning where available, and restricted access controls. Users must not upload harmful, unlawful, malicious, or unauthorised files to the MDOI system.

10. API Security

MDOI API services shall be protected through secure API keys, authentication, access permissions, rate limiting, monitoring, and logging. Users and organisations must not share API credentials or use API access for scraping, abuse, system overload, unauthorised integration, or security bypass.

11. Audit Logging and Monitoring

The system shall maintain audit logs of important activities, including account access, identifier registration, metadata updates, visibility changes, file uploads, API usage, role changes, and administrative actions. Logs may be reviewed to detect misuse, investigate incidents, and support accountability.

12. System Availability and Continuity

MDOI shall take reasonable measures to maintain reliable access to the dashboard, metadata registry, identifier resolver, and related infrastructure. These measures may include backups, monitoring, maintenance planning, redundancy, incident response, and disaster recovery procedures.

13. Security Incident Management

Any suspected or confirmed security incident shall be assessed, contained, investigated, documented, and resolved as quickly as reasonably possible. Where required, affected users, organisations, service providers, or authorities may be notified.

14. Infrastructure Security

Servers, databases, storage systems, resolver services, and application environments shall be configured and maintained securely. Security updates, access restrictions, backup procedures, monitoring tools, and system hardening practices shall be applied where appropriate.

15. Third-Party Service Providers

Where MDOI uses hosting providers, payment processors, communication tools, analytics systems, or technical partners, such providers must support reasonable security, confidentiality, and compliance standards. Third-party access shall be limited to authorised operational purposes.

16. Data Backup and Recovery

MDOI shall maintain appropriate backup procedures for critical system data, metadata records, identifier records, and operational files. Backup and recovery processes shall support continuity, preservation, and restoration in the event of accidental loss, technical failure, cyber incident, or service disruption.

17. Prohibited Security Activities

Users must not attempt to hack, disrupt, overload, reverse-engineer, bypass access controls, upload malware, exploit vulnerabilities, scrape restricted data, impersonate another user, misuse API services, or interfere with the operation of the MDOI infrastructure.

18. Administrative Responsibilities

System administrators and authorised technical personnel must follow secure operational procedures, protect privileged access, maintain confidentiality, document

critical changes, monitor system health, and act promptly on security alerts or identified risks.

19. User Responsibilities

Users must use the MDOI system responsibly, maintain accurate account information, protect credentials, comply with all security notices, avoid suspicious links or unauthorised tools, and promptly report security concerns to the Foundation.

20. Compliance

This policy supports compliance with applicable information security, data protection, intellectual property, digital governance, and institutional requirements. Users and organisations must also comply with relevant laws, regulations, contractual obligations, and ethical standards.

21. Enforcement

Violation of this policy may result in warnings, restricted access, suspension of dashboard privileges, revocation of API access, account termination, removal of harmful content, or other actions necessary to protect MDOI infrastructure and users.

22. Policy Review and Updates

This policy may be reviewed and updated periodically to reflect emerging cyber threats, platform improvements, legal requirements, infrastructure changes, and community feedback. Continued use of the MDOI system constitutes acceptance of the updated policy.

23. Conclusion

This Information Security Policy strengthens trust in the MDOI ecosystem by protecting digital records, metadata, identifiers, users, organisations, and technical infrastructure. By following this policy, all participants contribute to a secure, reliable, and resilient digital knowledge infrastructure.