

Field	Value
Document ID	GOV-MLR-001
Version	1.0
Effective Date	December 2024
Document Owner	Chief AI Officer
Classification	Internal Use
Review Cycle	Annual

Table of Contents

Model Registry & Catalog Governance Standard..... 1

1. Executive Summary..... 1

2. Purpose and Business Objectives..... 1

2.1 Primary Purpose..... 1

2.2 Business Objectives..... 1

2.3 Strategic Alignment..... 2

3. Scope and Applicability..... 2

3.1 Organizational Scope..... 2

3.2 Model Type Coverage..... 3

3.3 Lifecycle Stage Coverage..... 3

3.4 Geographic and Regulatory Scope..... 4

4. Regulatory and Standards Framework.....4

4.1 ISO 42001:2023 Artificial Intelligence Management Systems..... 4

4.2 NIST AI Risk Management Framework..... 5

4.3 Additional Regulatory Alignment.....5

5. Governance Structure and Authority Matrix..... 6

5.1 Decision Rights Authority Matrix..... 6

5.2 Comprehensive RACI Matrix..... 7

5.3 Governance Bodies and Committees..... 8

6. Model Registry Technical Architecture..... 9

6.1 Core Infrastructure Components..... 9

6.2 API Architecture and Specifications..... 10

6.3 Data Architecture and Schema Design..... 11

6.4 Integration Architecture..... 12

7. Model Registration and Metadata Standards..... 13

7.1 Mandatory Registration Fields..... 13

7.2 Model Lineage and Provenance Tracking..... 15

7.3 Performance Metrics and Validation Standards..... 16

8. Model Promotion and Approval Workflows..... 18

8.1 Automated Validation Gates..... 18

8.2 Manual Review and Approval Process..... 19

8.3 Exception Handling and Emergency Procedures..... 21

9. Access Control and Security Framework.....	22
9.1 Role-Based Access Control Matrix.....	22
9.2 Authentication and Authorization Framework.....	23
9.3 Comprehensive Audit and Monitoring.....	25
10. Integration with Enterprise Systems.....	26
10.1 CI/CD Pipeline Integration.....	26
10.2 Enterprise Monitoring Integration.....	28
10.3 Data Ecosystem Integration.....	29
11. Compliance Monitoring and Reporting.....	30
11.1 Regulatory Compliance Framework.....	30
11.2 Automated Compliance Monitoring.....	31
11.3 Audit Support and Evidence Management.....	32
12. Performance Monitoring and Metrics.....	34
12.1 Operational Performance Indicators.....	34
12.2 Model Governance Effectiveness Metrics.....	36
12.3 Continuous Improvement Analytics.....	37
13. Training and Change Management.....	39
13.1 Comprehensive Training Program.....	39
13.2 Change Management Strategy.....	42
13.3 Knowledge Management and Documentation.....	43

Model Registry & Catalog Governance Standard

1. Executive Summary

This governance standard establishes the comprehensive framework for implementing and operating an enterprise Model Registry & Catalog as the authoritative system of record for all machine learning models within the organization. The standard addresses regulatory compliance requirements under ISO 42001:2023, NIST AI Risk Management Framework, and emerging AI regulations while providing operational excellence for AI/ML lifecycle management.

The Model Registry & Catalog serves as the central control point for:

- Model inventory management and version control across all development environments
- Automated governance gates ensuring compliance before production deployment
- Complete audit trails supporting regulatory examinations and risk assessments
- Standardized metadata collection enabling model interpretability and lineage tracking
- Role-based access controls protecting intellectual property and sensitive model information
- Integration with enterprise systems supporting DevSecOps and MLOps workflows