AI MODEL GOVERNANCE POLICY

of

Cosmix LLP

DOCUMENT INFORMATION

Document:	AI MODEL GOVERNANCE POLICY
Document Number:	COS/POL/14
Version:	1.0
Document Date:	17-06-2026
Prepared By:	HOD-IT
Reviewed By:	CISO
Approved By:	CEO
Classification Level:	Internal

Modification History

Sl. No.	Description of Change	Review Date	Version No.
1	Initial Basic Release	**17-06-2026**	1.0

Contents

1. PURPOSE

- LLP acknowledges that effective management of software development activities, system configurations, and technology changes is essential for maintaining a secure, stable, and reliable information technology environment.
- The purpose of this Policy is to establish a structured framework to ensure that applications, software solutions, infrastructure components, and system changes are developed, configured, tested, approved, and implemented in a controlled manner.
- This Policy aims to:
  (i) Ensure security requirements are incorporated throughout the application lifecycle;
  (ii) Prevent unauthorized development activities, configuration modifications, and system changes;
  (iii) Maintain the confidentiality, integrity, and availability of organizational information assets;
  (iv) Reduce operational and security risks arising from incorrect configurations, vulnerable applications, or uncontrolled changes;
  (v) Ensure traceability, accountability, and appropriate approvals for all technology-related modifications.

This Policy establishes requirements for secure software development practices, configuration governance, and controlled change implementation within LLP.

2. SCOPE

- This Policy applies to all applications, software components, information systems, infrastructure elements, configuration items and technology resources that are developed, implemented, managed, or supported by LLP.
- The Policy applies to Designated Partners, Employees, IT and application support teams, Developers, Consultants, Contractors, External vendors and service providers involved in development, maintenance, configuration, or change activities.
- The requirements defined under this Policy shall be followed throughout the lifecycle of technology assets, including planning, development, testing, deployment, modification, maintenance, and retirement.

3. POLICY STATEMENT

LLP shall maintain defined controls for software development, configuration management, and change implementation activities. All technology changes shall be evaluated, approved, tested, and implemented through controlled processes to ensure business continuity and information security.

The organization shall ensure:

(i) **Secure development and maintenance of applications:** Applications shall be designed and maintained considering security, reliability, and business requirements.

(ii) **Controlled system configurations:** System configurations shall be documented, monitored, and modified only through authorized processes.

(iii) **Authorized and tested changes:** Changes shall undergo appropriate assessment and testing before implementation.

(iv) **Segregation of responsibilities:** Roles related to development, approval, testing, and deployment shall be appropriately separated.
(v) **Availability of records and evidence:** Relevant documentation shall be maintained to demonstrate compliance and accountability.

4. SECURE SOFTWARE DEVELOPMENT & APPLICATION SECURITY CONTROLS

(A) Secure Development Practices

- LLP shall ensure security requirements are considered during all stages of software development and enhancement.
- Development activities shall follow secure practices to minimize vulnerabilities, ensure applications meet business and security expectations.

(B) Development, Testing and Production Environment Control

- Development, testing, and production environments shall be appropriately separated to prevent unauthorized changes and operational impact.
- Access to each environment shall be restricted based on roles, responsibilities, and business requirements.

(C) Application Security Testing

- Applications and major modifications shall undergo appropriate testing before being deployed into production.
- Security reviews, vulnerability checks, and functional validations shall be performed to identify and address potential risks.

(D) Source Code Management

- Source code shall be securely maintained to protect organizational intellectual property and prevent unauthorized modifications.
- Access to source code repositories shall be restricted and all modifications shall be traceable through appropriate version control mechanisms.

(E) Third-Party Development Controls

- Third-party developers and service providers shall comply with LLP security and confidentiality requirements.
- External development activities shall be monitored and reviewed before acceptance and implementation into business environments.

5. CONFIGURATION MANAGEMENT

(A) Configuration Identification and Control

- LLP shall maintain proper identification and management of system configurations supporting business operations.
- Configuration details shall be documented and controlled to ensure accuracy, security, and operational stability.

(B) Configuration Inventory Management

- An updated inventory of applications, hardware, software and configuration components shall be maintained.
- Periodic reviews shall be conducted to identify unauthorized components and ensure accuracy of records.

(C) Baseline Configuration Management

- Approved baseline configurations shall be established for critical systems and applications.
- Any deviation from approved configurations shall be reviewed, authorized, documented, and monitored.

(D) Secure Configuration Requirements

- Systems shall be configured according to security requirements and approved hardening standards.
- Unnecessary services, applications, and access permissions shall be disabled or restricted to reduce security risks.

6. CHANGE MANAGEMENT

(A) Change Management Process

- All application, infrastructure, and configuration changes shall follow a formal change management process.
- The process shall ensure changes are properly evaluated, approved, tested, implemented, and monitored.

(B) Change Request Initiation

- All planned changes shall be initiated through a documented change request process.
- Change requests shall include business justification, impact assessment, implementation details, and rollback plans.

(C) Review and Approval

- Changes shall be reviewed by relevant stakeholders before implementation.
- Approval shall consider business impact, security risks, technical feasibility, and testing outcomes.

(D) Testing and Validation

- Changes shall be tested before production deployment to ensure functionality and security requirements are achieved.
- Testing evidence and approval records shall be maintained for verification and audit purposes.

(E) Production Deployment and Post Implementation Review

- Only authorized personnel shall implement approved changes into the production environment.
- Post implementation verification shall be performed to confirm successful deployment and identify any unexpected issues.

(F) Emergency Changes

- Emergency changes may be implemented through an expedited process where immediate action is required.
- Such changes shall be documented, reviewed, and validated after implementation to ensure effectiveness.

7. ACCESS CONTROL AND SEGREGATION OF DUTIES

- LLP shall implement appropriate access restrictions and role separation to reduce unauthorized activities.
- Development, approval, testing, and deployment responsibilities shall be separated wherever possible to maintain accountability.

8. DOCUMENTATION AND MONITORING

- Records related to development activities, configurations, changes, testing, and approvals shall be maintained securely.
- Periodic monitoring and reviews shall be performed to ensure compliance with this Policy and identify improvement opportunities.

9. EXCEPTION MANAGEMENT

- Any deviation from this Policy shall follow the approved exception management process.
- Exceptions shall be documented, risk assessed, approved by authorized personnel and reviewed periodically.