COMPLIANCE & REGULATORY POLICY

of

Cosmix LLP

DOCUMENT INFORMATION

Document:	COMPLIANCE & REGULATORY POLICY
Document Number:	COS/POL/07
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

- The purpose of this Policy is to establish guidelines to ensure that LLP's information systems, business processes, and operations comply with applicable legal, regulatory, contractual and information security requirements.

- This Policy aims to protect organizational information assets, prevent compliance breaches, ensure responsible handling of information, and support effective governance through regular monitoring, reviews and improvements.

2. SCOPE

- This policy applies to all information assets, systems, applications, processes and resources managed or accessed by LLP under its Information Security Management System (ISMS) framework.

- This policy applies to founders, partners, employees, consultants, contractors and third-party personnel accessing organizational information or systems.

- All users shall ensure compliance with applicable security requirements while handling organizational information.

3. POLICY STATEMENT

A) Legal, Regulatory and Contractual Compliance

- LLP shall identify, document and comply with applicable statutory, regulatory, legal, contractual and business requirements relevant to its operations and information systems.

- Appropriate controls, responsibilities, and processes shall be established to ensure continued compliance and timely response to changes in applicable requirements.

B) Intellectual Property and Software Compliance

- LLP shall ensure that all software, applications, digital content and other resources are used in accordance with applicable licensing terms and intellectual property requirements.

- The organization shall:
  (i) Use only authorized and properly licensed software;
  (ii) Maintain software inventory and licensing records;
  (iii) Restrict unauthorized installation of applications;
  (iv) Review and approve open-source, freeware, or third-party software before usage.

- Users shall not use unauthorized software or resources that may create legal or security risks.

C) Protection and Retention of Records

- Important business, legal, regulatory, and security-related records shall be identified, maintained, and protected throughout their retention period.

- LLP shall ensure:
  (i) Records are protected against unauthorized access, modification, loss or destruction;
  (ii) Retention requirements are defined;
  (iii) Records can be retrieved when required for business, audit, or legal purposes.

D) Privacy and Protection of Personal Information

- LLP shall ensure appropriate protection of personal and confidential information collected or processed during business activities.

- The organization shall:

(i) Collect personal information only for legitimate business purposes;
(ii) Restrict access based on business need;
(iii) Prevent unauthorized sharing or disclosure of personal information;
(iv) Ensure compliance with applicable privacy and data protection requirements.

E) Security Compliance and Reviews

- LLP shall periodically review compliance with information security policies, standards and procedures.

- The organization shall conduct appropriate assessments, including technical reviews, vulnerability assessments and security evaluations for critical systems, where required.

- Identified gaps, risks and non-compliance issues shall be documented and addressed through corrective actions.

F) Cryptographic and Security Controls

- Where required, LLP shall implement appropriate encryption and security controls to protect sensitive information.

- Cryptographic measures shall be applied considering information sensitivity, business requirements, and applicable legal obligations.

4. REVIEW AND MONITORING

- LLP shall conduct periodic reviews of information security practices to assess effectiveness of controls, identify improvement areas, and ensure continued compliance.

- Review findings shall be documented, communicated to responsible stakeholders and corrective actions shall be implemented where required.

5. POLICY REVIEW & EXCEPTIONS

- Review annually or earlier if laws, technology, audits or incidents require.
- Exceptions must be documented, risk-assessed, reviewed and approved.