AI POLICY

of

Cosmix LLP

DOCUMENT INFORMATION

Document:	AI POLICY
Document Number:	COS/POL/02
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 Full Release	**17-06-2026**	1.0

Contents

1. PURPOSE

- LLP recognizes that Artificial Intelligence (AI) and Generative Artificial Intelligence (GenAI) technologies can significantly enhance productivity, innovation, knowledge management, and service delivery. At the same time, the use of such technologies introduces legal, ethical, privacy, security and operational risks that require appropriate governance and oversight.
- This Policy establishes the principles, responsibilities, and minimum control requirements governing the acquisition, development, deployment, and use of AI systems within LLP. The objective is to encourage responsible innovation while ensuring that AI systems are used in a manner that is transparent, secure, fair, accountable and compliant with applicable legal and regulatory requirements.
- Through this Policy, LLP seeks to:
  (i) Promote responsible and trustworthy use of AI technologies;
  (ii) Protect client, employee, and organizational information;
  (iii) Ensure appropriate human oversight of AI-assisted activities;
  (iv) Mitigate risks arising from bias, inaccuracies, privacy breaches, and misuse of AI;
  (v) Support compliance with applicable laws, regulations, contractual obligations and recognized industry standards.

2. SCOPE

- This Policy applies to all partners, employees, consultants, contractors, interns, temporary staff & third-party service providers who utilize, develop, procure, manage, or interact with AI systems on behalf of LLP.
- The requirements of this Policy extend to all AI and GenAI solutions operating within the organization's information systems, business processes, client engagements, advisory services and support functions.
- This Policy forms part of the organization's Information Security Management (ISM) and shall be read in conjunction with applicable information security, privacy, acceptable use, data protection, and risk management policies.

3. RISK CATEGORIZATION AND COMPLIANCE

LLP adopts a risk-based approach towards the deployment and use of AI systems. The level of governance, oversight, and control applied to an AI system shall be proportionate to the potential impact of that system on individuals, business operations, clients, regulatory compliance, and organizational reputation.

AI systems shall be classified into the following categories:

(i) **Minimal Risk:** Applications with limited impact that support routine business activities and do not materially affect individual rights or business decisions.

(ii) **Limited Risk:** AI systems that generate content, recommendations, summaries, or communications requiring transparency measures and user awareness.

(iii) **High-Risk:** AI systems used in areas such as recruitment, legal analysis, compliance monitoring, financial assessments, governance reviews, or any activity where outputs may materially influence decisions, rights, obligations, or regulatory outcomes.

(iv) **Prohibited Uses:** AI applications that conflict with applicable laws, ethical standards, human rights principles, or organizational values shall not be permitted.

4. TRANSPARENCY, ACCOUNTABILITY & KEY PRINCIPLES

- LLP is committed to ensuring that AI technologies are deployed responsibly and in a manner that promotes trust, accountability, and transparency.
- Appropriate documentation shall be maintained regarding the purpose, intended use, capabilities, limitations, and governance requirements applicable to AI systems.
- Individuals using AI technologies shall be adequately trained to understand the benefits, limitations, risks, and responsibilities associated with such systems.
- Where appropriate, users, clients, and stakeholders shall be informed when they are interacting with AI systems or receiving AI-generated content.
- The organization shall periodically review AI systems to evaluate compliance with internal requirements, regulatory expectations, ethical principles, and risk management objectives.

- Key Principles taken into consideration are as follows:

(A) Lawful, Fair and Transparent Use

- ❖ AI solutions shall be implemented in accordance with applicable legal, regulatory, and ethical requirements, including internationally recognized AI governance frameworks, where relevant.
- ❖ Individuals shall be appropriately informed whenever AI-generated content or AI-enabled interactions form part of client-facing services or communications.
- ❖ Privacy and data protection assessments shall be undertaken for AI applications involving sensitive or personal information, wherever required under applicable laws.

(B) Purpose Limitation & Data Minimization

- ❖ Data used by AI systems shall be limited to legitimate, defined, and authorized business purposes.
- ❖ The organization shall take reasonable measures to avoid the use of unauthorized, copyrighted, inaccurate, biased, or unreliable datasets while developing or configuring AI solutions.

(C) Human-Centricity & Human-in-the-Loop

- ❖ AI technologies shall support informed human decision-making and shall not replace professional judgement in critical or high-impact activities.
- ❖ Appropriate Human-in-the-Loop (HITL) controls shall be maintained for AI applications where human review, validation, or intervention is necessary before decisions are finalized

(D) Bias and Discrimination Prevention

AI systems shall be periodically evaluated to identify and mitigate bias, discrimination, or unintended outcomes, using recognized industry practices and appropriate governance frameworks.

(E) Ethics and Professional Conduct Principles

The organization shall ensure that AI systems are designed, deployed, and used in accordance with the following principles:

- Integrity
- Fairness and Non-Discrimination
- Accountability
- Transparency
- Privacy and Confidentiality
- Respect for Human Rights
- Professional Competence and Due Care
- Security and Safety
- Responsible Innovation

Employees shall not rely solely on AI-generated outputs where professional judgement is required.

AI-generated outputs shall never be knowingly used to mislead, deceive, manipulate, or create unfair outcomes for customers, employees, regulators or other stakeholders.

(F) Responsible AI Usage

- AI systems shall be used only for legitimate business purposes approved by the organization.
- Users shall remain accountable for decisions, recommendations, and outputs generated using AI systems.
- AI shall assist and augment human decision-making and shall not replace professional judgement in critical business processes.
- Employees shall not use AI systems for unlawful, discriminatory, deceptive, fraudulent, or unethical purposes.
- Confidential, proprietary, personal, or client information shall not be uploaded to public AI platforms without appropriate authorization and safeguards.
- AI-generated outputs shall be validated before use in business, legal, financial, regulatory, customer-facing, or strategic activities.

(G) AI Output Disclaimer Requirements

- All AI-generated content shall be treated as advisory or assistive output unless independently reviewed and approved by authorized personnel.
- Users shall be informed whenever content, recommendations, communications or decisions are generated wholly/ partially using AI.
- Appropriate disclaimers shall accompany AI-generated content shared externally where required.
- AI outputs shall not be represented as verified professional advice unless reviewed by qualified personnel.

- ❖ Users must recognize that AI systems may generate inaccurate, incomplete, outdated, or misleading information and therefore outputs must be independently validated before reliance.

(H) Explainability and Traceability of AI Systems

- ❖ AI system owners shall ensure that appropriate documentation is maintained regarding AI model functionality, intended use, limitations, assumptions, and known risks to support transparency and accountability.
- ❖ For high-risk or business-critical AI applications, appropriate mechanisms shall be implemented to understand the factors influencing AI-generated recommendations, classifications, or decisions.
- ❖ AI-generated outputs that may impact legal, financial, compliance, regulatory, client, or business decisions shall maintain sufficient traceability, including relevant input information, AI system details, output generated, and human review performed, wherever applicable.
- ❖ AI systems shall be periodically evaluated to ensure that outputs remain understandable, reliable, and aligned with intended business objectives.
- ❖ Where AI solutions are obtained from third-party providers, LLP shall seek appropriate transparency regarding model behaviour, limitations, training approach, and available explainability documentation.
- ❖ Explainability considerations shall be incorporated throughout the AI lifecycle, including AI selection, development, deployment, monitoring, and retirement activities.

5. DATA PROTECTION AND PRIVACY

LLP shall ensure that the processing of personal data through AI and Generative AI systems is carried out in compliance with applicable privacy and data protection laws, including the GDPR, the DPDP Act, 2023, internationally applicable AI framework and other relevant regulatory requirements.

To support this objective:

- Privacy risk assessments, including a Data Protection Impact Assessment (DPIA), shall be conducted where required before deploying AI systems that process personal data.
- Personal data used for AI training or processing shall be collected and used only for lawful and authorized purposes, with appropriate consent or other legal basis wherever applicable.
- Suitable privacy controls, such as data minimization, anonymization, or pseudonymization, shall be implemented to protect personal information.
- AI solutions involving large-scale processing of personal data shall be reviewed to ensure the processing is lawful, transparent, and aligned with the intended business purpose.

(A) Data Ingestion and Data Quality

The quality, integrity and legality of data used by AI systems directly influence the reliability and trustworthiness of AI-generated outputs. Accordingly, LLP shall ensure that all data collected, imported, or ingested into AI systems is managed in a secure, lawful and controlled manner.

- AI systems shall ingest only data that is relevant, accurate, authorized, and necessary for the intended business purpose.
- Prior to ingestion, datasets shall be assessed for quality, completeness, accuracy, potential bias and compliance with applicable legal, contractual, and regulatory obligations.
- Personal, confidential, proprietary, or client information shall only be ingested into AI systems where there are a valid business purpose and appropriate legal basis for processing.
- Unauthorized, copyrighted, confidential, or unlawfully obtained datasets shall not be used for AI model training, fine-tuning, testing, or inference.
- Appropriate validation controls shall be implemented to prevent corrupted, manipulated, malicious, or inaccurate data from being introduced into AI systems.
- Data ingestion activities shall be appropriately documented to maintain traceability, accountability, and auditability throughout the AI lifecycle.

(B) Data in Transit Security

Information exchanged between users, AI platforms, cloud services, applications, APIs and integrated systems shall be protected against unauthorized access, interception, alteration, or disclosure while in transit.

LLP shall ensure that:

- Data transmitted to or from AI systems is protected using industry-recognized secure communication protocols and encryption mechanisms.
- Secure APIs, encrypted communication channels, and authenticated connections shall be used for all AI integrations and data exchanges.
- Confidential, personal, regulated or client information shall not be transmitted through unsecured/ unauthorized communication channels.
- Access to AI interfaces and connected services shall be restricted to authenticated and authorized users only.
- Data transfers involving third-party AI providers shall comply with applicable contractual, regulatory, cross-border data transfer, and privacy requirements.
- Network communications supporting AI services shall be monitored for suspicious activity and unauthorized data transmission.

(C) AI Data Breach and Security Incident Management

Any actual or suspected security incident involving AI systems or AI-processed information shall be promptly reported, investigated, contained, and managed in accordance with the organization's Information Security Incident Management procedures.

The organization shall ensure that:

- AI-related data breaches, unauthorized disclosures, prompt injection attacks, model poisoning, data leakage, or unauthorized access attempts are immediately reported to the designated Information Security function.
- Appropriate containment measures are implemented to minimize operational, legal, financial, and reputational impacts.

- ❖ Root cause analysis shall be performed for significant AI-related security incidents, and corrective actions shall be implemented to prevent recurrence.
- ❖ Where required by applicable laws or contractual obligations, affected clients, regulators, or relevant authorities shall be notified within the prescribed timelines.
- ❖ Incident records shall be maintained to support investigations, regulatory compliance, audit requirements, and continual improvement of AI governance controls.
- ❖ AI systems affected by security incidents shall be reviewed before being restored to production environments to ensure that identified vulnerabilities have been adequately addressed.

6. HUMAN OVERSIGHT AND ACCOUNTABILITY

Even with high levels of automation, the local and internationally accepted Acts requires human oversight, especially for high-risk systems. The company should ensure:

- AI systems shall be continuously monitored, and authorized personnel shall have the ability to intervene, suspend, or override system outputs whenever necessary.
- Human oversight shall be maintained throughout the lifecycle of high-risk AI systems.
- Authorized personnel shall have the authority to review, override, suspend, or terminate AI-generated recommendations or decisions.
- Critical decisions involving employment, legal matters, financial reporting, taxation, safety, compliance, customer rights, or regulatory obligations shall require human review and approval.
- AI systems shall be designed to allow timely human intervention whenever abnormal, biased, inaccurate, or unexpected outcomes are detected.
- Escalation procedures shall be established for AI-related incidents requiring management review.

7. TRAINING & AWARENESS

- Mandatory GenAI ethics training for all employees.
- Role-based training programmes shall be conducted to ensure personnel possess the knowledge and skills necessary for the responsible use of AI technologies.

7.1 Ethical AI Awareness

- Employees shall receive awareness training regarding ethical AI usage, fairness, transparency, bias management, accountability and responsible handling of AI-generated outputs.
- Training shall include AI-related regulatory obligations, privacy considerations, intellectual property risks and professional responsibilities.

8. THIRD-PARTY AI PROVIDERS

Where AI solutions or services are procured from third-party providers, LLP shall conduct appropriate due diligence to ensure that such providers comply with applicable legal, regulatory, contractual and information security requirements.

The organization shall ensure that agreements with third-party AI providers include, at a minimum:

- Provisions requiring compliance with applicable AI governance, privacy, and data protection laws.
- Appropriate transparency regarding the AI system's functionality, limitations, training methodology, and decision-making processes, where relevant.
- Defined responsibilities for managing legal, ethical, operational, and security risks associated with the use of AI services.
- Adequate safeguards for protecting organizational and client information, including confidentiality, data security, and incident reporting obligations.

9. APPLICATION GUIDELINES FOR GENERATIVE AI (GENAI)

A) Legal, Regulatory and Compliance Services

- GenAI may be used to assist in legal research, regulatory monitoring, contract review, policy drafting, compliance assessments, and preparation of advisory documents.
- All legal opinions, compliance recommendations, notices, agreements, regulatory filings, and client deliverables generated or assisted by GenAI shall undergo review and approval by qualified personnel before issuance.
- GenAI outputs shall not be treated as legal advice, regulatory interpretations, or compliance conclusions without human validation.
- Users shall independently verify legal references, case laws, statutory provisions, regulatory updates, and citations generated by AI systems.
- Confidential client information, privileged communications, and sensitive legal documents shall not be uploaded to public AI platforms unless specifically authorized and protected through appropriate safeguards.

B) Risk Management, Governance and Advisory Services

- GenAI may be used to support risk assessments, internal audits, governance reviews, compliance monitoring, control testing, and preparation of management reports.
- AI-generated risk ratings, observations, recommendations, or findings shall be validated by designated reviewers before reliance.
- Explainability and transparency shall be maintained for AI-assisted assessments, particularly where findings may influence management decisions, regulatory reporting, or client engagements.
- High-risk AI applications used in governance, risk, compliance, forensic investigations, or due diligence activities shall be subject to enhanced review and oversight.

C) Client Interaction and Communication

- Clients shall be informed whenever they are interacting with AI-enabled tools such as chatbots, virtual assistants, automated response systems, or AI-assisted communication platforms.
- AI systems shall not impersonate employees, consultants, legal professionals, auditors, or authorized representatives of the organization.
- Reasonable measures shall be implemented to minimize hallucinations, inaccurate responses, or misleading information provided through AI-assisted client interactions.
- All externally shared AI-generated reports, summaries, analyses, presentations, or communications shall be reviewed by authorized personnel before issuance.
- Where appropriate, AI-generated content shall contain suitable disclaimers regarding its AI-assisted nature.

D) Human Resources and Recruitment

- GenAI may be used to assist in job description preparation, candidate communication, interview scheduling, workforce analytics, and recruitment support activities.
- Final hiring, promotion, compensation, disciplinary, performance management, or termination decisions shall not be based solely on AI-generated recommendations.
- Human review and approval shall be mandatory for all employment-related decisions.
- Where AI tools are used for resume screening, candidate ranking, behavioural assessments, or talent analytics, periodic fairness, bias, and discrimination assessments shall be conducted.
- Recruitment-related AI systems shall comply with applicable employment, labour, privacy, and anti-discrimination laws.

E) Marketing, Business Development and Knowledge Management

- GenAI may be used for drafting marketing materials, articles, proposals, presentations, training materials, research summaries and business communications.
- AI-generated content shall be reviewed for accuracy, intellectual property compliance, confidentiality obligations, and regulatory requirements before publication.
- GenAI-generated content shall not contain false, misleading, deceptive, defamatory, discriminatory, or unsubstantiated claims.
- Marketing and promotional content shall comply with applicable consumer protection laws, advertising standards, professional conduct requirements, and contractual obligations.
- AI-generated content shall not infringe copyrights, trademarks, proprietary rights, or confidential information belonging to third parties.

F) Finance, Taxation and Corporate Advisory Services

- GenAI may be used to assist in financial analysis, tax research, corporate compliance tracking, due diligence, documentation support, and preparation of advisory materials.

- AI-generated financial, taxation, accounting, or corporate compliance outputs shall be independently verified by qualified professionals before client reliance or submission to any authority.
- GenAI shall not be used as the sole basis for tax positions, statutory filings, certifications, financial reporting conclusions, or professional opinions.
- Appropriate human oversight shall be maintained for all client-facing financial, taxation, accounting, and advisory deliverables.

10. AI ACQUISITION AND DEVELOPMENT

- The procurement, development or implementation of any new AI or Generative AI solution shall be carried out in accordance with the organization's approved technology acquisition and governance procedures, with all necessary approvals obtained prior to deployment.
- Where AI solutions are sourced from General Purpose AI (GPAI) providers (such as ChatGPT, Gemini, or similar platforms), appropriate documentation relating to the model, training methodology, available datasets, capabilities, limitations, and vendor disclosures shall be obtained and retained, wherever available.
- AI applications classified as high-risk shall undergo controlled testing, validation, and sandbox evaluation before being introduced into the production environment.
- Developers shall ensure that AI-generated content, code, or other outputs do not infringe intellectual property rights, copyrights, licensing requirements, or other proprietary rights of third parties.
- AI system owners and development teams shall maintain adequate documentation covering the AI system's intended purpose, functionality, assumptions, known limitations, risks, and operational controls to support governance, transparency, and ongoing lifecycle management

11. REPORTING AND COMPLIANCE AUDITS

To promote effective AI governance and continued compliance with applicable legal, regulatory, and organizational requirements, LLP shall implement the following measures:

- Designate appropriate personnel or a responsible function to oversee AI governance, monitor AI-related risks, and ensure adherence to this Policy and applicable regulatory obligations.
- Conduct periodic reviews and compliance assessments of AI systems to evaluate their alignment with established governance requirements, security controls, and applicable legal standards.
- Maintain a formal process for reporting, investigating, documenting, and resolving AI-related incidents, non-compliance, or security events. Root cause analysis (RCA) shall be performed where appropriate, and corrective and preventive actions shall be implemented to mitigate recurrence.

12. NON-COMPLIANCE & PENALTIES

- Unauthorized use, deployment, or misuse of AI technologies, including non-compliance with this Policy, may attract appropriate disciplinary or corrective action.
- Periodic compliance assessments and internal or independent audits shall be conducted to evaluate adherence to this Policy and identify opportunities for continual improvement.

13. ROLES AND RESPONSIBILITIES

- The designated business or delivery team shall be responsible for conducting sandbox testing, validating AI solutions prior to deployment, and maintaining records of testing activities and outcomes.
- AI-related risk assessments shall be carried out collaboratively by the respective business functions and the Information Security team before the implementation of AI systems and periodically thereafter, based on risk.
- The designated AI Governance function or authorized personnel shall oversee the monitoring, periodic review, and governance of AI systems operating within the LLP's IT environment.
- Appropriate business and IT teams shall ensure that AI-related logs, audit trails, and operational records are securely maintained in accordance with the organization's logging, monitoring, and record retention requirements.
- The Information Security function shall manage the reporting, investigation, and escalation of AI-related security incidents in accordance with the organization's Incident Management Policy and applicable response procedures.

14. CONCLUSION

LLP is committed to leveraging Artificial Intelligence in a manner that balances innovation with responsibility. By implementing appropriate governance, transparency, security, privacy, ethical safeguards, and human oversight, the organization seeks to maximize the benefits of AI while minimizing associated risks.

This Policy reflects the organization's commitment to responsible AI practices and shall serve as the foundation for the secure, ethical, and compliant adoption of AI technologies across all business operations and client engagements.

The Policy shall be reviewed periodically to ensure continued alignment with evolving regulatory requirements, industry standards, technological developments, and organizational objectives.