DATA PROTECTION & PRIVACY POLICY

of

Cosmix LLP

includes,

(i) Data Masking policy
(ii) Data Retention and Disposal policy
(iii) Confidentiality policy
(iv) Threat Intelligence policy
(v) Data Protection and Information Security (IS) policy

DOCUMENT INFORMATION

Document:	DATA PROTECTION & PRIVACY POLICY
Document Number:	COS/POL/01
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

The purpose of this Policy is to establish standards, controls, and procedures for protecting information assets, confidential data, systems, networks and technology infrastructure.

This Policy provides a framework for:

- Protection of confidential and sensitive information;
- Management of cybersecurity risks and incidents;
- Secure collection, processing, storage, and disposal of data;
- Compliance with applicable laws, contractual obligations, and industry practices;
- Prevention of unauthorized access, disclosure, alteration, or destruction of information.

This policy sets forth the basic principles by which the LLP processes/protect the personal data of customers, suppliers, business partners, employees, and other individuals, and indicates the responsibilities of its business departments and employees while processing personal data.

2. SCOPE

The policy sets the minimum standard and shall guide all COSMIX LLP employees and Agents even if local law is less restrictive. This policy is applicable to all scenarios where personal data is involved.

3. POLICY STATEMENT of organisation i.e., LLP

This policy establishes the principles, requirements and governance framework for the secure classification, protection, retention, handling, masking, storage, disposal, privacy management, threat intelligence and cybersecurity operations related to LLP's data, information assets, systems, networks and digital infrastructure, in compliance with applicable legal, regulatory, contractual, and business requirements. The policy aims to strengthen Cosmix LLP's overall cybersecurity and privacy posture through the implementation of appropriate administrative, technical and physical security controls to protect information assets against unauthorized access, disclosure, alteration, disruption, loss, misuse, cyber threats, and other security incidents. It further supports the continuous improvement of LLP's security capabilities through effective threat intelligence operations, proactive identification and communication of Indicators of Compromise (IOCs), implementation of data masking and information classification practices and adoption of privacy principles aligned with GDPR 2016/679, the Digital Personal Data Protection Act, 2023, AICPA GAPP and other applicable laws.

This policy also defines governance requirements, data retention requirements, cybersecurity monitoring, incident response, risk management and procedures to ensure appropriate organizational and technical measures are implemented for safeguarding sensitive and critical information throughout its lifecycle and maintaining the confidentiality, integrity and availability of Cosmix LLP information assets and services.

4. DATA MASKING POLICY

LLP shall ensure that sensitive data is adequately protected through appropriate data masking controls to prevent unauthorized access, disclosure, misuse, or identification of individuals and confidential business information. Data masking shall be implemented as an additional layer of protection over standard information security controls such as access management, encryption and monitoring.

a) Data Classification

- Sensitive data requiring masking shall include Personally Identifiable Information (PII) such as names, addresses, phone numbers, email IDs, location data, biometric information, financial information, employee records, customer data, vendor data, and other confidential business information.
- Data shall be classified based on sensitivity, criticality, legal, regulatory, and contractual requirements before applying masking controls.

b) Data Masking Techniques

LLP shall implement appropriate masking techniques based on business and security requirements, including:

- Randomization – replacing original data with random values
- Substitution – replacing data with fictitious but realistic values
- Tokenization – replacing sensitive data with unique tokens
- Format-Preserving Encryption (FPE) – encrypting data while maintaining original format
- Shuffling – rearranging data records to protect privacy

c) Masking Scope and Environment

- Data masking may be applied to full datasets or selected subsets of data.
- Masking shall primarily be implemented in non-production environments such as development, testing, quality assurance, analytics, training, and third-party integrations.

d) Data Masking Process

The data masking process shall include:

- Identification and discovery of sensitive data across systems, applications, and databases
- Classification of data based on sensitivity levels
- Definition and documentation of masking rules for each data category
- Execution of masking activities using approved automated tools, scripts, or technologies
- Validation and testing to ensure masked data remain usable for business and testing purposes
- Periodic review, monitoring and enhancement of masking controls based on evolving threats and regulatory requirements.

e) Approval and Documentation

- Necessary approvals shall be obtained from data owners and relevant stakeholders prior to implementing masking activities.
- Detailed documentation of masking procedures, techniques, rules, and exceptions shall be maintained.

f) Data Retention and Disposal

- Masked data shall be retained, stored and securely disposed of in accordance with applicable legal, regulatory, contractual, and organizational retention requirements.

g) Compliance, Monitoring and Training

- Regular audits, compliance assessments, and monitoring activities shall be conducted to ensure the effectiveness of the data masking program.
- Appropriate incident response procedures shall be established for handling any security incidents involving masked data.
- Employees involved in data masking activities shall receive periodic training and awareness on masking techniques, tools, and regulatory requirements.

Data Masking Procedure

(i) **Data Discovery** - Identify systems, applications, and databases containing sensitive data requiring masking.

(ii) **Data Classification -** Classify data based on sensitivity, criticality, and applicable legal or regulatory requirements.

(iii) **Masking Rules -** Define masking rules and select appropriate masking techniques for different categories of sensitive data.

(iv) **Masking Execution -** Perform data masking using approved tools, scripts, or automated methods to protect sensitive information.

(v) **Testing and Validation -** Validate that masked data remains usable for business, testing and development purposes without exposing original data.

(vi) **Documentation -** Maintain records of masking activities, rules, tools used, approvals, and validation results.

(vii) **Monitoring and Maintenance -** Periodically review and update masking controls, techniques and procedures to ensure continued effectiveness.

(viii) **Compliance and Auditing -** Conduct regular audits and compliance assessments to ensure adherence to the Data Masking Policy and regulatory requirements.

(ix) **Incident Response -** Establish procedures to report and address incidents or breaches involving masked data.

(x) **Training and Awareness -** Provide periodic training and awareness to employees involved in data masking activities.

5. DATA RETENTION AND DISPOSAL

(A) Data Retention

Introduction/ Preface

(a) LLP maintains IT system records to Support business operations and comply with legal, regulatory and industry requirements. This policy ensures records are retained for the required period, remain accessible when needed, and are securely disposed of when eligible.

(b) Improper retention or premature destruction of records may expose LLP to legal, regulatory, or business risks.

(c) All employees and vendors of LLP handling records must comply with this policy.

Requirements - Records not subject to a Legal Hold Notice

Data Retention Policy requires that -

i. Records not subject to a Legal Hold Notice or Permanent Records Notice must be retained and destroyed according to Data Destruction and Media Disposal.
ii. Retention periods and destruction dates must follow approved business, legal, and regulatory requirements. No discretionary Changes are allowed unless approved by the LLP's information security team.
iii. Destruction of eligible records should be automated wherever possible to ensure a consistency.
iv. Regular audits must be conducted to verify compliance with this Policy.
v. Financial transaction records must be retained for a minimum 8 years from the record date.

Exception: Backup tapes used solely for business continuity or disaster recovery are not official business records. Their retention should be based on continuity and recovery requirements.

Requirements - Records subject to a Legal Hold Notice

Data Retention Policy requires that -

i. Legal and regulatory may issue a Legal Hold notice for records related to litigation, investigations, audits, or other critical matters.
ii. Records under a Legal Hold must be preserved as required.
iii. Legal Hold remains effective until formally evoked in writing.
iv. Recipients must notify relevant personnel and ensure identified records are protected.
v. Compliance with Legal Hold directives is mandatory.

(B) Data Destruction and Disposal

Introduction/ Preface
Data must be securely destroyed once its retention period expires.

Requirements

i. Paper and electronic records eligible for disposal and not under legal hold must be securely destroyed. E-waste disposal must follow the Electronic Waste Disposal Guideline.
ii. Paper records must be shredded. Electronic data may be deleted or media sanitized without destroying the storage device.
iii. Records under litigation or legal hold must not be destroyed until all holds are removed.

(C) Media Disposal

Introduction/ Preface
Storage media must be properly sanitized to prevent data recovery. Sanitization methods include clearing, purging, and destruction, depending on data classification.

Requirements

i. Media must be sanitized according to the highest classification of data stored on it.
ii. Media containing only Public may be cleared, purged, or destroyed.
iii. Media containing internal, confidential, or sensitive data must be destroyed.
iv. Records of media destruction and disposal must be maintained.

Non-Adherence/ Exception - 5(A), 5(B), 5(C)
Any deviation from this policy must be documented separately by LLP.

6. CONFIDENTIALITY POLICY

Data is classified from **least restrictive** to **most restrictive** based on protection and access control requirements.

A) Public Information

Public Information is freely available to the public and does not require authentication or authorization.

Examples:

- Marketing and sales brochure
- Publicly available manuals
- Press releases
- Job postings
- Information on LLP's public websites
- Product and service brochures shared with customers, etc.

B) Internal Information

i. Internal Information is intended for authorized employees or approved third parties.

ii. Unauthorized disclosure could negatively impact LLP, its customers, employees or business partners.

Examples:

- Meeting minutes
- Vendor contracts
- Internal communications and HR notices
- Information security awareness materials

B1) Customer Information:

- Telephone numbers
- Mailing and billing addresses

B2) Business Customer Information:

- Business contact details
- Mailing and billing addresses

B3) Employee Information:

- Contact details
- Performance appraisals
- Time and expense records

B4) Third-Party Information:

- Vendor contracts
- Technical documentation
- Vendor personnel information

C) Confidential Information

Confidential Information includes business-critical data that could cause financial, legal, operational, or reputational harm if disclosed without authorization.
Examples:

- Bank account and financial information
- Departmental financial records
- Purchasing information
- Merger and acquisition documents
- Corporate strategic plans
- Legal and litigation documents
- Product specifications and designs
- Engineering drawings
- Customer payment information, invoices, and billing records.

D) Sensitive Information

Sensitive Information includes personal data that can directly or indirectly identify an individual and requires enhanced protection
Examples:

- Full name
- Date of birth
- Driver's license or |D number
- PAN or tax identification details
- Parent's legal surname
- Background check results
- Credit reports
- Health and medical information
- Passwords, security questions, PINs, and access credentials
- Customer personal details (excluding payment information)

Non-Adherence/ Exception – 6 A), B), C), D)

Any deviation in this policy must be documented separately by LLP.

7. THREAT INTELLIGENCE POLICY

(i) LLP shall establish and maintain a Cyber Threat Intelligence (CT) Program to collect, analyse, and share intelligence on emerging cyber threats.

(ii) Intelligence Sources
Threat intelligence may be gathered from:

- SOC (Security Operation Center) /SIEM (Security Information and Event Management) platforms
- Government and industry intelligence feeds
- Internal security logs and network data
- Open-Source intelligence (OSINT)
- Threat intelligence sharing communities

(iii) Intelligence Analysis and Sharing
Collected intelligence shall be analysed to identify threats and vulnerabilities and shared with relevant stakeholders, including:

- Information Security Team
- IT Operations Team

Indicators of Compromise (IOCs) shall be integrated into security tools such as SIEMs and firewalls to enable real-time detection and response

(iv) Cyber Threat Intelligence Procedure

a. Establish a CTI Team
LLP shall maintain a dedicated Cyber Threat Intelligence (CTI) Team led by the Information Security Head and supported by Information security and IT operation personnel.

b. Identify Intelligence Sources
The team shall identify and subscribe to relevant intelligence feeds and establish procedures for collecting internal security data.

c. Analyse Intelligence
The team shall assess collected intelligence, prioritize threats, and identify vulnerabilities using appropriate tools and techniques.

d. Disseminate Intelligence
Relevant threat intelligence shall be communicated promptly to authorized stakeholders.

e. Support Security Decisions
Threat intelligence shall be used to strengthen security controls and proactively identify, assess, and mitigate risks.

(v) Best Practices

- Periodically review and update intelligence sources.
- Ensure relevant stakeholders receive actionable intelligence.
- Provide regular training to CTI team members.
- Review and improve the CTI program on a scheduled basis.
- Continuously monitor the evolving

(vi) Exception Management

- Security exceptions may be approved when risks are adequately mitigated through compensating controls or when the residual risk is low, acceptable, and does not conflict with minimum security requirements or business needs.
- All exception requests must be approved by the respective Business Head and the information security head or Management representative.

Terms and Definitions

- **Indicator of compromise (IOC) –** Evidence that may indicate a security breach or cyberattack.
- **Threat –** A potential event or action that exploits a vulnerability and negatively impacts system, applications or data.
- **Threat Hunting -** A. proactive process of identifying hidden threats or suspicious activities that bypass traditional security controls.
- **Threat Intelligence -** Information and insights about cyber and physical threats, vulnerabilities, and threat actors used to prevent and mitigate security incidents.

8. DATA PROTECTION AND INFORMATION SECURITY (IS) POLICY

a) Notice

LLP shall inform data subjects about the collection, processing, storage, and disclosure of their personal data through clear and understandable notices in English or any language listed in the Eighth Schedule of the Constitution of India.
The notice shall include:

- Types of personal data collected
- Purpose of collection
- Any legal requirement for collection
- How the data will be used or processed
- Disclosure to third parties and the purpose of such disclosure
- How data subjects can access, correct, or delete their data
- Contact details of the Data Protection Officer/Representative (DPO/DPR)

Where possible, notice shall be provided before or at the time of data collection.

b) Choice and Consent

LLP shall obtain consent where required and clearly communicate available choices regarding the collection, use, or disclosure of personal data.
LLP shall:

- Obtain appropriate consent (opt-in or opt-out)
- Clearly explain available choices and consequences of non-consent
- Use personal data only for agreed purposes
- Obtain fresh consent for new purposes
- Inform data subjects of their right to withdraw consent
- Consent requirements shall comply with applicable laws and regulations.

c) Collection

LLP shall collect personal data fairly, lawfully, and only as necessary for specified purposes. LLP shall:

- Follow data minimization principles
- Clearly identify mandatory and optional data fields
- Comply with applicable laws
- Obtain verifiable parental/guardian consent for minors where required
- Collect data directly from data subject's whenever possible bat
- Ensure third-party data collection complies with privacy requirements

d) Storage, Usage and Retention

Personal data shall be processed, stored, and retained only for legitimate business, legal, or contractual purposes and in accordance with:

- Stated purposes
- Obtained consent
- Applicable laws and regulations

Data shall be retained and disposed of according to the guidelines mentioned section 5 of this policy.

e) Access

LLP shall enable data subjects to exercise their privacy rights, including:

- Access to personal data
- Rectification of inaccurate data
- Ensure of data no longer required
- Restriction of processing where applicable
- Data portability
- Objection to processing for direct marketing

Requests may be submitted through designated email addresses or forms communicated in Privacy notices.

f) Cookie Management

LLP shall maintain a Cookie Policy and obtain consent for cookies where required by law.

- Cookie consent banners shall be displayed on public-facing websites and applications.
- The Legal Team shall review and approve the Cookie Policy.
- The policy shall be reviewed periodically to ensure compliance.

g) Disclosure and Third-Party Transfer

Personal data may be shared with authorized third parties for legitimate business purpose. LLP shall:

- Disclose data only for notified purposes
- Obtain consent where required
- Require third parties to implement privacy and security controls
- Restrict subcontracting without prior written approval
- Ensure third parties process data according to agreed requirements
- Business owners managing third-party relationships are responsible for compliance.

h) Security

LLP shall implement appropriate administrative, technical, organizational, and physical safeguards to protect personal data from unauthorized access, disclosure, alteration, loss, or destruction.

i) Data Integrity and Quality

LLP shall maintain personal data that is accurate, complete, relevant, and up to date, and encourage data subjects to update their information when necessary.

j) Monitoring and Enforcement

LLP shall monitor compliance with this policy and applicable privacy regulations. Activities include:

- Managing privacy-related inquiries and complaints
  Investigating and responding to incidents and breaches
- Conducting privacy compliance assessments
- Performing annual Privacy Impact Assessments (PIA) and Data Protection impact Assessments (DPIA)
- Providing regular privacy awareness training

Violations may result in disciplinary action, including termination of employment or contracts, and may lead to legal consequences.

k) Breach Notification

- In the event of a personal data breach, LLP shall notify relevant stakeholders, regulatory authorities and affected individuals, without undue delay and in accordance with applicable legal requirements.
- Where notification is delayed, the reasons shall be documented. Additional notification requirements shall apply where mandated by regulations such as GDPR.

Exemptions

In specific circumstances permitted by law, LLP may process personal data without notice or consent, including:

- Criminal investigations
- Protections of individuals or public safety
- Compliance with legal obligations
- Audits and regulatory reviews
- Legal claims and emergency situations

Roles and Responsibilities

(i) LLP through its designated partners approves privacy strategies and major policy exceptions.

(ii) Responsibility of Data Protection Representative (DPR)

- Managing the privacy program
- Monitoring legal and regulatory changes
- Updating privacy policies and notices
- Handling privacy exceptions
- Delivering privacy awareness training
- Monitoring compliance

(iii) Legal Department - Supports privacy compliance, legal interpretation, and regulatory obligations.

(iv) Responsibility of IT Security Team

- Security systems used to process personal data
- Conducting security monitoring and assessments

(v) Business Units and Privacy Representatives - Responsible for implementing privacy requirements within their respective functions.

Exception

Exceptions to this policy may be approved by the LLP through its designated partners were justified by legal, regulatory, or operational requirements and supported by appropriate compensating controls.

References

- EU General Data Protection Regulation (GDPR)
- Digital Personal Data Protection Act, 2023 (India)
- AICPA Generally Accepted Privacy Principles (GAPP)

9. Key Definitions

- **Personal Data:** Information that identifies or can identify and individual
- **Sensitive Personal Data:** Special categories of personal information requiring enhanced protection.
- **Processing:** Any operation performed on personal data.
- **Data Quality:** Accuracy, completeness, and relevance of data.
- **Explicit Consent:** Direct and affirmative agreement,
- **Implicit Consent:** Consent inferred from actions or circumstances.
- **Information Security:** Protection of confidentiality, integrity, and availability of information.

10. Policy Review

This policy shall be reviewed annually by LLP through its Information Security Team, considering compliance assessments, audit findings, and emerging risks. Updated versions shall be communicated to relevant stakeholders.