ACCEPTABLE USAGE POLICY

of

Cosmix LLP

DOCUMENT INFORMATION

Document:	ACCEPTABLE USAGE POLICY
Document Number:	COS/POL/06
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

Sl. No.	Contents	Page No
1	Purpose	
2	Scope	
3	Policy Statement	
4	Monitoring & Enforcement	
5	Policy Review & Exceptions	

1. PURPOSE

- The purpose of this Policy is to define appropriate and secure usage requirements for LLP's information assets, technology resources, applications, devices, and organizational data.
- This Policy ensures responsible use of information resources, protection of confidential information, prevention of misuse, reduction of cybersecurity risks and safeguarding of LLP's business interests and reputation.

2. SCOPE

This Policy applies to all partners, employees, consultants, contractors and third-party personnel accessing or using LLP's information assets, including:

- Computers, laptops, mobile devices and endpoints;
- Applications, systems, cloud platforms and networks;
- Communication tools and organizational information.
- All users are responsible for ensuring secure and compliant use of organizational resources.

3. POLICY STATEMENT

- Organizational systems, devices, and information shall be used only for authorized business purposes and in accordance with applicable policies, procedures and legal requirements.
- Users shall protect organizational assets, maintain confidentiality of business information and immediately report any loss, theft, unauthorized access, or security incident.
- Devices and systems containing organizational information shall be secured through appropriate controls such as passwords, screen locking and access restrictions.
- Only approved and authorized software, applications and tools shall be installed or used on organizational systems.
- Confidential information shall not be shared through personal email accounts, unauthorized cloud platforms, social media, messaging applications, or other unapproved channels.
- Users shall protect credentials and shall not share passwords, user IDs, access tokens, or use another person's account.
- Access to systems and information shall be provided based on business requirements and the principle of least privilege.
- Users shall not attempt unauthorized access, bypass security controls, introduce malware, conduct unauthorized security testing, or perform activities that may compromise organizational systems.
- Organizational resources shall not be used for illegal, unethical, inappropriate, or unauthorized activities.
- Email and communication platforms shall be used primarily for official business purposes. Confidential information shared electronically shall be protected through appropriate security measures.
- Internet access shall be used responsibly. Users shall not access harmful content, download malicious software, share confidential information publicly, or upload organizational data to unauthorized platforms.
- Antivirus and security controls installed on organizational devices shall remain active and shall not be disabled or modified without authorization.

- External storage devices shall be used only with appropriate approval and security checks.
- Information shared with external parties shall be authorized and protected through appropriate confidentiality and security measures.

4. MONITORING AND ENFORCEMENT

- LLP reserves the right to monitor, review and audit usage of organizational systems and information assets for security and compliance purposes.
- Any misuse, policy violation, unauthorized access or security breach may result in corrective actions, restriction of access rights or disciplinary measures, legal proceedings depending on the severity and impact of the violation.

5. POLICY REVIEW & EXCEPTIONS

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