ACCESS MANAGEMENT POLICY

of

Cosmix LLP

LLPIN: **ACY-1156** GSTN: **29AAWFC5668A1Z0**
Regd. Office: **1st floor, 49/1, Coconut Avenue Road, Malleshwaram, Bangalore North, Bangalore - 560003, Karnataka**
Email: cosmixllp@gmail.com Website: cosmixgroup.com

DOCUMENT INFORMATION

Document:	ACCESS MANAGEMENT POLICY
Document Number:	COS/POL/09
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

LLPIN: **ACY-1156** GSTN: **29AAWFC5668A1Z0**
Regd. Office: **1st floor, 49/1, Coconut Avenue Road, Malleshwaram, Bangalore North, Bangalore - 560003, Karnataka**
Email: cosmixllp@gmail.com Website: cosmixgroup.com

Contents

LLPIN: **ACY-1156** GSTN: **29AAWFC5668A1Z0**
Regd. Office: **1st floor, 49/1, Coconut Avenue Road, Malleshwaram, Bangalore North, Bangalore - 560003, Karnataka**
Email: cosmixllp@gmail.com Website: cosmixgroup.com

1. PURPOSE

The purpose is to establish a framework for managing logical and physical access to LLP's information assets, systems, applications, networks and facilities. The Policy aims to ensure that access is granted only to authorized individuals based on business requirements, thereby safeguarding the confidentiality, integrity and availability of organizational information while minimizing the risk of unauthorized access, misuse, or data compromise.

2. SCOPE

This policy applies to all employees, partners, consultants, contractors, interns, and third-party personnel who access or manage LLP's information assets, technology resources, applications, databases, cloud services, networks and physical locations. It covers the complete lifecycle of user access, including account creation, privilege allocation, review, modification, suspension, and revocation.

3. POLICY STATEMENT

a) Access Control Principles

Access to information and systems shall be granted strictly on the principles of Need-to-Know, Least Privilege, and Role-Based Access Control (RBAC). Users shall be provided only the minimum level of access necessary to perform their assigned responsibilities. Each user shall be assigned a unique user ID to ensure accountability and traceability of activities.

b) User Access Management

User accounts shall be created, modified, and removed only after obtaining appropriate business approval. Access rights shall correspond to the user's job role and be updated promptly whenever responsibilities change. Accounts of employees, contractors, or third-party personnel leaving the organization shall be disabled or revoked without undue delay.

c) Privileged Access

Administrative and privileged access shall be granted only where operationally justified and approved by the designated authority. Such access shall be periodically reviewed and monitored to ensure it remains appropriate and is not misused.

d) Authentication Controls

Users shall maintain the confidentiality of their authentication credentials. Temporary and default passwords shall be changed immediately upon first use, and password practices shall comply with the organization's security requirements. Multi-factor authentication shall be implemented wherever feasible for privileged and remote access.

e) Access Review and Monitoring

User access rights shall be reviewed periodically and after significant organizational changes such as transfers, promotions, or termination of employment. System logs and access records shall be maintained to support monitoring, audit activities, and investigation of security incidents.

f) Physical Access

Access to offices, server rooms, records storage, and other secure locations shall be restricted to authorized personnel through appropriate physical security controls. Visitors shall be managed in accordance with established security procedures.

4. MONITORING AND ENFORCEMENT

All personnel shall comply with this Policy and protect their assigned access privileges. Any unauthorized access, misuse of credentials, or violation of access control requirements may result in disciplinary action, suspension of access rights, contractual action, or legal proceedings, as applicable.

5. POLICY REVIEW & EXCEPTIONS

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