PASSWORD POLICY

of

Cosmix LLP

DOCUMENT INFORMATION

Document:	PASSWORD POLICY
Document Number:	COS/POL/04
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 define clear and consistent standards for password management and clear desk/clear screen practices across LLP. These standards are intended to protect company accounts, applications, and systems from unauthorized access, misuse, and potential cyberattacks.
- Additionally, the clear desk and clear screen guidelines are designed to reduce the risk of sensitive information being exposed or compromised by ensuring that both physical and digital materials are properly secured when not in use.

2. SCOPE

This policy applies to LLP and all associated entities. It is mandatory for all employees, contractors, consultants, and vendors who interact with LLP's information systems or facilities.

The policy covers:

i. Clear desk practices
ii. Clear screen practices
iii. Password management systems
iv. Use of secret authentication information

3. POLICY STATEMENT

3A) Password Policy

- Passwords must be changed at **first login** and updated in every **30 days** thereafter.
- Passwords must be at least **10 characters long** and include a mix of uppercase/lowercase letters, numbers, and special characters.
- The last **five passwords** cannot be reused.
- Accounts lock after **five failed login attempts**; lockout lasts **60 minutes** with reset after **15 minutes**.
- Passwords must remain confidential and never be shared.
- Default application passwords must be changed immediately.
- Special accounts without expiry (e.g., system-level IDs) must be configured as **non-interactive**.
- Administrators must enforce these rules using automated controls.

3B) Clear Desk Policy

- Confidential papers and electronic media must be stored securely in locked cabinets when not in use.
- Printouts and faxes must be collected immediately and not left unattended.
- Meeting rooms, whiteboards, and tables must be cleared after use.
- Departments are responsible for ensuring secure storage of critical materials.
- Access to printers and copiers must be restricted to authorized staff.

3C) Clear Screen Policy

- Computers must be locked before being left unattended.
- Screensavers with password protection must activate after **15 minutes of inactivity**.
- Sensitive files or passwords must not be left visible on desks or screens.
- Employees should remain aware of their surroundings when viewing confidential information to prevent unauthorized viewing.

4. POLICY REVIEW & EXCEPTIONS

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