ANJANI PORTLAND CEMENT LIMITED

CYBER SECURITY POLICY

March 2026

ANJANI PORTLAND CEMENT LIMITED

Regd. Office: #6-3-553, Unit No. E3 & E4, 4th Floor, Quena Square Off: Taj Deccan Road, Erramanzil, Hyderabad – 500082, Telangana
CIN: L26942TG1983PLC157712 Website: www.anjanicement.com

CYBER SECURITY POLICY

Confidentiality Statement

Document Control Document Name	Cyber Security Policy
Document Reference Number	APCL-CSP
Classification	Public
Version Number	R2.0
Date	30.03.2026
Reviewed by	IT Team
Approved by	Board

Revision History Date	Version	Description	Created by
30.06.2025	R2.0	Reviewed Policy	Xxxxx

Distribution

- Intranet Portal
- E-mail

Documentation Status

This is a controlled document. This document may be printed; however, any printed copies of the document are not controlled. The electronic version maintained in the Intranet Portal is the controlled copy.

1. Purpose

This Cybersecurity Policy outlines the principles and guidelines for safeguarding the company's information assets, systems and data against cyber threats and ensuring the protection of sensitive information, in compliance with relevant data protection laws.

2. **Scope**

This policy applies to all employees, contractors, third-party vendors, and any individuals granted access to APCL's information systems and data.

3. **Information Classification**

All information will be classified based on its sensitivity, and appropriate security measures will be implemented to protect each classification level.

Public: Information meant for public disclosure.

Internal: Information restricted to employees and authorized personnel.

Confidential: Highly sensitive information requiring the highest level of protection.

4. **Access Controls**

Access to information systems and data will be granted based on the principle of least privilege. Users will have access rights only to the resources necessary for their role and responsibility.

5. **Password Management**

Secure password practices will be enforced, including regular updates, strong password requirements, and multi-factor authentication wherever applicable.

6. **Data Encryption**

Sensitive data, both in transit and at rest, will be encrypted to protect against unauthorized access.

7. **Network Security**

Firewalls, intrusion detection/prevention systems and other security measures will be implemented to safeguard the integrity and availability of the network.

8. **Incident Response**

A comprehensive incident response plan will be in place to address any cybersecurity incidents promptly. This includes root cause analysis followed by reporting procedures, containment, eradication, recovery, and post-incident analysis.

9. **Employee Training**

Regular training programs on cybersecurity best practices will be provided to all employees. Employees will be informed about the potential risks and consequences of security breaches and the importance of adhering to security policies.

10. **Data Privacy Compliance**

APCL will comply with all applicable data protection laws and regulations.

Personal data will be collected, processed, and stored responsibly and individuals will have the right to access, correct, and delete their personal information.

11. **Third-Party Security**

Vendors and partners with access to company's systems or data will be required to adhere to strict security and privacy standards consistent with this policy.

12. **Audits and Assessments**

Periodic cybersecurity audits and risk assessments will be conducted to identify vulnerabilities and ensure ongoing compliance with this policy.

13. **Reporting Security Concerns**

All employees are encouraged to report any security concerns, potential vulnerabilities or incidents promptly to the designated cybersecurity contact.

14. **Review and Update**

This policy will be regularly reviewed and updated to adapt to evolving cybersecurity threats and changes in the business environment.

15. **Enforcement**

Violation of this policy may result in disciplinary action, including but not limited to suspension, termination, and legal action. All employees are required to report any suspected violations promptly.

16. **Cyber Security Contact Information**

For any Information Technology security concerns or to communicate any potential vulnerabilities or incidents or any doubts in this policy, please contact Shri D Krishnamoorthy, Chief Information Security Officer at dk@chettinadcement.com

The Company is committed to fostering a culture of cybersecurity awareness and responsibility to protect the organization and its stakeholders from the growing risks associated with cyber threats and data breaches.

* * * * * * *