JK LAKSHMI CEMENT Ltd.

CYBER SECURITY POLICY

Title	Cyber Security Policy
Version Number	3
Effective Date	15th May 2023
Authorized By	President & Director
Number of Revisions	2
Last Revised Date	1st April 2021

Purpose: The purpose of this policy is to ensure the confidentiality, integrity, and availability of our Company's information assets, while reducing the risk of unauthorized access, disclosure, or destruction of Company data. This policy establishes guidelines for Employees and Business Partners who access, use, or handle Company information systems and data.

Scope: This policy applies to all Employees, Customers, Vendors who access Company information systems and data, including but not limited to email, network systems, and data storage devices.

1. **Access controls:** Access to Company information systems and data will be granted based on the principle of least privilege, which means that employees and business partners will only be granted access to the systems and data they need to perform their job duties. Access to Company systems and data will be controlled through the use of strong authentication and access controls, including password policies and two-factor authentication where feasible.

2. **Data protection:** All Company data, including personally identifiable information (PII) and intellectual property, must be protected from unauthorized access, disclosure, or destruction. This includes implementing data encryption, implementing physical and logical access controls, regular backup and recovery processes, and limiting the use of portable storage devices.

3. **Network security:** Company networks must be secured to prevent unauthorized access and to protect against cyber-attacks. This includes using

firewalls, intrusion detection and prevention systems, and other security technologies to protect against malware and other security threats.

4. **Email security:** Email is a primary means of communication in our Company, and as such, must be secured against unauthorized access and disclosure. This includes using email encryption for sensitive information, implementing anti-phishing controls, and enforcing the use of strong passwords and two-factor authentication for email accounts.

5. **Incident response:** In the event of a security incident, such as a data breach or cyber-attack, the Company will follow an incident response plan that includes identifying and containing the incident, assessing the damage, notifying affected parties, and implementing remediation measures.

6. **Employee training:** All employees and business partners will receive regular training on cyber security best practices and policies to ensure they are aware of the latest threats, vulnerabilities, and best practices for protecting the Company's network and data their responsibilities in safeguarding Company data.

7. **Third-party security**: Third-party vendors and contractors who access Company systems or data must adhere to the same security policies and standards as Company employees.

Enforcement: Violations of this policy may result in disciplinary action, up to and including termination of employment or contract. business partners who violate this policy may also be subject to legal action in accordance with the IT amendment Act 2008.

This policy shall be reviewed periodically for its suitability and updated as necessary.

Date: 08/05/2023
Place: New Delhi

Arun Shukla
(President & Director)