Information Security Policy

Shree Cement (hereinafter referred as 'Shree Cement' or 'Company') is on a growth path. In the age of digitalization, significant amount of data is generated across its operations. While digitalization helps in improving efficiency, the data becomes vulnerable to IT security incidents. The Company believes that information security is required to be managed diligently to ensure the business continuity.

Purpose

The purpose of this Policy is to maintain security and confidentiality of information assets owned by Shree Cement.

Scope

This Policy applies to all the employees of Shree Cement and its subsidiaries, contract workers, partners, suppliers, customers, third-party and their employees who have access to Shree Cement's premises, systems and information.

This Policy also applies to all the information, computers and data communication systems owned, licensed, and administered by Shree Cement.

All the people covered in the scope of this Policy shall comply with the information security procedures. Failure to do so shall result in disciplinary action.

Policy Principles:

Shree Cement shall:

- Comply with all the applicable national and international regulatory requirements related to Information Technology and cyber security .
- Monitor and review risks related to cyber security and take appropriate preventive, detective & corrective control measures to mitigate the risk.
- Implement system back-up procedures at appropriate frequency based on data protection requirements.
- Protect all the hardware and software assets from physical and cyberattacks.
- Protect confidential information from unauthorized access, use, disclosure, modification, and disposal, whether intentional or unintentional.
- Implement strong information management systems.
- Implement effective information security risk management framework, as part of enterprise risk management framework.
- Structure strong password setting mechanism along with role-based access control to IT systems.
- Protect end points through data leakage prevention.

- Build and maintain a secure network using firewall configuration having necessary capability to protect the IT Asset and information of the company.
- Establish reporting channels in case of any suspicious activity with regards to information security.
- Report, investigate and take appropriate actions for all types of information security breaches.
- Implement Incident Response Plan through effective threat detection and remediation capabilities.
- Promote secured work culture with awareness programs for employees on information security.
- Collaborate with cyber security and data privacy experts to continually improve the information security management system.
- Conduct independent external verification of IT Infrastructure and vulnerability analysis at least twice a year.
- Plan & Implement Business Continuity Procedures & regular testing thereof.

Governance and Responsibility

Head of IT Security and Digital activities in the company is responsible for implementation and review of this policy. The matters related to information security are communicated to risk management committee of the Board of Directors, as part of enterprise risk management framework.

Reporting of an IT Security Incident

Any IT Security related incidents can be reported through incident reporting mechanism defined by the company.

Policy Approval

This Policy was approved by the Board of Directors of the Company at its meeting held on 22nd May 2023 and shall be reviewed periodically.