KANSAI NEROLAC PAINTS LTD.
BUSINESS CONTINUITY POLICY

Business continuity is important for our organization which is catering to both industrial and decorative customers to ensure that our business continuity management arrangements are developed and implemented in a safe, prioritized and structured manner with the commitment of the senior management team.

Objective:

To put-in place a documented framework and process for an effective Business Continuity Plan (BCP) in case of a disaster and meet the following objectives.

- **Disaster Management, Incident Response and Sustainenance of business operations**
- **Minimize the impact of the disaster**
- **Faster recovery of the Operations and services**
- **Communication with customers, employees and all relevant stakeholders.**

Disaster event hereby refers to:

a) Physical Risk (Natural Calamities like Flood, Earthquake, Storms and major accidents like fire)
b) Cyber Security Risks
c) Pandemic Risk
d) Geopolitical Risks (Acts of war, Trade barrier, sanctions, Terrorism)

Scope:

This Business Continuity Policy covers all the Manufacturing Units, R&D Centre, Head Offices, Depots/ Regional Distribution Centres and Regional Offices. This plan applies to the factors which assumes occurrence of a disaster event or a very high impact risk event which can interrupt business.

Approach for Business Continuity:

The approach for Business Continuity adopted by KNPL includes the following:

a) Disaster Management, Incident Response and Sustainenance of business operations: The policy endeavours to ensure business continuity at its own plants as well as at customer sites. As part of this, multiple manufacturing facilities have been set up across the country to take care of business continuity in case of eventuality

b) Minimize the impact of the disaster: The policy endeavours to put-forth systems in place to prevent and early detect the source of a disaster event or a very high impact risk occurrence, in order to minimise the impact of the disaster. Preparedness and counter measures are also examined at regular intervals to deal with such events.

c) Faster recovery of the Operations and Services: The policy endeavours to put in place the Infrastructure and human resource capability to resume the operations and services at the affected site and ensure that minimal loss (Tangible/Intangible) occurs in case of any disaster event and there is optimal backup available.

d) **Communication with customers, employees and all relevant stakeholders:** The policy endeavours to put in place communication with all stakeholders.

Containment Strategy for business continuity

- **Critical manufacturing locations & processes:** Combination of alternate manufacturing facilities to meet the demand during the disaster event based on the type of products manufactured and manufacturing process deployed.

- **R&D location:** Lab infrastructure and testing equipment, as well as intellectual capital, must be protected against damage and loss. Alternate resources to be made available for critical testing equipment.
- **Data recovery:** Create facility to recover and restore its critical enterprise application, technology infrastructure and operations during non-availability of / damage to primary data centre. Ensure business continuity through use of cloud platforms for availability, backup and recovery processes.

- **Point of Sale:** Business continuity at customer site to be sustained by ensuring uninterrupted sale transactions and material supplies through use of backup internet connectivity and completion of transactions from a remote location.
- **Critical human resources talent:** Thorough knowledge management system, important talent and critical skill-sets to be identified and enhanced through cross-skilling and up-skilling.
- **Treating critical documents:** Intellectual property rights, critical statutory documents, land records and records required to be retained as per company law are to be digitalized as backup

- **Treating critical material supplies:** Wherever possible, a multiple vendor selection and on-boarding plan has to be designed.
- **Cyber security**: Ensure processes and controls to secure IT infrastructure viz. computers, servers, mobile devices, networks from malicious cyber-attacks. Undertake third party cyber security audits to detect threats and strengthen the system. Build employee awareness on cyber security.

Authority & Responsibility:

Business Continuity Plan Committee consisting of senior management of the organization (Management Committee) reports to Risk Management committee is responsible centrally for adopting the policy, review and amendments. Management framework for managing the business continuity plan is laid out in the BCP framework. The framework includes identification of key personnel to guide and facilitate the recovery teams at the affected sites for undertaking recovering activities.

Execution

BCP shall not be invoked for addressing day-to-day failures like system failure or an occurrence of incident/ accident not pertaining to business closure.

Review Frequency: Once a year