Prepared by	Viral Joshi
Checked by	Shital Salunkhe
Approved by	Nehal Mehta

Risk and Crisis Management Policy

1. Purpose and Scope

This document outlines the Risk and Crisis Management governance framework for **ANJ Turnkey Projects Private Limited ("ANJ or "The Company")**, a design and build company. It details responsibilities, structures, and procedures for identifying, mitigating, and responding to risks and crises that may affect operations, clients, projects, and reputation of the Company.

2. <u>Governance Structure</u>

2.1) It is the responsibility of the Board of Directors of the Company for Strategic oversight on enterprise risk and crisis response.

2.2) The Managing Director of the Company is responsible for ensuring the integration of risk management into daily operations.

2.3) Health, Safety & Risk Committee of the Company is responsible for Reviews of the project-specific risks and compliance.

2.4) Crisis Management Team (CMT) of the Company is responsible during a crisis to coordinate the response to such a situation.

2.5) Project Managers are responsible to Identify and escalate risks during the project planning and delivery.

3. Risk Management Framework:

3.1) The risk management shall provide reasonable assurance in protection of business value from uncertainties and consequent losses.

3.2) All the employees of the Company shall be responsible for identifying and mitigating key risks in their respective domain.

3.3) All the employees the Company shall ensure efficient usage / allocation of the resources they are entrusted with.

3.4) The occurrence of risk, progress of mitigation plan and its status will be monitored on a periodic basis.

4. Risk Management Procedure:

4.1 Risk Identification

The purpose of risk identification is to identify events that can have an adverse impact on the achievement of the business objectives. Such Risks may, amongst others, be classified into a) strategic; b) operations; c) financial; d) legal / regulatory; e) human resources; f) environmental; g) natural disasters, h) sectoral, i) sustainability, particularly, ESG related risks, j) information, k) cybersecurity etc. The Risk Management Committee shall ensure that risks identified are documented in the form of a risk register ("Risk Register") to be maintained by the Company in the electronic form. Risk Register incorporates risk description, category, classification, mitigation plan and the responsible function / department.

4.2 Risk Assessment

Assessment involves quantification of the impact (to the extent possible) of risks to determine potential severity and probability of occurrence. Each identified risk is assessed on two factors which determine risk exposure:

a) Potential impact if the event occurs; and b) likelihood of the occurrence/ re-occurrence of the event.
b) Risk categories: After taking into account the existing controls, the risks are assessed to ascertain the current level of risk. Based on the above

assessments, each of the risks shall be categorized as – low, medium and high.

4.3 Risk Mitigation

All the identified risks shall be mitigated by using any of the following risk mitigation plans:

a) Risk avoidance: By not performing an activity that could carry risk. However, such avoidance can result in losing out on the potential gain that accepting (retaining) the risk may have allowed.

b) Risk transfer: Mitigation by having another party accepts the risk, either partial or total, typically by contract or by hedging / insurance.

c) Risk reduction: Employing methods/solutions that reduce the severity of the loss.

d) Risk retention: Accepting the loss when it occurs. Risk retention is a viable strategy for small risks where the cost of incurring against the risk would be greater than the total losses sustained. All risks that are not avoided or transferred are retained by default.

e) Risk Awareness: Raising awareness about managing risks across the organization.

4.4 Monitoring and Reporting

Risk monitoring, reviewing, mitigating and reporting are critical components of risk management process. Once risks are identified, they shall be prioritized on the basis of impact, dependability on other functions, effectiveness of existing controls, probability of re-occurrence, etc. Internal auditors should review the risk register once a year and add any new material risk identified to the existing list. These will be taken up with respective functional/departmental heads for its mitigation. The existing process of risk assessment of identified risks and its mitigation plan will be appraised by the Board on an annual basis.

5. Risk Management Committee of the Board (RMCB):

The board shall constitute an RMCB and the RMCB shall have a minimum of 02 directors as members.

6. Crisis Management:

Crisis Management Policy is important to define the criteria for what the Company is required to do when any crisis situation arises within the organization / department or at its factory / Manufacturing Unit. It also Identifies who will take action and what their roles will be so that Company can minimize harm and restore operations as soon as possible.

Crisis Management Includes anticipating threats, developing strategies to minimize harm, and implementing these strategies when a crisis occurs.

7. Responsibilities of Crisis Management Team (CMT):

The Crisis Management team must ensure below:

1. Establish site emergency plans at all sites to manage events whose impacts while serious do not require the resources needed by a crisis;
2. Establish and maintain a Crisis Management manual, including an escalation protocol, and appropriate Business Continuity / Disaster Recovery plans to maintain production and customer service levels;
3. Ensure compliance with applicable legal and regulatory requirements and conform to the requirements of ANJ Crisis Management Technical Standard;
4. Establish and maintain a Crisis Management organization with defined roles and responsibilities for managing a Crisis;
5. Establish a crisis management governance programme to oversee the development and maintenance of a crisis management plan that also fosters and reinforces organizational resilience
6. Identify generic outcomes and quantify the impact of incidents whose severity is sufficient that they would be designated as a Crisis;
7. Identify response options to be invoked in the event that an incident is declared as a Crisis;
8. Plan for and provide access to physical and technical resources likely to be required during the management of a Crisis;
9. Ensure a communication protocol is established and functional to disseminate timely and accurate information among internal and external stakeholders during a Crisis;
10. Establish a programme of training, desk-top tests and full-scale drills designed to simulate high risk incidents and crisis scenarios; and
11. Pursue excellence through continuous improvement based on learnings from Crisis scenarios and drill programme