FRAUD RISK MANAGEMENT POLICY

Introduction

Monarch Surveyors and Engineering Consultants Limited ("Monarch" or "the Company") is unwavering in its commitment to integrity, ethical behaviour and accountability. **Fraudulent conduct erodes stakeholder trust, imperils statutory compliance and exposes the organisation to financial as well as reputational harm.** Operating **in tandem with the Code of Conduct, Insider-Trading Policy and Whistle-blower Policy**, this Fraud Risk Management Policy ("the Policy") articulates Monarch's strategy for preventing, detecting, investigating and remediating fraud in alignment with Section 177 of the Companies Act 2013, Regulation 22 of the SEBI (Listing Obligations and Disclosure Requirements) Regulations 2015, the Institute of Chartered Accountants of India Guidance Note on Fraud and the internationally recognised COSO Fraud Risk Management framework.

Definitions

"Fraud" means any intentional act or omission designed to deceive or mislead, resulting in loss, misappropriation of assets, misstatement of financial statements or the securing of an improper personal benefit. **It includes financial and non-financial misconduct such as manipulation of non-financial KPIs, ESG data, cyber fraud, phishing, unauthorised system access and other digitally enabled schemes.** A "suspected fraud" is a circumstance that gives rise to a reasonable belief that wrongdoing may have occurred or may be in progress. "Whistle-blower" denotes any employee, director, contractor, supplier, customer or external stakeholder who, acting in good faith, reports a potential breach through Monarch's vigil mechanism.

Objectives

The Policy aims to embed zero tolerance for fraud; promote a **speak-up culture** that encourages timely reporting; delineate governance roles; integrate fraud-risk assessment with ERM and internal-audit planning; ensure systematic risk identification, evaluation and mitigation; provide secure and anonymous disclosure channels; guarantee independent investigation; mandate proportionate disciplinary, civil and criminal action; preserve evidence; and maintain compliance with statutory and regulatory requirements.

Scope

This Policy applies to all directors, permanent and temporary employees, trainees and consultants; to joint-venture partners, agents, suppliers, subcontractors, advisers and any other third party acting on the Company's behalf; and to each subsidiary, associate, overseas branch, site office or project consortium under Monarch's operational control.

Guiding Principles

Monarch favours proactive prevention because robust controls are less costly than remediation; early detection through data analytics and vigilant reporting is crucial; investigations must be fair, confidential and retaliation-free; corrective justice requires penalising wrongdoing and strengthening controls; and lessons learned feed continuous improvement.

Governance Framework

The Board of Directors is ultimately accountable for fraud-risk management, sets the tone at the top and receives **an anonymised summary of whistle-blower activity and consolidated fraud dashboard** every quarter. The Audit Committee monitors implementation of the Policy, pre-authorises investigations, reviews incidents whose financial impact exceeds **Rs 100,000.00** or whose risk-score surpasses **3** and may request periodic **deep-dive analyses of fraud trends or thematic risks**. Where conflict of interest arises, the Committee may directly appoint an external forensic auditor. The Chief Executive Officer champions an anti-fraud culture and endorses disciplinary measures. The Head of Internal Audit & Risk maintains the Fraud-Risk Register, leads or commissions investigations and tracks remediation. Functional heads own frontline controls, while all employees and third parties must comply with the Policy and report red flags.

Fraud-Risk Management Process

Risk identification draws on workshops, scenario planning, external intelligence and loss-event analysis. Each risk is scored for impact and likelihood; residual high risks require mitigation plans. Preventive controls include segregation of duties, authority matrices, vendor and supplier UBO checks, access controls and staff rotation; high-risk vendors or partners are subject to **enhanced due-diligence and periodic re-validation**. Detective controls include ERP exceptions, reconciliations and surprise audits. Key risk indicators are reported to the Audit Committee at the same cadence as the assessment.

Whistle-blower and Incident-Intake Mechanism

Suspected fraud can be reported via toll-free phone, dedicated e-mail, secure portal or physical drop-box. Identities are protected; each disclosure receives a docket number; retaliation is prohibited. The custodian acknowledges receipt within seven days, screens within five, and provides anonymised periodic summaries of all complaints including those screened out to the Audit Committee for trend analysis.

Investigation Protocol

Investigations are conducted by Internal Audit & Risk or an external forensic advisor authorised by the Audit Committee Chair. Evidence is preserved; interviews and digital forensics performed. Interim findings indicating regulatory breach or urgent risk are escalated to the Audit Committee Chair within one business day. A draft report including **root-cause analysis and control recommendations to prevent recurrence** is delivered to the Audit Committee within **15** days. Findings relevant to financial reporting are shared with statutoryy auditors.

Corrective and Disciplinary Actions

Where fraud is substantiated, Management **in consultation with Human Resources to ensure procedural fairness** imposes disciplinary action proportionate to severity, intent and impact, ranging from warnings to termination, recovery of losses, vendor blacklisting (minimum three years), law-enforcement complaints and regulator notifications. Repeat offenders or systemic failures may trigger broader control reviews. All decisions appear in the action-taken report tracked by the Audit Committee.

Regulatory and Statutory Reporting

Section 143 (12) of the Companies Act requires the Statutory Auditor to report fraud ≥ ₹ 1 crore to the Central Government. The Company Secretary files stock-exchange disclosures under Regulation 30 for material frauds, adhering strictly to statutory timelines.

Training and Awareness

An anti-fraud module forms part of induction. Existing employees complete annual e-learning, and high-risk teams attend tailored workshops that include case-study discussions and fraud scenarios to reinforce practical understanding. Completion statistics are reviewed by Human Resources and the Audit Committee.

Record Retention

Investigation case files, evidence logs, and correspondence are retained for eight years or longer if litigation is ongoing then disposed of under the Archival Policy.

Policy Review

This Policy is reviewed **annually** by the Audit Committee or sooner if regulatory developments or significant fraud trends warrant and updated upon Board approval.

Effective Date

This Policy comes into force on **April 1, 2025** and supersedes all earlier versions of Monarch's fraud-risk management guidelines.