KOWLASSUR CONSTRUCTION SERVICES CC
t/a DECOMA SERVICES

IT RISK POLICY

TABLE OF CONTENTS

1. INTRODUCTION

1.1. This Policy has been adopted by the Managing Member to underscore the importance of ethics and to assist the Organization and its employees to deal with situations that require careful consideration and/or action to ensure and maintain ethical compliance in exercising their responsibilities. The Managing Member will review this Policy at least annually and, if appropriate, revise this Policy from time to time.

2. DEFINITIONS AND INTERPRETATION

2.1. Unless otherwise expressly stated, or the context otherwise requires, the words and expressions listed below shall, when used in this Policy, bear the meanings ascribed to them below and cognate expressions bear corresponding meanings:

2.1.1. “Managing Member” means a person who is involved in the daily management of a company. The managing member has an interest in the business as an owner. This person is also in an authoritative position that allows him or her to represent the company in contract negotiations and agree to the terms of a binding contract;

2.1.2. “IT Officer” means the IT Officer and its designated assignee(s);

2.1.3. “IT Systems” means the computers, terminals, printers, networks, modem banks, online and offline storage media and related equipment, software, and data files that are owned, managed, or maintained by the Organisation. For example, IT Systems include the Organisation and departmental information systems, laptops, desktop computers, the Organisation’s network, and internet services;

2.1.4. “Organisation” means Kowlassur Construction Services CC T/A Decoma Services;

2.1.5. “Risk Officer” means the individual appointed by the Managing Member in order to perform the specific roles and responsibilities contained in terms of item 5 hereof. The Managing Member shall undertake this role until such time as a Risk Officer is appointed;

2.1.6. “Staff” means any person employed by the Organisation;

2.1.7. “User” means any person, whether authorized or not, who makes any use of any IT System from any location. For example, Users include a person who accesses IT Systems on the Organisation’s premises, or via an electronic network;

2.1.8. “this Policy” means this IT Risk Policy.

2.2. In this Policy:

2.2.1. table of contents and paragraph headings are for purposes of reference only and shall not be used in interpretation;

2.2.2. unless the context clearly indicates a contrary intention, any word connoting any gender includes the other genders, and the singular includes the plural and vice versa;

2.2.3. When a number of days are prescribed such number shall exclude the first and include the last day unless the last day is not a business day, in which case the last day shall be the next succeeding business day.

3. IT RISK APPROACH

3.1. In approaching risk and developing risk strategy, the Managing Member shall ensure that the risk strategy (KING IV: 11 : 1a – 2):

3.1.1. identifies opportunities and associated risks;

3.1.2. includes the potential and negative effects of the risks on the achievement of organisational objectives;

3.1.3. treats risk as integral to the way it makes decisions and executes its duties.

3.2. The Managing Member shall oversee risk management results in (KING IV : 11 : 6a – 6f):

3.2.1. an assessment of risks and opportunities emanating from the triple context in which the organisation operates and the capitals that the organisation uses and affects;

3.2.2. an assessment of the potential upside or opportunity presented by risks with potentially negative effects on achieving organisational objectives;

3.2.3. an assessment of the organisation's dependence on resources and relationships as represented by the various forms of capital;

3.2.4. the design and implementation of appropriate risk response;

3.2.5. the establishment and implementation of business continuity arrangements that allow the organisation to operate under conditions of volatility and to withstand and recover from acute shocks;

3.2.6. the integration and embedding of risk management in the business activities and culture of the organisation.

3.3. The Managing Member shall evaluate and agree the nature and extent of the risks that the Organisation should be willing to take in pursuit of its strategic objectives and approve in particular the (KING IV : 11 : 4a – 4b):

3.3.1. organisation's risk appetite, namely its propensity to take appropriate levels of risk;

3.3.2. limit of the potential loss that the organisation has the capacity to tolerate.

3.4. The Managing Member shall consider the need to receive periodic independent assurance on the effectiveness of risk management. (KING IV : 11 : 7)

4. COMBINED ASSURANCE MODEL

4.1. In order to put together a combined assurance model risks need to be identified and then layers of protection identified.

4.2. The layers of protection include:

4.2.1. Management responsible for risk (i.e. Managing Member);

4.2.2. Management not responsible for risk (i.e. Management);

4.2.3. External assurance (i.e. Internal audit, external auditors, Health and Safety inspectors, sustainability and environmental auditors, legal, internal forensic fraud examiners and auditors, statutory actuaries, external actuaries, regulatory inspectors).

4.3. The Managing Member shall take legal requirements into account to consider whether:

4.3.1. to assurance should be applied to the underlying data used to prepare a report (KING IV 15:45a);

4.3.2. the nature, scope and extent of assurance are suited to the intended audience and purpose of a report;

4.3.3. the specification of applicable criteria to the measurement or evaluation of the underlying subject matter or report is suited.

4.4. Management shall satisfy itself that the combined assurance model is effective and sufficiently robust for the Organization to be able to place reliance on the combined assurance underlying the statements that the Managing Member makes concerning the integrity of the Organisation's external reports. (KING IV : 15 : 46)

4.5. The Managing Member shall ensure that external reports disclose information about the type of assurance process applied to each report, in addition to the independent, external audit opinions provided in terms of legal requirements and ensure that the information includes a brief description of the nature, scope and extent of the assurance functions, services and processes underlying the preparation and presentation of the report. (KING IV : 15 : 47a)

4.6. The organization shall ensure that external reports disclose information about the type of assurance process applied to each report, in addition to the independent, external audit opinions provided in terms of legal requirements and that the information includes a statement by the Managing Member on the integrity of the report and the basis for this statement, with reference to the assurance applied. (KING IV : 15 : 47b)

5. INSURANCE

5.1. The Managing Member shall be responsible for the management of the Organisation's insurance Policy, covering cybercrime and IT related risks and shall ensure that suitable and adequate contributions or premiums are made monthly.

5.2. The Managing Member shall deliberate upon the adequacy or otherwise of the insurance policy.

5.3. The insurance policy shall be protected against excessive losses arising from heavy or numerous claims by suitable reinsurance cover. The Managing Member shall be responsible for reviewing and renegotiating cover through the insurance brokers agents for that purpose.

5.4. The Risk Officer shall be responsible for ensuring that the insurance cover in respect of those assets under their control is sufficient, having regard to the current value and replacement costs of those assets, and shall notify the Managing Member without delay of any new insurable risk or any alteration in an existing insurable risk which has arisen in connection with the Organisation.

5.5. The Risk Officer shall within 30 (thirty) days of a claim arising, notify the Managing Member of any potential third-party claim, or of fire damage to or loss of the Organisation's property or of any injury to employees of the Organisation where such matter is or even might be covered by insurance. In the case of third-party claims this is of utmost importance as any delay or failure to report an occurrence can prejudice the Organisation's rights. Any claims not reported within 90 (ninety) days of the occurrence will be rejected by the Board.

5.6. Insurance claims shall only be processed by the Risk Officer where confirmation of the insured damage and a request for reimbursement or reinstatement have been authorised and received by the Managing Member.

5.7. The Managing Member shall be responsible for the payment of all insurance premiums. Provided that all or any systems, procedures and mechanisms put in place by the Organisation shall be approved by the Managing Member.

6. IT RISK ASSESSMENT

6.1. The degree of impairment can extend from a minor disruption to total destruction of the IT system. Loss of hardware, software, data files, critical personnel or any combination can have impact upon the ability of the Organisation to maintain most management and operational functions.

6.2. For purposes of planning and reporting, disasters are defined as:

6.2.1. Minor

6.2.1.1. The lowest of impact/outage that allows for recovery within twenty-four (24) hours with existing resources and does not result in significant deviation from normal production.

6.2.2. Major

6.2.2.1. Interrupts IT operations and impacts other operations, and recovery requires additional resources but can be accomplished on site.

6.2.3. Catastrophic

6.2.3.1. Interrupts IT operations and impacts other operations, and recovery requires additional resources, operations must be moved to and or provided by a secondary site or agency while recovery occurs.

6.3. Probable Disaster

Disaster	**Degree**	**Probability**
Description	*Minor, Moderate, Major*	*Low, Moderate, High*
Electrical	Minor	High
Hardware Failure	Major	Moderate
Software Failure	Major	Moderate
Malware / Virus	Minor to Moderate	Low
Hacking	Major to Catastrophic	Moderate
Dishonest staff (fidelity)	Major	High
Fire	Major	Low
Water	Major	Low
Vandalism	Minor to Major	Low

7. IT DISASTER RECOVERY

7.1. Disaster Recovery Team

7.1.1. The disaster recovery team consists of:

7.1.1.1. primary critical team members:

(a) Management Representatives

(b) Nominated IT Specialist

7.1.1.2. key business continuity individuals identified in the Organisation's Disaster Recovery Plan.

(a) Management Representatives

7.1.2. The disaster recovery team will be led by the primary critical team members and liaise with the Managing Member.

7.1.3. The disaster recovery team is responsible for:

7.1.3.1. identifying the extent of damage to all IT Infrastructure, including faxes, copiers and other facilities;

7.1.3.2. determining the condition of the equipment;

7.1.3.3. supplying a salvage report to the Managing Member;

7.1.3.4. assessing of operational capability;

7.1.3.5. defining of restoration requirements;
7.1.3.6. scheduling and supervising salvage and restoration;
7.1.3.7. scheduling and supervising Staff as required within each primary area of responsibility;
7.1.3.8. establishing emergency production procedures;
7.1.3.9. recreating as quickly and closely as possible, original site operations including backup, security, data entry, information distribution and user assistance functions;
7.1.3.10. advising Users of the disaster and recovery and operations procedures;
7.1.3.11. assisting Users in recovery operations;
7.1.3.12. assisting IT vendors and analysts in program recovery;
7.1.3.13. supervising and co-ordinating the entire recovery process and allocating resources;
7.1.3.14. certifying non-recoverable items;
7.1.3.15. procuring replacement items and supplies;
7.1.3.16. identifying repair requirements and arranging for repairs;
7.1.3.17. acting as vendor liaison;
7.1.3.18. adjusting the recovery plan as needed; and
7.1.3.19. making disaster recovery management decisions.