Information Security Management System Policy

1.0 Purpose

The purpose of Information Security Management is to protect Kings Solutions Group Limited ('Kings') from loss of information or any other asset(s) hard or soft resulting from internal or external activities.

This includes all assets critical to the secure operation of the business' external assets i.e. belonging to customers, suppliers and business partners associated with Kings.

The implementation of this policy demonstrates the commitment of the organisation to maintain and improve security initiatives and provides confidence to business partners in the conduct of their business with Kings Solutions Group Limited. It is the policy of Kings:

- **To preserve Confidentiality - t**hat is to protect assets and information from unauthorised disclosure
- **To maintain Integrity** – that is to protect information from unauthorised or accidental modification ensuring accuracy and completeness of the organisations assets
- **To ensure Availability** – that is to ensure that information and assets are available as and when required adhering to the organisations business objectives

2.0 Scope

All Assets including information belonging to Kings and/or the client and in possession or custody of the Company's employees, representatives, partners and service providers and their personnel are within the scope of this policy, in all locations.

3.0 Goals

To identify through appropriate risk assessment, the degree of protection of all assets, the preparedness against threats, to understand their vulnerabilities and the threats that may expose them to risk.

To manage and minimise risks, to an acceptable level through the design, implementation and maintenance of a formal Security Management System (SMS).

To comply with legislation including:

- All legislative requirements
- To comply with contractual obligations that lay down the requirements for Asset and Information Security
- Commitment to comply with the requirements of ISO 27001
- Commitment to continual improvement adherence with the controls and where possible implement industry best practice
- Commitment to review this policy on an annual basis or more frequently as required.

Information Security Management System Policy

4.0 Responsibilities

Kings Management Team are responsible for the day to day operation of the SMS.

All staff have a duty to inform management of any incidents and shall do so via the Incident Management Procedure or the Whistleblowing Policy. This is outlined in individual job descriptions.

The Compliance Officer is responsible for ensuring the SMS conforms to the requirements of ISO 27001 and for reporting on performance and any issues to senior management, either through Management Review or Board reports.

5.0 Leadership

The Chief Executive Officer assumes ultimate responsibility for the SMS demonstrating the commitment and leadership from top management.

The CEO shall ensure adequate resources are available to all managers to maintain the SMS.

6.0 Disciplinary Action

Any deliberate attempt to jeopardize any information, asset(s) or associated infrastructure will be subject to disciplinary action, including but not limited to immediate termination.

Bob Forsyth
Chief Executive Officer