



"Your Identity Secured, your payments made Safe"

ISIGNTHIS LTD

Corporate Governance Policies

Risk Management and Internal Compliance and Control

1. Risk Management and Internal Compliance and Control

Management determines the Company's risk profile and is responsible for overseeing and approving risk management strategy and policies, internal compliance and internal control. The Company's process of risk management and internal compliance and control includes:

- (a) establishing the Company's goals and objectives, and implementing and monitoring strategies and policies to achieve these goals and objectives;
- (b) continuously identifying and reacting to risks that might impact upon the achievement of the Company's goals and objectives, and monitoring the environment for emerging factors and trends that affect these risks;
- (c) formulating risk management strategies to manage identified risks and designing and implementing appropriate risk management policies and internal controls; and
- (d) monitoring the performance of, and continuously improving the effectiveness of, risk management systems and internal compliance and controls, including an ongoing assessment of the effectiveness of risk management and internal compliance and control.

Within the identified risk profile of the Company, comprehensive practices are in place that are directed towards achieving the following objectives:

- (a) effectiveness and efficiency in the use of the Company's resources;
- (b) compliance with applicable laws and regulations; and
- (c) preparation of reliable published financial information.

The Board oversees an ongoing assessment of the effectiveness of risk management and internal compliance and control.

The responsibility for undertaking and assessing risk management and internal control effectiveness is delegated to management. Management is required by the Board to report back (at least annually) on the efficiency and effectiveness of risk management, inter alia, by benchmarking the Company's performance against industry standards.

The risk profile of the Company contains both financial and non-financial factors including but not limited to political, social, economic and environmental risks. Consideration will be given to whether the Company has a material exposure to any of these risks.

To mitigate/manage these risks, the Company has in place a broad range of risk management policies and procedures including competent management in all disciplines, an experienced Board, regular Board meetings, six monthly financial audits, rigorous appraisal of new investments and advisers familiar with the Company.

Due to the nature of the Company's operations and services provided additional steps are required in regards to risk management and compliance control.

The Company has undertaken a full compliance audit in regards to the Payment Card Industry (PCI) standards of maintaining, storing and handling financial transactions and data. The Tier 1 certification allows iSignthis to offer full payment processing services.

The certification covers technical, security and operational procedures of the Company.

Additional to the PCI certification the Company will maintain certification to to ISO 27001.

ISO 27001 Information Security and data protection brings supreme importance to data for organisations globally and is mandatory for businesses who are safeguarding both their client and company data against potential threats. By integrating a robust information security management system the Company can ensure that the quality, safety, service and product reliability has been safeguarded to the highest level.

ISO 27001 is the international standard which is recognised globally for managing risks to the security of information you hold. Certification to ISO 27001 allows the Company to prove to y clients and other stakeholders that we are managing the security of information in our possession. ISO 27001:2013 (the current version of ISO 27001) provides a set of standardised requirements for an information security management system (ISMS). The standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving ISMS.

The ISO 27001 Information Security Management system (ISMS) standard provides a framework for Information Security Management best practice that helps organisations:

- protect clients and employee information
- manage risks to information security effectively
- achieve compliance
- protects the company's brand image

The Chief Executive Officer and the Chief Financial Officer are required in conjunction with the preparation of the annual report, the half yearly report, and any quarterly financial reports required to be lodged in accordance with the ASX Listing Rules, to state to the Board in writing that, in their opinion, the financial records of the Company have been properly maintained and that the financial statements comply with the appropriate accounting standards and give a true and fair view of the financial position and performance of the Company, and that the opinion has been formed on the basis of a sound system of risk management and internal control that is operating effectively.

Management is responsible for the ongoing management of risk with standing instructions to appraise the Board of changing circumstances within the Company and within the national and international business environment.

This policy is reviewed annually.