ISMS Policy

Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

FIS, entrusted by clients with their information and records management, identifies the importance and implements appropriate measures. Information security is achieved by implementing a suitable set of controls (based on risk profile), including policies, processes, procedures, organisational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that specific security objectives are met.

This policy applies to all information that is physically or electronically generated, received, stored, printed, filmed, or keyed; and to the IT applications and systems that create, use, manage and store information and data. The policy covers the following areas:

- Information Security Risk Management
- HR Security and Access Control
- Communications and Operations Management
- Physical and Environmental Security
- System Acquisition, Development and Maintenance
- Vendor Management
- Information Security Incident Management
- Information Security aspects of Business Continuity Management
- Compliance Management

FIS is committed to continuous improvement of information security management system. The policy is directly aligned with the Information Security Industry standard AS/NZS ISO/IEC 27001:2013

Approved by: Matthew Cocker [CIO]

Date: 31-10-2019