Information Security Policy Statement

Iqarus Holdings Pte Limited and its subsidiary operations is a global provider of intelligent and integrated healthcare solutions to its customers in complex and demanding operating environments in order to keep their workforce safe, healthy and productive.

Iqarus acquires information, uses it, shares it and protects it and behind these activities is the critical requirement for effective data security to ensure its confidentiality, integrity and availability.

Effective security of this information is achieved through appropriate conduct, and through compliance with applicable legislation and Iqarus policies and procedures.

Iqarus is committed to the following objectives and expectations:

- Information assets and information processing facilities are protected against unauthorised access.
- Resources are provided to support the implementation and maintenance of the Information Security Management System ('ISMS'), as per ISO 27001:2013 requirements.
- ISMS is integrated into the Quality Management System.
- Statutory and legal obligations (expressed or implied) concerning information security are met.
- Security of information transferred within the organisation and with any external entity is protected.
- The availability of information assets and information processing facilities is assured.
- Confidentiality of information and classification of data is given a high priority.
- Information Security policies are communicated to all staff, who shall receive awareness training.
- Business continuity plans including security of data are prepared, maintained, and exercised.
- Information is protected from unauthorised disclosure.
- Unauthorised use of information assets and processing facilities is prohibited.
- Cryptography is used to protect the confidentiality, authenticity and/or integrity of information.
- Information and information processing facilities are protected against malware.
- Information is protected against loss of data by implementing a back-up policy across all projects.
- Loss, damage, theft or compromise of assets and interruption to Iqarus operations are prevented.
- Information classification is monitored to ensure that information receives an appropriate level of protection in accordance with its importance to Iqarus.
- Operational Software is controlled to ensure the integrity of operational systems.
- Actual or suspected breaches of information security are reported and investigated.
- Commitment to continual improvement of the management system through objectives, awareness, auditing and training.
- Controls are commensurate with risks faced by Iqarus.
- Correct and secure operations of information processing facilities are ensured.
- Information Security policies are reviewed annually or following material changes to Iqarus.

This Information Security Policy will be communicated to all staff and to organisations working for or on behalf of Iqarus, all of which are expected to cooperate and assist in the implementation of this policy, whilst ensuring that their own work, so far as reasonably practicable, is carried out fulfilling the information security requirements.

***