Information Security Policy Statement

Ganymede Solutions Limited (GSL) are part of the RTC Group Ltd.

As part of our commitment to protecting our candidates, employees, clients, suppliers and 3rd parties data, we have implemented a stringent Information Security Management system to protect both the security and integrity of the data we process.

As part of our commitment to managing individual's rights, we have appointed a Compliance Manager, responsible for all Data Protection activities, to work alongside the RTC Group Data Protection Representative.

GSL is committed towards securing the Confidentiality, Integrity and Availability of information for the day-to-day Business and Technical operations. The security of information and other assets is therefore regarded as fundamental for the successful business operation of GSL.

GSL has adopted an Information Security Management System (ISMS) comprising of the Information Security Policies, Procedures and Processes to effectively protect data/information of GSL and its customers from information security threats, whether internal or external, deliberate or accidental. ISMS in GSL is aligned to the requirements of ISO 27001: 2013 and ISO 9001:2015.

The management of GSL is committed to ensure that:

- Regulatory and legislative requirements related to GSL are met
- The confidentiality of information is protected and prevents disclosure of valuable or sensitive information
- The integrity of information is maintained to ensure its accuracy and completeness
- The availability of information is maintained to meet business needs, candidate and client's requirements
- Business continuity plans are developed, maintained and tested
- Information security awareness is provided to all GSL employees
- Incident management process is established and implemented to ensure that all breaches of information security, actual or suspected are reported and investigated
- Risks are mitigated to an acceptable level through a risk management framework
- The information security management system is continually improved
- Appropriate resources are allocated in order to implement, operate and review an effective Information Security Management System
- All stakeholders are responsible for implementation of respective security policies and procedures within their area of operation, and oversee adherence by their team members
- GSL management acknowledges the need of continual improvement and has introduced various methods to ensure that effectiveness and continual improvement of the processes are achieved.
- GSL shall follow a formal disciplinary process for employees who have allegedly violated the information security policies and procedures.
- GSL shall ensure that the review of the Information Security Policy and related documents is performed at least on an annual basis or when significant changes occur to ensure suitability, adequacy, and effectiveness of the ISMS framework.

Date of Issue 17/01/2020
Approved by: Paul Crompton,
Managing Director