QUALITY MANAGEMENT SYSTEM

SECURITY POLICY

To support the achievement of the vision and mission it is React Engineering Limited's policy to ensure that all information that is received, produced or processed by the Company is handled safely and is securely protected. Information includes, but is not limited to, electronic data, hardcopy data and communications.

The security of information is of critical importance to the Company's business and significant problems can arise if the confidentiality, integrity and availability of information is not maintained e.g. loss of business and profitability, loss of customer confidence, poor company image, failure to meet legal and/or contractual requirements etc.

React adopts the following risk appetite: risk cautious for risks to Confidentiality, and risk open for risks to Integrity and Availability.

The Directors and the Executive Team are committed to ensuring that this Security Policy is implemented and will provide strong direction to the achievement of the objectives and intent of this Policy and the Security Procedure.

All staff are expected to comply with the requirements and the intent of this Security Policy and the accompanying Security Procedures. Employees are also expected to inform the Directors and Executive Team of any shortfalls in, or improvements to, this Policy and accompanying Procedure.

In order to achieve the above objectives, React Engineering Limited will:

- Establish and maintain the Security Policy and Procedure and review and revise as necessary.
- Establish and maintain a Security Management System and an Information Assurance Governance
- Framework to suitably manage the risks associated with creating, processing and storing Government Security Classified Information (GSC), Sensitive Nuclear Information (SNI) and Personal Information.

- Protect the Confidentiality, Integrity and Availability of all information held by the Company, in compliance with Government legislation, the mandatory requirements set out in the Government Security Policy Framework, Security Assessment Principles (SyAPs) and Information Assurance Standards.
- Protect the Confidentiality, Integrity and Availability of React's Information Technology (IT) equipment and systems.
- Provide resources to establish, implement, operate, monitor, audit, review, maintain and improve the Security Management System, and establish roles and responsibilities for security.
- Provide training in the provisions of the Security Management System to all members of the Company, with special induction training to new starters and ensure all members of the Company are kept informed of any changes.
- Ensure good security is an objective for all personnel in the Company and that all personnel are aware of their responsibilities under the law.
- Ensure all staff and persons given access to information have appropriate security (vetting) clearance for the level of information they have access to.

For and on behalf of React Engineering Limited,

Phil Redfern
Managing Director

Paul Botterill
Senior Information Risk Owner (SIRO)