INFORMATION SECURITY POLICY

Information is the principal commodity used and produced in the course of the Nuclear Technologies division's business operations. Nuclear Technologies' is committed to protecting the confidentiality, integrity and availability of the Company's information, and that of its clients, in order to minimize the legal and commercial impacts of security incidents, whether internal, external, deliberate or accidental, and to support business continuity. The "need to know" principle is endorsed and required to be practiced by all Nuclear Technologies' employees.

Information takes many forms and may be stored as hard copy, on computers or personally, and transferred physically, electronically or by the spoken word. Nuclear Technologies requires its employees and sub-contractors to follow its Company procedures and client's rules controlling the generation, transfer, use and storage of all forms of information in the course of its business.

Nuclear Technologies' procedures are designed to be consistent with the Cabinet Office's Security Policy Framework, our clients' and Contracting Authorities' requirements and the principles of commercial confidentiality. They also support the mitigation requirements of the Company's Security Risk Assessment. Their implementation is monitored by internal and external audits and they are reviewed regularly as part of the Company Management System Review process. The outputs from these processes are used to identify opportunities for improvements to the Management System.

Information security is controlled in Nuclear Technologies by conformance to the relevant TUV SUD (UK) Group Policies and to the relevant divisional policies and Company Procedures (CPs), or other Company documents. The requirements are that:

- The Divisional Director for Nuclear Technologies is nominated to be responsible for security matters. The Divisional Director acts as the divisional Senior Information Risk Owner for the Nuclear Technologies and will ensure that:
    - Roles and responsibilities for security are clearly defined;
    - Security risks are assessed and appropriate control measures are established and maintained;
    - Coherent security procedures are in place and communicated to all employees;
    - Security training is provided as required to personnel in accordance with their security role;
    - There is a sufficient level of security awareness, and
    - A good culture of security is promoted and that all employees understand their responsibilities.
- A Security Controller is appointed to carry out the routine management of security activities.
- Business Managers and Project Managers act as Information Asset Owners for their own areas of activity or projects.
- Access to a Vetting Officer is available.

Individual employees are vetted prior to employment, briefed on appointment, sponsored for appropriate national security vetting and their security status is reviewed regularly thereafter in accordance CP5.0 –Security – Personal, Information & Materials They are made aware of their security responsibilities in accordance with CP5.0.

- Return of Company assets is controlled by SSC-HR-02 Leaver Clearance Certificate
- Monitoring and reporting of performance is controlled in accordance with CP1.05 – Audits.
- Review the security threats, risk and control measures annually.
- The security, integrity and availability of electronic data is controlled in accordance with applicable Accreditation Document Sets, including CP5.02, and procedures operated by TUV SUD Services (UK) Ltd, to whom Nuclear Technologies sub-contracts the management of its IT system.
- Receipt, handling, storage and transmission of protectively marked information, access controls and physical security in Nuclear Technologies' offices are controlled in accordance with CP5.0 – Security – Personal, Information & Materials.
- Provisions to safeguard the confidentiality of Nuclear Technologies' business data and intellectual property, and that of its clients, are contained in Nuclear Technologies' contract Terms and Conditions.
- Information Security control measures that contribute to Nuclear Technologies' business continuity process are described in the Company Risk Register and Security Risk Register.

Nuclear Technologies' employees are responsible for the Security of information under their control, and under the control of their sub-contractors, and therefore report any breaches, whether suspected or actual, in accordance with CP4.02 – Accident, Incident, Ill Health, Near Miss and Absence due to Illness Reporting. This procedure makes provision for investigation and analysis of incidents to facilitate learning of lessons and prevention of re-occurrence.

This policy relates to the Nuclear Technologies division and is an extension of the overarching TUV SUD (UK) Group Security Policy Statement.

Karen Hildred
Technical Director
Issue 7– May 2021