



Information Security and Digital Risk Policy

Purpose

This policy establishes the commitment and approach by which Integrated Engineering & Technology LLC (IET) manages information security and digital risk, to provide assurance to our clients and build competitive advantage.

Commitment

IET is committed to:

- establishing, implementing and continual improving an effective Information Security Management System (ISMS) that protects the confidentiality, integrity and availability of all critical information ensuring a secure environment for our clients and business operations.
- strict compliance with legal, regulatory and contractual requirements to protect data through adherence to relevant laws and industry standards.
- identifying assessing and managing information security risks by implementing appropriate controls and treatment strategies to protect both business and client data.
- allocate the necessary resources, define clear roles and responsibilities and foster a culture of awareness and training to maintain a strong information security framework within the company.

Responsibility

The General Manager is responsible for the effective implementation and maintenance of information security management.

The Head of ICT is responsible for monitoring information security, and digital risk across the business and ensuring security measures are applied proportionately in line with IET's risk appetite.

Process owners are responsible for monitoring and reviewing the implementation of information security measures in their respective operations.

Project principals are responsible for the application of information security requirements on projects. This includes the identification and treatment of information security, and digital risks, and considering security measures from the outset.

Approach

We operate an integrated management system conforms to ISO 27001.

We recognise and where possible exceed our client expectations and contractual obligations.

We recognise that our people are our best line of defence in identifying and mitigating digital or physical security risks. We therefore put great emphasis on training our people and leading by example to ensure appropriate security behaviours are understood and observed.

We ensure appropriate security is in place for the information we hold, including the security of our offices and the storage of archived information.

Analysis, review, feedback, and learning enable us to continuously improve the way we manage information risk, ensuring we meet the security needs of our business, our staff and our clients.

A blue ink handwritten signature, appearing to read 'Hamed Nasser Hamed Al Hinai', with a large, stylized flourish at the end.

Hamed Nasser Hamed Al Hinai

Director and Board Member

01-Nov-2024