Information security and digital risk management

Purpose

This policy establishes the commitment and approach by which Mott MacDonald manages information security and digital risk, to provide assurance to our clients and build competitive advantage.

Commitment

Managing information security and digital risk is a cornerstone of our relentless focus on excellence and digital innovation. By doing so we build confidence in our brand and earn the long term trust of our clients.

Information is a key asset for our clients and essential to our ability to deliver insightful and innovative projects. Ensuring its confidentiality, integrity and availability is vital to the delivery of our services and to the reputation of the Group.

Our treatment of information security risk is embedded into all our activities and is supported by our business integrity policy and Our Code.

Responsibility

An executive board director is responsible for the effective implementation and maintenance of information security management.

The Group head of capability is responsible for monitoring information security and digital risk across the business and ensuring security measures are applied proportionately in line with Group risk appetite.

General managers 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

Our business management system provides an integrated process to govern our internal operations and projects. The management system meets the requirements of ISO 27001 and Cyber Essentials Plus and is independently certified in appropriate geographical locations around the world.

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 on leading by example to ensure appropriate security behaviours are observed and understood.

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.

James Harris
Executive chair