Information Security Management Policy Statement

This policy defines how Information Security is set up, managed, measured, reported on and developed within sineQN and is aligned to BS ISO/IEC 27001:2013 The International Standard for Information Security to which sineQN is registered. This allows sineQN to adopt Information Security Best Practice which is validated by an external third party.

This policy has been reviewed and approved by the Managing Director and ensures:-

- sineQN commits to satisfy applicable requirements related to Information Security
- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Availability of information for business processes will be maintained
- Legislative and regulatory requirements will be met
- Business Continuity Plans will be developed, maintained and tested
- Information security training will be given to all sineQN employees and sub-consultants
- All actual or suspected information security breaches will be reported to the Information Security Manger and will be thoroughly investigated and satisfactorily avoided.
- Establish and maintain the risk criteria and retain documented information about the risk assessment process
- Strive to Continually improve the Information Management System

The Management Representative is responsible for maintaining and communicating this policy within the organisation

All managers are directly responsible for implementing the policy and ensuring staff compliance in their respective areas.

Compliance with the Information Security Management Policy is mandatory.

Signed:

Gavan Mackenzie –
Managing Director
May 2016