Information Security

policy statement

SCEE's information Security Policy provides guidelines in order to safeguard company information, reduce business and legal risk and protect company knowledge and reputation.

The policy applies to any data and information, whether it is

- stored in SCEE owned and managed systems
- transferred through SCEE owned and managed systems
- transmitted via any electronic medium including social media and online information portals

This policy applies to all part-time and full-time employees, contractors, consultants, interns, volunteers and visitors. This policy also applies to all software that is owned/developed by or licensed to the company as well as workstations, servers, or other devices which are used to create, access or modify company data.

Employees must ensure acceptable use of company equipment (or their own equipment for company purposes) during or after company hours. As these systems can access and store corporate information. Employees and contractors are responsible for ensuring that this equipment is used in an effective, ethical and lawful manner at all times.

The IT department will maintain security protections across all corporate systems and data and will endeavour to protect all systems and information against evolving cyber security threats.

There are no exceptions to this policy.

Graeme Dunn
Managing Director/CEO

Date: 28th June 2019

Doc ID: SCEE-BS-IT-POL-0004 Rev: 3.0