Information Security Statement

On a daily basis the media reports of yet another organisation which has been the victim of a cyber-attack and this is ever more prevalent during a worldwide pandemic. Usually it's the loss of corporate data, intellectual property or customer's personal and or financial data. The consequences have varied from regulatory fines and reputational loss, through to the corporate failure of a business and we know that cyber criminals can infiltrate an organisations system for days, or even years, without being detected. So businesses and government need to understand where the key cyber risks exist within the organisation, how to detect them and how to protect themselves from this rising ever present threat at the right level of cost to the organisation.

Solstice' senior management recognises the position of trust we hold with our clients and the responsibilities that this places upon us to protect the data and information at the heart of the services and solutions we deliver for them.

We view the implementation and maintenance of a robust Information Security Management System (ISMS) to be key to honouring these responsibilities; Protecting all business information assets within, or managed by, Solstice from threats internal or external be they malicious or accidental.

We have therefore developed a risk assessment-based ISMS founded on the international standard 27001:2013 to identify and control information security in line with our clients' trust in us, best practice and all legal, regulatory and contractual requirements.

Our ISMS is embedded within our working culture, day-to-day management and strategic direction, with all managers fully engaged during its implementation and all staff receiving awareness training on joining and regularly thereafter. Within this fully integrated approach, it is our policy to monitor performance of our ISMS through objectives and monitoring metrics, identifying opportunities for improvement and responding to emergent threats with resources regularly reviewed to ensure that staff time, technology and budgets are available to support this. As part of this commitment to continual improvement, our policy is to conduct a full management review at least annually or when need is identified to ensure compliance to the ISO 27001 standards and ongoing effectiveness of our ISMS.

David Cattermole / David Cole

Directors

21/09/2021