Information Security Policy

1. Our Information Security Management System (ISMS) ensures the confidentiality, integrity and availability of Information at Kallidus. It is realised through the policies, procedures and controls within the ISMS manual.

2. The management at Kallidus are committed to continued review and improvement in order to reduce the risk of security incidents and ensure continued contractual, and legal, compliance.

   New and existing requirements are informed through stakeholder feedback, industry associations, Information Security suppliers and the press sources of official bodies such as the ICO.

   An evaluation of the company's compliance is undertaken as part of the audit programme.

3. A risk assessment framework, defined by 6.1.2) *Risk Assessment Methodology*, in the ISMS manual, has been created for setting and reviewing objectives to achieve the company's overall aim of reducing business risk.

4. Kallidus operates a business risk approach to the controls that are implemented in the business. A risk methodology, approved by management, can be found in the ISMS manual 6.1.2) Risk Assessment Methodology and it defines the method of risk assessment.

   An acceptable level of risk has been agreed and management approve resources to treat risks that fall outside of this by agreeing controls within a risk treatment plan.

   The risk register is regularly reviewed by management and the risk 'owners', who acknowledge and accept the residual risk.

   To ensure that all staff, customers and third parties are aware of the company's Information Security Management System, and their particular responsibilities within it, this policy is displayed and communicated publicly with awareness training provided.

5. The management gives complete approval and commitment to this policy.

Signed: 

Dated : 20th January 2022

Chief Technology Officer: Arun Mundray
Kallidus