INFORMATION SECURITY POLICY

As a modern, forward-looking business, Sycous recognises at senior levels the need to ensure that its business operates smoothly and without interruption for the benefit of its customers, shareholders and other stakeholders.

To provide such a level of continuous operation, Sycous has implemented an Information Security Management System (ISMS) in line with ISO 27001.

The purpose of this policy is to protect all information assets within the company from all internal and external threats, whether deliberate or accidental. This policy aims to protect the confidentiality, integrity and availability of information in all forms, whether stored electronically, transmitted across networks, or printed on paper.

This policy applies to systems, people and processes that constitute the company's information systems, including board members, directors, employees, suppliers and other third parties who have access to Sycous systems.

The company is committed to:

- Satisfying all applicable requirements related to information security
- Continual improvement of the information security management system
- setting & achieving information security objectives through regular review of objectives at Management Review
- The implementation and maintenance of an Information Security Management System (ISMS) that is independently certified as compliant with ISO 27001
- The systematic identification of security threats and the application of a risk assessment procedure that will identify and implement appropriate control measures.
- Regular monitoring of security threats and the testing/auditing of the effectiveness of control measures.
- The maintenance of a risk treatment plan that is focussed on eliminating or reducing security threats.
- The clear definition of responsibilities and authorities for implementing the information security management system.
- The provision of appropriate information, instruction and training so that all employees are aware of their responsibilities and legal duties and can support the implementation of the ISMS.
- The implementation and maintenance of the sub-policies documented within the system

Any contravention of this policy or other information security related policies and procedures will be dealt with under the appropriate procedures. This may involve the disciplinary procedure being invoked. Since this policy refers to minor issues through to illegal activities, the sanctions for breaches may range from informal warning to dismissal.

Signed:

Matthew Hall, Managing Director

Date: 29th June 2023