Supplier Security Policy

The Directors at Verner Wheelock understand the information security needs and expectations of its interested parties both within the organisation and from external parties including, amongst others, clients, suppliers, regulatory and Governmental departments. The Company has recognised that the disciplines of confidentiality, integrity and availability of information in information security management are integral parts of its management function and view these as their primary responsibility and fundamental to best business practice.

To this end Verner Wheelock has produced this information security policy aligned to the requirements of ISO/IEC27001:2013 to ensure that the Company:

- Identifies and documents the type of organisation that has access to its information systems
- Manages the lifecycle of the supplier relationship
- Defines the type of information access that each supplier will be allowed
- Defines the minimum level of security requirement for each type of information asset and the type of access as a basis for supplier agreements
- Produce a procedure for monitoring adherence to established security requirements
- Produce accuracy controls to ensure the integrity of information provided by both parties
- Defines the type of obligation applicable to the supplier to protect the company's information
- Manages incidents and contingencies associated with supplier access including individual responsibilities
- Manages resilience, recovery and contingency arrangements to ensure the availability of the information or information processing concerned
- Provide awareness training to personnel and subcontractors involved in these arrangements
- Documents, where necessary, the information security requirement in an agreement between parties
- Manages the necessary transition of information, information processing facilities and anything else that needs to be moved, ensuring that information security is maintained throughout the transition period.

The Directors also understand that certain suppliers may have inadequate information security management and will, in such cases, identify and apply controls necessary to ensure security is maintained. It will use confidentiality agreements, non-disclosure agreements and second party audits where appropriate. The Company will also consider any Data Protection regulations and will be aware of all legal and contractual responsibilities in the area.

Responsibility for upholding this policy is truly company-wide under the authority of the Managing Director who encourages the personal commitment of all staff to address information security as part of their skills.

Signed by: A Wheelock
Date: 1st February 2021

Managing Director

RELATED DOCUMENTATION

Information Security Policy	Confidentiality and Non-Disclosure Agreement
Communications Policy	Privacy and GDPR Policy