Information Security Policy

1. Purpose

The purpose of this document is to demonstrate the commitment of Partners, Senior management, and employees to information security at Ingleton Wood, providing an ISMS framework to which all policies and procedures are adhered to.

2. Policy

The Partnership board and senior management of Ingleton Wood, operating in a multi-disciplinary practice of built environment experts working within all sectors including defence, education, and healthcare.

We are committed to preserving the confidentiality, integrity, and availability of all the physical and electronic information and information-related assets to meet the purpose and objectives of the as summarised in the Context of the organisation.

Information and information security requirements are aligned to our practices strategic direction and our objectives, considering internal and external issues that may affect the practice and the requirements of our interested parties.

Our ISMS objectives are defined and measured in accordance with the requirements of ISO27001:2013.

The ISMS framework defines policies and procedures for establishing and maintaining security controls. The framework clarifies processes used to protect the practice from information security and cybersecurity risks, enabling the practice to continually improve and deliver its overall purpose and objectives.

Ingleton Wood operates a risk-based approach to managing information security risks that the practice faces. The approach prioritises the risks based on their potential impact and likelihood and creates controls and policies to mitigate them. All risks are aligned to our Statement of Applicability (SofA).

The Management review panel and Partnership Board is responsible for the overall management and maintenance of the risk treatment plan, risk owners are responsible for the assigned tasks within the risk treatment plan.

The ISMS is subject to review and improvement as part of the Management Review process, and outputs from these meetings are fed into the Partnership Board meetings. Other representatives across the practice are periodically invited to the Management Review meetings, to further support the management of the ISMS and to complete relevant work as required, all of which is documented in accordance with the standard.

All employees and relevant Interested Parties associated to the ISMS are required to comply with this policy. Appropriate training and materials to support it are available for those in scope of the ISMS and communication forums such as the practices intranet are available to ensure engagement on an ongoing basis.

Ingleton Wood are committed to achieving and maintaining certification of the ISMS to ISO27001 along with other relevant accreditations against which our practice has sought certification.

This policy is reviewed periodically to respond to any changes in the practice strategic direction, it's risk assessment or risk treatment plan, at least annually.

3. Definitions

In this policy and the related set of policies contained within the ISMS, 'information security' is defined as:

preserving
This means that all relevant Interested Parties have, and will be made aware of, their responsibilities that are defined in their job descriptions or contracts to act in accordance with the requirements of the ISMS.

All relevant Interested Parties will receive information security awareness training and more specialised resources will receive appropriately specialised information security training.

the availability
This means that information and associated assets should be accessible to authorised users when required and therefore physically secure. The environment must be resilient, and the practice must be able to detect and respond rapidly to incidents or events that threaten the continued availability of assets, systems and information.

confidentiality
This involves ensuring that information is only accessible to those authorised to access it and preventing both deliberate and accidental unauthorised access to the practice and relevant Interested Parties information, proprietary knowledge, assets, and other systems in scope.

and integrity
This involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial, or complete, destruction or unauthorised modification, of either physical assets or electronic data.

of information and other relevant assets
The information can include digital information, printed or written on paper, transmitted by any means, or spoken in conversation, as well as information stored electronically. Assets include all information-based processing devices owned by the practice or those of relevant Interested Parties in scope that are processing practice related information.

Document Owner and Approval

The IT Partner is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the requirements set out in ISO27001:2013.

A current version of this document is available to all employees in the ISMS framework environment.

This information security policy has been approved by the Management Review Panel and Partnership Board and is issued on a version-controlled basis. For the purposes of ISMS solution approval, the Audit and Compliance Manager is the approver on behalf of the PMB.