Instem Information Security Management System

INFORMATION SECURITY POLICY

Intended Outcome of the system

The intended outcome of our Information Security Management System (ISMS) is to protect information assets to an appropriate level of the following: -

Confidentiality: Ensuring the information is accessible only to those who are authorised to have access

Integrity: Safeguarding the accuracy and completeness of information and processing methods

Availability: Ensuring access when required

Our Promise

Instem undertakes to keep safe the information that it receives and holds for its customers, staff and other stakeholders. We will only make such information available to those that need to see it and we will strive to ensure that all the information that we keep is necessary, complete and accurate.

Objectives

It is the objective of this policy and the supporting system to minimise undesired effects by identifying, reducing or preventing the impact of internal and external threats and vulnerabilities and to ensure:

- that business, regulatory, legislative and other information security requirements are understood and met;
- that we identify measurable Information Security objectives that we use to monitor and drive improvement;
- that the integrity of our ISMS is maintained when changes are planned and implemented, and we remain vigilant in an environment of constantly evolving threats;
- that all our people are aware, trained and competent in fulfilling their contribution to protect our information;

The ISMS is implemented in a manner that ensures that our widely geographically dispersed business can still operate with world-leading efficiency and effectiveness.

Continuous Improvement

As an organisation we are committed to the on-going review and improvement of our ISMS.
This policy is reviewed yearly as part of the Management review of the system.

Responsibilities

All staff are responsible for completing their required security training, including information security awareness training, as well as adhering to all security policies and procedures. This includes, but is not limited to practicing good cyber hygiene, ensuring the privacy and accuracy of information, and for reporting security incidents and responding to security notices as appropriate.

Approvals

Meaning of Signature: Approval by Management

Approver	Role	E-Signature	Date
Phil Reason	CEO	*Electronically signed by: Phil Reason Reason: Approve Date: Mar 7, 2024 12:25 EST*	Mar 7, 2024

Changes in this issue

General description of change	Reason for change
No changes – annual review	Annual review