7. Management Statement

SurgiQ is a knowledge-intensive organisation and needs to protect its growth and its shareholders' interests by protecting the value it creates. This includes the know-how we generate, our staff and third parties who make it possible and our clients exploiting it everyday.
SurgiQ has therefore decided to implement and maintain an Integrated Management System (IMS) in compliance with ISO/IEC 27001:2017 and ISO/IEC 9001:2015 standards and defined an Integrated Management System (IMS) Policy.

Scope
The scope of our IMS is "**Design, development, configuration, delivery and support of software solutions in the healthcare market** " which adheres to our core business of delivering innovative solutions based on our SurgiQ products to clients in the healthcare market and defines the perimeter of this policy.
The policy is implemented at all levels of the organisation by all users.

Aims
This policy is aimed at maintaining and improving service levels offered to our Clients. It is among SurgiQ aims to ensure that:

- customer is satisfied
- information are protected and not purposely or accidentally delivered to unauthorised individuals and entities
- information integrity is guaranteed and protected from erroneous or intentional modifications
- information are available at any moment to any authorised user
- business continuity is guaranteed by appropriate plans and actions
- staff is trained and audited on the policy and on the ISMS in general

Objectives
SurgiQ commits to:

1. the creation and fostering of a company culture on quality and information security
2. the identification of information and other assets' value, associated risks and potential threats and the management of such risks to bring it to an acceptable level through the implementation and maintenance of an IMS
3. the pro-active and early adoption of any mandatory regulation in terms of data protection, privacy and personal identifiable data

Governance & Responsibilities
This policy is produced and maintained by SurgiQ management. Specific roles and bodies (our CISO and the Information Security Committee) are in charge of defining and improving it and of monitoring its application.
Staff, at any level, and external collaborators must adhere to procedures defined by SurgiQ to make sure the policy is correctly implemented.
Staff, at any level, is responsible to prevent, report and react to information security incidents, and is subject to judgement and legal actions whenever applicable if found guilty.

Review
The policy is reviewed periodically to both improve it and make sure it suits business needs.