Information security policy statement

The objective of this Information Security Policy Statement is to ensure that CardioScan delivers a consistently high level of information security throughout its global businesses.

CardioScan is committed to protecting the company's employees, properties, information, reputation and customer's assets and their patients from potential threats; to implementing and maintaining compliance with ISO 27001; and to continuous, practical improvement of our information security practices. This will help reduce risk, maintain our reputation in the industry and meet our legal/regulatory and customers' requirements.

CardioScan commits to:

- Protecting its people, information, intellectual property, assets, activities and facilities against misuse, loss, damage, disruption, interference, espionage, or unauthorised disclosure. It is also critical that we retain the confidence of those who entrust sensitive information to CardioScan;
- Clearly understanding the requirements and expectations of our customers and relevant regulatory authorities;
- Working closely with our customers and suppliers to deliver services in a security conscious manner;
- Ensuring every employee shares responsibility for effective information security;
- Developing and maintaining security policies and controls designed to meet the requirements of ISO 27001. The policy statements contained in our Information Security Policy (ISP), procedures, guidelines, and standards, reflect the minimum requirements necessary to maintain an acceptable standard for protecting our information assets and, at the same time, our reputation;
- Implement an Information Security Management System (ISMS) and ensure it is maintained, continually improved, and supported with adequate resources to achieve the objectives set in this Policy Statement

Our approach to achieving these objectives is to enhance information security through investment in technology, processes, and employee skills and all staff are asked to consider and accept the important role they play in maintaining an effective information security program throughout CardioScan.

Management are responsible for embedding information security risk management in our core business activities, functions and processes and all personnel have a responsibility to report perceived and actual information security breaches and/or IT incidents to the IT Service Desk or their immediate managers.

Information Security Risk awareness and our tolerance for risk are key considerations in our decision making that will improve the way we both manage our business and deliver services to our customers.

This policy will be reviewed, and if necessary, revised, annually to keep up to date.

Signed:

Jeremy Steele
Chief Executive Officer

Document Number: C-POLICY-03
Document Name: Information Security Policy Statement

Date Modified: 29/01/2020
Version: 2

CardioScan