

## Information Security Policy

### Canon Medical Systems Ltd

Canon Medical Systems Limited (CMSUK) has adopted a security policy to meet with the requirements of ISO27001:2022 - Information Technology - Security techniques - Information security management systems - Requirements.

It is the Company's policy to ensure that information, systems used to hold or process information and data, staff, external personnel and or contractors, are administered and operate in a safe & secure environment in order to

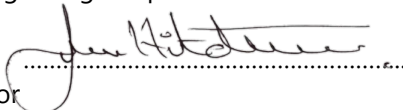
- Protect the trusted partner status of the Company
- Reduce the risk of the corruption or loss of user confidence or customer information
- Protect information confidentiality, integrity & availability
- Protect appropriate access to information & information systems to authorized users of information
- Ensure compliance with current legislation & regulatory requirements especially the GDPR and the Data Protection Act 2018
- Establish a business continuity plan to minimize departmental damage by minimizing the impact of information security breaches and disaster,
- Protect networks & information processing systems from loss, theft, unauthorized copying, and tampering & intended or accidental change to information or software.
- Safeguard the Company against the use of illegal or unlicensed software.
- Prevent the inadvertent or malicious introduction of viruses or other interference

CMSUK recognises that Information Technology / Information Systems play a major role in our business activities. Like any other asset, the data in our possession and the infrastructure that handles it, must be kept secure. A breakdown in security could have serious effects on our business. Any breach could result in a direct financial loss, a loss of confidence, or a breach of legal and/or regulatory requirements. For these reasons the Board of Directors have approved the creation and companywide implementation of an Information Security Management System ("ISMS") and programme.

The ISMS establishes standards that represent the minimum-security requirements that apply to all our information systems, and the processes that support them. It also gives important responsibilities to managers who must ensure compliance within their areas of control. This will ensure that there is a correct balance between the objectives of creating and maintaining an open, trusting environment in which information, with limited exceptions, is made freely available to all employees, while protecting our data from accidental or deliberate loss, alteration, or disclosure.

It is essential that this Policy is fully implemented and that all employees are aware of their responsibilities regarding the protection of data and systems against unauthorised access or disclosure.

Mark Hitchman  
Managing Director



Date 13th January 2023

This policy is available to interested parties on request.