Canon
CANON MEDICAL SYSTEMS LTD

Made For life

Information Security Policy
Canon Medical Systems Ltd

Canon Medical Systems Limited has adopted a security policy to meet with the requirements of ISO27001:2013 - 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

The Company has appointed an Information Security Officer directly responsible for managing, monitoring and advising on information security. Appropriate training & guidance is provided to all concerned with the implementation of this policy.

Security objectives will be set, measured and analyzed for key parts of our ISMS system.

The Policy will be communicated to all new employees, and is displayed at key locations.

As part of this policy the Company will undertake a programme of regular audits to verify compliance to the standard.
The Company will undertake regular Management Reviews [Security Forums] to assess the suitability of the programme & to review audits and security breaches. Opportunities for continual improvement will be identified where appropriate and will be actioned.

Mark Hitchman M. Hitchman Date 22-01-20
Managing Director

This policy is available to interested parties on request.

POL-0018[02]