# Information Security Policy – Beacon Medical Systems Ltd (Beacon)

**Document Control**

**Policy Owner:** Senior Information Risk Officer (SIRO) / Engineering Lead
**Approval Date:** 05/11/2025
**Effective Date:** 05/11/2025

**Review Date:** November 2026

**Note:** This policy must be reviewed annually or when significant changes occur to ensure its continued relevance and effectiveness.

| Date | Version | Author | Reason for amendment |
|---|---|---|---|
| 08/06/2024 | 2.0 | Claire Robinson (DPO) | Create formalised Information Security Policy for ISO 27001 (referencing prior policies) |
| 05/11/2025 | 2.1 | Claire Robinson | Alignment with Beacon Control Framework (November 2025) and ISO/IEC 27001:2022 updates |

**1. Introduction**

Information is one of Beacon Medical Systems Ltd's (Beacon's) most valuable assets. Protecting information to a consistently high standard gives service users, customers, and partners confidence to engage with Beacon, supports compliance with legal and contractual obligations, and maintains organisational reputation and operational resilience.
This policy sets out Beacon's approach to ensuring the confidentiality, integrity, and availability of all information assets through an Information Security Management System (ISMS) aligned with ISO/IEC 27001.

**2. Purpose and Objectives**

The objectives of this policy are to:

- Protect information assets under Beacon's control.
- Ensure that all staff understand their roles and responsibilities regarding information security.
- Provide a consistent framework for implementing security controls.

- Establish and maintain the security, confidentiality, and integrity of information, systems, applications, and networks.
- Demonstrate best practice and regulatory compliance in information management.

### 3. Scope

This policy applies to all Beacon employees, contractors, agency staff, consultants, and third parties with authorised access to Beacon's information, systems, or facilities. It covers both corporate systems and the SaaS platform environments managed or hosted by Beacon.

### 4. Definitions

**Information Asset:** Any data or information of value to Beacon, whether physical (paper, removable media) or electronic (databases, emails, software code).
**Information Security:** The protection of information assets from threats to ensure business continuity, minimise operational disruption, and maximise business opportunity, through ensuring:

- **Confidentiality** – access only to authorised persons.
- **Integrity** – protection against unauthorised alteration or corruption.
- **Availability** – access to authorised users when required.

### 5. Leadership and Commitment

Top management demonstrates leadership and commitment to information security by:

- Ensuring that the ISMS is aligned with Beacon's strategic direction.
- Providing appropriate resources to implement and maintain security controls.
- Communicating the importance of effective information security management.
- Supporting continual improvement of the ISMS and ensuring regular performance reviews.

The Chief Executive Officer (CEO), Chief Technical Officer (CTO), and Senior Information Risk Officer (SIRO) are considered *Top Management* for ISMS purposes.

### 6. Roles and Responsibilities

**All Staff:** Must complete annual Data Security and Protection (DSP) training, understand how to handle, store, and share information securely, and report any suspected breaches or weaknesses immediately.

**Chief Executive Officer:** Holds overall accountability for information security.

**Head of Engineering / SIRO:** Responsible for technical controls, ensuring compliance with data protection and information security requirements.

**CISO/Quality Manager:** Leads the ISMS and advises the Board on risk management, ensuring assessment and control measures are implemented and reviewed.

**Data Protection Officer (DPO):** Advises on UK GDPR and Data Protection Act compliance, monitors data protection practices and DPIAs, and acts as contact point for the ICO and data subjects.

### 7. Risk Assessment and Treatment

Beacon maintains a systematic approach to identifying, evaluating, and mitigating information risks by:

- Conducting regular risk assessments;
- Documenting and reviewing risk treatment plans;
- Applying risk control measures to reduce likelihood and impact;
- Ensuring all significant risks are logged within the central risk register.

### 8. Asset Management

Beacon maintains an inventory of all information assets and their classification by sensitivity. Each asset has a designated owner responsible for security and lifecycle management. Assets are handled, stored, and disposed of securely in accordance with classification.

### 9. Access Control

Access to information systems is granted based on the principle of least privilege and a demonstrated business need. Access requests are approved and logged; two-factor authentication is used wherever possible. External access must be formally authorised and contractually governed.

### 10. Data Protection and Training

All staff must complete mandatory annual training covering data protection, cyber security, and acceptable use. Compliance training completion is recorded in Beacon's Training Matrix.

### 11. Incident Reporting and Exceptions

All exceptions to this policy must be logged and approved by the SIRO or CTO. Security incidents must be reported immediately via the IT Ticketing System or directly to the Information Security and Risk Manager. Non-compliance by others must be reported to management or the SIRO.

### 12. Non-Compliance and Corrective Action

Failure to comply with this policy may result in disciplinary action, up to and including termination. Non-conformities identified through audits or monitoring will be corrected through formal action plans overseen by the SIRO and reported to the management review board.

### 13. Business Continuity

Information security requirements will be integrated within Beacon’s Business Continuity and Disaster Recovery planning to ensure resilience and service availability during disruption.

### References

- Identity & Access Control Policy
- **ISO/IEC 27001:2022** – A.5.17 (Authentication information), A.5.18 (Use of privileged utility programs)
- **ISO/IEC 27002:2022** – Information security, cybersecurity and privacy protection
- **NIST SP 800-63B –** Authentication and Lifecycle Management
- **Cyber Essentials Plus**

### Annex A: ISO/IEC 27001:2022 Controls

| Control Reference | Control Description |
|---|---|
| **A.5.17** | Authentication information – Allocation and management of authentication information must be controlled by a formal management process. |
| **A.5.18** | Use of privileged utility programs – Restrict and tightly control use of utilities capable of overriding system/application controls. |
| **A.5.15** | Access control – Implement rules for access to information and systems based on business and security requirements. |
| **A.5.16** | Identity management – Assign unique identities to users and manage them throughout their lifecycle. |
| **A.5.20** | Use of privileged accounts – Ensure privileged accounts are strictly controlled, traceable, and used only when necessary. |

### Related Beacon Policies

**Access Control Policy –** Governs identity verification, account lifecycle, and role-based access.

**Configuration Management Policy –** Ensures password-related configuration items (e.g. authentication services, PAM systems) are recorded and reviewed.

**Incident & Problem Management Policy –** Defines how suspected password compromises are reported and managed.

**Business Continuity and Disaster Recovery Policy –** Ensures credential management during DR/BCP invocation.

**Data Centre Management & Cloud Security Policy –** Applies to password controls for cloud services and hosted environments.