Information Security Policy

Document Control

Policy Owner: Senior Information Risk Officer (SIRO) / Engineering Lead
Approval Date: [Date]
Effective Date: [Date]
Review Date: [Date]

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

08/06/2024	2.0	Claire Robinson (DPO)	Create formalised Information Security Policy for ISO 27001 (referencing other previous Pando policies).
		Rob Cherry (Reviewer)	

1. Introduction

Our information is an asset and needs to be protected to give our service users, customers, and partners confidence to engage with us, maintain our reputation, and meet our legal, regulatory, and contractual obligations.

The purpose of Beacon's Information Security Policy is to protect, to a consistently high standard, all information assets. The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and corporate way.
- Assurance that Beacon is providing a secure and trusted environment for the management of information used in delivering its business.
- Demonstration of best practice in information security.
- Assurance that risks are identified, and appropriate controls are implemented and documented.

2. Definition - Information Asset

An information asset can be described as information or data that is of value to the organisation, including such information as patient records, intellectual property, or

customer information. These assets can exist in physical form (on paper, CDs, or other media) or electronically (stored on databases, in files, on personal computers).

3. Information Security Definitions

Information security controls protect information assets from a range of threats to ensure business continuity, minimise damage to business operations, and maximise business opportunities. Information security has three elements:

- **Confidentiality** – ensuring that information is available only to those individuals or groups who are authorised to access it.

- **Integrity** – preventing unauthorised tampering with, or corruption of, information assets or information processing facilities.

- **Availability** – ensuring that authorised users have access to information assets and services when required and without undue delay.

4. Objectives

The objectives of this policy are to establish and maintain the security and confidentiality of information, information systems, applications, and networks owned or used by Beacon by:

- Ensuring that all members of staff are aware of their information security roles, responsibilities, and accountability and fully understand their own responsibilities.
- Describing the expected behaviours and principles of security and outlining how these must be implemented in the organisation to establish a consistent approach to security.
- Creating and maintaining within Beacon an appropriate level of awareness of the need for information security as an integral part of the day-to-day business.
- Protecting information assets under the control of Beacon.

5. Scope

This policy applies to all members of Beacon, including management, general staff, contractors and sub-contractors, agency staff, consultants, interns, and other work experience personnel.

This policy is applicable to security that can be protected by technology and the behaviours of the people managing and accessing information in the line of Beacon's business. Information security is also about people's behaviour in relation to the information they are responsible for, helped by the appropriate use of technology.

6. Top Management Leadership and Commitment

Commitment to information security extends to senior levels of Beacon and is demonstrated through this policy and the provision of appropriate resources to provide and develop an appropriate information security management system (ISMS) and associated controls.
Within the scope of this ISMS, the Chief Executive Officer (CEO), Chief Engineering/Technical Officer (CTO), and Senior Information Risk Manager (SIRO) are considered as top management.
Top management will ensure:

- The information security policy and information security objectives of Beacon are established and compatible with the strategic direction of Beacon.
- The appropriate resources are available to maintain the information security management system and ensure information security controls are appropriately embedded in other Beacon processes as required.
- Effective communication of the information security management system and conforming to the information security management system requirements.
- The information security management system achieves its objectives.
- Direction and support are provided to persons to contribute to the effectiveness of the information security management system.
- The promotion of continual improvement and support others in their areas of responsibility.

Top Management will also ensure that a systematic review of the performance is conducted on a regular basis to ensure that quality objectives are being met and quality issues are identified through the audit programme and management processes. Management review will be carried out at least annually.

7. Roles and Responsibilities

All Staff
All staff are responsible for information security and must understand and comply with this policy and associated guidance. In particular, all staff should take appropriate precautions to protect the security and confidentiality of information. Staff must undertake their mandatory annual data security and protection (DSP) training and understand:

- What information they are using, how it should be protectively handled, stored, and transferred.
- What procedures, standards, and protocols exist for the sharing of information with others.
- How to report a suspected breach of information security within the organisation or raise any information security concerns with the Senior Information Risk Officer (SIRO).

Chief Executive Officer

Responsibility for information security resides ultimately with the Chief Executive. This responsibility is discharged through the designated roles of the Head of Engineering who fulfils the SIRO role, the Head of Operations, Team Leaders and all staff.

Head of Engineering

The Head of Engineering is responsible for ensuring that all Beacon's SaaS Platform Product electronic equipment and assets have adequate security measures to comply with data protection and data security legislation and regulations.

Senior Information Risk Officer

The Senior Information Risk Officer (SIRO) is responsible for developing, implementing, and enforcing suitable and relevant information security procedures and protocols to ensure Beacon systems and infrastructure (corporate and SaaS Platform) remain compliant with all relevant legislation and security governance.

The Senior Information Risk Officer is responsible for information risk within Beacon and advises the board on the effectiveness of information risk management across the organisation.

The Senior Information Risk Officer is also responsible for ensuring that the People team have policies and procedures so that:

- All employees have appropriate education, training, skills, and experience to meet their information security responsibilities.
- The skills required will be determined and reviewed on a regular basis together with an assessment of existing skill level within Beacon.
- Appropriate and proportionate pre-employment checks are performed to reduce information security risks.

The Data Protection Officer (DPO)

The DPO assists the controller or the processor in all issues relating to the protection of personal data. In particular, the DPO must:

- Inform and advise the controller or processor, as well as their employees, of their obligations under data protection law.
- Monitor compliance of the organisation with all legislation in relation to data protection, including in audits, awareness-raising activities as well as training of staff involved in processing operations.
- Provide advice where a DPIA has been carried out and monitor its performance.
- Act as a contact point for requests from individuals regarding the processing of their personal data and the exercise of their rights.
- Cooperate with DPAs and act as a contact point for DPAs on issues relating to processing.

The organisation must involve the DPO in a timely manner. The DPO must not receive any instructions from the controller or processor for the exercise of their tasks. The DPO reports directly to the highest level of management of the organisation.

8. Risk Assessment and Treatment

A systematic approach will be taken to identify, assess, and treat risks associated with information security. This involves:

- Conducting regular risk assessments using established methodologies to identify threats and vulnerabilities to information assets.
- Evaluating risks based on their potential impact and likelihood.
- Implementing appropriate risk treatment plans to mitigate identified risks, which may include avoiding, transferring, accepting, or reducing risks through the implementation of controls.
- Documenting and regularly reviewing risk assessments and treatment plans to ensure their effectiveness and make necessary adjustments.

9. Asset Management

To ensure comprehensive protection of information assets:

- An inventory of all information assets will be maintained, categorising them according to their importance and sensitivity.
- Each asset will have an assigned owner responsible for its security.
- Procedures will be established for the proper handling, storage, and disposal of information assets to prevent unauthorised access, alteration, or destruction.
- Regular reviews will be conducted to ensure that the asset management process remains effective and up to date.

10. Access to Systems

Access to systems and information is granted with an approved request ticket or upon joining with a new joiner request and must only be granted where there is a justifiable business requirement and must be granted on a least privilege basis.

Access to applications is provided by individual password-protected accounts, with 2-factor authentication enabled where possible.

Use of Beacon systems must be in line with the Acceptable Use policy guidelines.

Contracts with external contractors that allow access to the organisation’s information systems must be in operation before access is allowed. These contracts must ensure that the

staff or subcontractors of the external organisation comply with all appropriate security policies.

11. Data Protection and Information Security Training

All staff must undertake the following security and compliance training courses within 3 months of starting and annually:

- Data protection / UK GDPR and Cyber Security Awareness online course (e-LfH).

12. Exceptions and Reporting

- All exceptions to this policy are to be logged within the service management system and signed off by the Information Security and Risk Manager or the Chief Technology Officer.
- Any suspected threat to Beacon should be reported immediately in the IT Ticketing system or to the Information Security and Risk Manager.
- Employees observing others who are not in compliance with this policy should report the matter to the CTO.

13. Implications of Non-Compliance

Failure to comply with the Information Security Policy will result in management review and following of the Company disciplinary procedure as appropriate to the nature and severity of the non-compliance in the considered opinion of management, up to and including termination of employment, in line with Beacon's disciplinary process.

Control of Non-Conformities and Corrective Actions

- When a non-conformity is identified through daily checks, internal or external audits, it must be controlled through an appropriate corrective action to eliminate or at least minimise risk to Beacon or its interested parties.
- The SIRO will react to any non-conformities and take appropriate actions to control, correct, and report on the non-conformity to management.

Annex A Controls

To ensure the implementation of effective information security controls, Beacon will adhere to the controls specified in Annex A of the ISO 27001 standard. These controls include:

A.5 Information Security Policies

- **A.5.1 Management direction for information security**: Establish a framework for setting objectives and guiding principles for information security throughout the organisation.

A.6 Organisation of Information Security

- **A.6.1 Internal organisation**: Establish and maintain an information security management structure.
- **A.6.2 Mobile devices and teleworking**: Develop policies and procedures to manage risks associated with mobile devices and teleworking.

A.7 Human Resource Security

- **A.7.1 Prior to employment**: Implement screening and background verification of candidates.
- **A.7.2 During employment**: Provide ongoing security awareness and training.
- **A.7.3 Termination and change of employment**: Ensure the return of all organisational assets and removal of access rights upon termination or change of employment.

A.8 Asset Management

- **A.8.1 Responsibility for assets**: Ensure that information and associated assets are appropriately protected.
- **A.8.2 Information classification**: Classify information to ensure appropriate levels of protection.
- **A.8.3 Media handling**: Manage media securely to protect information.

A.9 Access Control

- **A.9.1 Business requirements for access control**: Limit access to information and information processing facilities to authorised users.
- **A.9.2 User access management**: Ensure users are given access only to the information and systems necessary for their role.
- **A.9.3 User responsibilities**: Implement user responsibilities for information security.
- **A.9.4 System and application access control**: Control access to systems and applications.

A.10 Cryptography

- **A.10.1 Cryptographic controls**: Use cryptographic techniques to protect information.

A.11 Physical and Environmental Security

- **A.11.1 Secure areas**: Prevent unauthorised physical access to information processing facilities.
- **A.11.2 Equipment security**: Ensure the secure use and disposal of equipment.

A.12 Operations Security

- **A.12.1 Operational procedures and responsibilities**: Establish procedures to ensure the correct and secure operation of information processing facilities.
- **A.12.2 Protection from malware**: Implement controls to prevent and detect malware.
- **A.12.3 Backup**: Implement procedures to ensure the availability of information.
- **A.12.4 Logging and monitoring**: Monitor systems to detect security events.
- **A.12.5 Control of operational software**: Ensure the integrity of operational software.
- **A.12.6 Technical vulnerability management**: Manage technical vulnerabilities.
- **A.12.7 Information systems audit considerations**: Minimise the impact of audit activities on operational systems.

A.13 Communications Security

- **A.13.1 Network security management**: Ensure the security of information in networks.
- **A.13.2 Information transfer**: Protect information in transit.

A.14 System Acquisition, Development, and Maintenance

- **A.14.1 Security requirements of information systems**: Ensure that information security is an integral part of information systems across the entire lifecycle.
- **A.14.2 Security in development and support processes**: Implement security measures in development processes.
- **A.14.3 Test data**: Protect test data.

A.15 Supplier Relationships

- **A.15.1 Information security in supplier relationships**: Ensure protection of information that is accessible by suppliers.
- **A.15.2 Supplier service delivery management**: Monitor and review supplier services.

A.16 Information Security Incident Management

- **A.16.1 Management of information security incidents and improvements**: Ensure a consistent and effective approach to the management of information security incidents.

A.17 Information Security Aspects of Business Continuity Management

- **A.17.1 Information security continuity**: Ensure the availability of information processing facilities.
- **A.17.2 Redundancies**: Implement redundancy measures to ensure information availability.

A.18 Compliance

- **A.18.1 Compliance with legal and contractual requirements**: Identify and meet applicable legal, regulatory, and contractual requirements.
- **A.18.2 Information security reviews**: Ensure that information security is implemented and operated in accordance with organisational policies and procedures.

References

- **ISO/IEC 27001:2013**: Information technology – Security techniques – Information security management systems – Requirements.
- **ISO/IEC 27002:2013**: Information technology – Security techniques – Code of practice for information security controls.
- **General Data Protection Regulation (GDPR)**: Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
- **Data Protection Act 2018**: The UK's data protection law
- **UK GDPR**: The UK's version of the EU GDPR which sits alongside the data protection Act.