



Pando is a subsidiary product of Beacon Medical Systems Ltd.  
Registered Address: 5 New Street Square, London, United Kingdom, EC4A 3TW  
Company number: 10420044

## 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 Pando'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 Pando is providing a secure and trusted environment for the management of information used in delivering its business;
- Demonstration of best practice in information security;
- Assurances that risks are identified and appropriate controls are implemented and documented.

## 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)

## 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.



Pando is a subsidiary product of Beacon Medical Systems Ltd.  
Registered Address: 5 New Street Square, London, United Kingdom, EC4A 3TW  
Company number: 10420044

## 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 Pando 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 Pando 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 Pando.

## Scope

This policy applies to all members of Pando, 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 Pando'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.

## Top Management Leadership and Commitment

Commitment to information security extends to senior levels of Pando 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 Pando are established and compatible with the strategic direction of Pando;
- The appropriate resources are available to maintain the information security management system and ensure information security controls are appropriately embedded in other Pando 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;



Pando is a subsidiary product of Beacon Medical Systems Ltd.

Registered Address: 5 New Street Square, London, United Kingdom, EC4A 3TW

Company number: 10420044

- Direction and support is 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 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 at least annually

## **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 Chief Engineering/Technology Officer (CTO), Director of Commercial, Head of People (HR) and all staff.

### **Chief Engineering/Technology Officer**

The Chief Engineering/Technology Officer is responsible for ensuring that all Pando'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 Information Security and Risk Manager is responsible for developing, implementing and enforcing suitable and relevant information security procedures and protocols to ensure Pando



Pando is a subsidiary product of Beacon Medical Systems Ltd.

Registered Address: 5 New Street Square, London, United Kingdom, EC4A 3TW

Company number: 10420044

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 Pando 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 Pando;
- Appropriate and proportionate pre-employment checks are performed to reduce information security risks.

### **The Data Protection Officer**

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.

### **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.



Pando is a subsidiary product of Beacon Medical Systems Ltd.

Registered Address: 5 New Street Square, London, United Kingdom, EC4A 3TW

Company number: 10420044

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

Use of Pando 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 sub-contractors of the external organisation comply with all appropriate security policies.

### **Compliance and 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).
- Fraud prevention online course
- Whistleblowing online course
- Anti-bribery online course

### **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 Pando 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.

### **Implications of Non-Compliance**

Failure to comply with 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 Pando's disciplinary process.

### **Control of Non-Conformities and Corrective Actions**

- When a nonconformity 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 Pando or its interested parties.



Pando is a subsidiary product of Beacon Medical Systems Ltd.  
Registered Address: 5 New Street Square, London, United Kingdom, EC4A 3TW  
Company number: 10420044

- The CTO along with the SIRO will react to any nonconformities and take appropriate actions to control, correct and report on the nonconformity to management.

## Authorisation & Document Control

<b>Document Title</b>	Information Security Policy			<b>Status</b>	Live
<b>Classification</b>	Internal and external on request	<b>Last Review</b>	April 2023	<b>Next Review</b>	April 2024
<b>Location</b>	Shared Drive – Policies folder				

<b>Authorisation</b>	<b>Responsible Person or Body</b>
<b>Document Owner</b>	Philip Mundy
<b>Authorised By</b>	Philip Mundy

## Related Policies

- Data classification policy;
- Password policy

## Version History

Version	Author	Issued	Summary of Changes
1.0	Claire Robinson	February 2022	New policy to replace separate Pando and Juno policies to reflect changes to business structure and organisational needs and to align for ISO 27001.
2.0	Clare Robinson	April 2023	Annual Update, update to Beacon Medical Systems Ltd.