INFORMATION SECURITY POLICY

Babylon's Information Security policy ensures the confidentiality, integrity, security and availability of internal, customer, patient and supplier information.

Inadequate information security controls can lead to incidents, such as breaches of confidentiality, corruption or unavailability of information, which could affect Babylon's patients' lives, our regulatory compliance position, our reputation. and continuing ability to deliver our services.

Information and information security requirements will continue to be aligned with Babylon's goals. Information security objectives are set annually by Babylon's Security Council to ensure that we are able to determine the effectiveness of the information security measures we have in place.

This policy is intended to be an enabling mechanism for information sharing, for electronic operations and for reducing information-related risks to acceptable levels. This policy applies to all Babylon operations in all geographic locations.

Information security management is achieved through the use of a number of controls including policies, processes, procedures, software, and hardware functions. These controls are continually monitored, reviewed and improved to ensure that specific security and business objectives are met. These controls are operated in conjunction with other business management processes and incorporate the applicable statutory and contractual requirements.

Information Security is controlled through the preservation of:

- **Confidentiality** - ensuring that information is only accessible to those authorised to access it and therefore to prevent both deliberate and accidental unauthorised access to Babylon's information.
- **Integrity** - safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorised modification, of either physical assets or electronic data.

  There must be appropriate contingency and data backup plans and security incident reporting procedure. Babylon must comply with all relevant data-related legislation in those jurisdictions within which it operates.
- **Availability** - information and associated assets should be accessible to authorised users when required and therefore physically secure.

In support of this Policy, Babylon's leadership are committed to:

- Manage and reduce information risk in an informed manner
- Ensure compliance to all applicable legal and regulatory requirements
- Provide appropriate information security resources
- Continual improvement of Babylon's information security management system.

The computer network must be resilient and Babylon must be able to respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information. There must be appropriate business continuity plans.

Babylon operates a programme of information security awareness and compliance through company inductions, training and internal audits.

Information security is everyone's responsibility. All employees are empowered to identify any potential security weaknesses and /or incidents and report through the appropriate management channels.

A robust system is in place to continually improve the security controls to:

- Take account of changes to business requirements and priorities;
- Consider new threat and vulnerabilities
- Confirm that controls remain highly effective and appropriate

Signed by

G mudie
G mudie (Mar 13, 2020)

Gary Mudie
Chief Product Officer and SIRO

A. Parsa
Ali Parsa (Mar 13, 2020)

Ali Parsa
Chief Executive Officer and Founder