medvivo
integrating health and care

Medvivo Group

Information Security Policy

V1

Date of Implementation:	10/01/2020
Date of Next Review:	10/01/2021
Version:	1
Responsible Executive Director:	Chief Information Officer
Author:	Head of Information Security & Compliance
Policy Location:	An electronic copy is available on the Medvivo intranet.
Equality Impact Assessment:	The Equality Impact Assessment screening did not indicate that this policy will have an adverse impact on any person or group in relation to Age, Race / Ethnicity, Gender, Religion, Sexual Orientation or Disability. At this stage it will not be necessary to conduct a full impact assessment. In the event that this policy is reviewed or amended, a further Equality Impact Assessment screen would be recommended.
Policy Status:	This policy does not give contractual rights to individual members of staff. The organisation reserves the right to alter any of its terms at any time although we will notify you of any changes.

Amendments Summary

Version	Date Issued	Section	Subject
1	10/01/2020	NA	First authorised version.

Contents

1. Introduction

1.1. The Medvivo Executive Management Team understand the information security needs and expectations of its interested parties both within the organisation and from external parties including, amongst others, patients, clients, suppliers, commissioners, regulatory and governmental departments.

1.2. Medvivo has recognised that the disciplines of confidentiality, integrity and availability of information in information security management are integral parts of its management function and view these as their primary responsibility and fundamental to best business practice.

1.3. The Medvivo Quality Committee have approved the Information Security Business Management System Manual and associated polices that make up the Medvivo ISO 27001:2017 certified Information Security Management System (ISMS)

2. Statement of Intent

2.1. The purpose of this policy is to protect all Medvivo information assets from all threats, whether internal or external, deliberate or accidental.

3. Scope

3.1. This policy applies to all Medvivo staff who either work for Medvivo or provide services on behalf of Medvivo (including contractors and sub-contractors).

4. Policy

4.1. It is the policy of Medvivo to ensure that Medvivo:

- Complies with all applicable laws, regulations and contractual obligations;
- Implements Information Security Objectives that take into account information security requirements following the results of applicable risk assessments;
- Communicates these Objectives and performance against them to all interested parties;
- Adopts an information security management system comprising a manual, policies and procedures which provide direction and guidance on information security matters relating to employees, customers, suppliers and other interested parties who come into contact with its work;
- Works closely with Customers, Business partners and Suppliers in seeking to establish appropriate information security standards;
- Adopts a forward-thinking approach on future business decisions, including the continual review of risk evaluation criteria, which may impact on information security;
- Instructs all members of staff in the needs and responsibilities of information security management;
- Constantly strives to meet, and where possible exceed, its customer’s expectations;

- Implements continual improvement initiatives, including risk assessment and risk treatment strategies, while making best use of its management resources to meet information security requirements better.

4.2. In addition, It is the policy of Medvivo to ensure that everyone within Medvivo:

- Handle company information and users' personal data in an appropriate manner;
- Limit personal use of Medvivo's information and telecommunication systems and ensure it doesn't interfere with their job performance;
- Do not use e-mail, internet and other company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Protect and do not disclose personal and sensitive data unless authorised;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third-party connections, etc.;
- Do not install unauthorised software or hardware unless they have explicit management approval;
- Always leave desks clear of personal or sensitive data and lock computer screens when unattended;
- Report information security incidents immediately, to the IT Service Desk.

5. Communication of Policy

5.1. This policy is a mandatory read and is available to all staff via Webvivo.

6. Monitoring and Review of the Policy

6.1. The Executive Management Team are responsible for reviewing the policy one year after implementation and bi-annually thereafter.

7. Associated Policies and Procedures

- Business Management System Manual (ISMS)
- Acceptable Use Policy
- Access Control Policy
- Data Protection Policy
- Confidentiality Policy
- Control of Records Policy
- Information Security Incident Management Policy
- Privacy and Data Sharing Policy
- Supplier Management Policy