POL – Information Security

Version 1

Table of Contents

1 Introduction

1.1 Purpose

The purpose of this policy is to establish and maintain effective information security practices within WAVY MEET. These practices aim to ensure the confidentiality, integrity, and availability of information, in accordance with ISO 27001 standards and the requirements of the European Medical Device Regulation.

1.2 Applicability and scope

This document applies to all employees, contractors, and third parties who have access to or are involved in the operation of the WAVY MEET. It covers all information assets, systems, and processes related to the platform's development, maintenance, and support.

1.3 Terms and definition

Term	Definition

1.4 Referenced documents

Reference	Document	Version (optional)
MDR	Regulation (EU) 2017/745 of the European Parliament and of the council of 5 April 2017 on medical devices	Regulation (EU) 2017/745
ISO27001	Information technology - Security techniques - Information security management systems - Requirements	ISO-IEC-27001-2017-E

2 Responsibilities

2.1 Data Protection Officer

The Data Protection Officer (DPO) will be responsible for implementing and overseeing information security within WAVY MEET, ensuring compliance with ISO 27001 and the European Medical Device Regulation.

3 Information Security Objectives:

Objective 1: To protect sensitive information related to WAVY MEET products and its users from unauthorized access, disclosure, alteration, and destruction.
Objective 2: To ensure the secure transmission of data (including personal and medical data) between the platform and the users, and among users.
Objective 3: To maintain the availability and reliability of WAVY MEET products, enabling uninterrupted access for healthcare professionals and referred patients.

4 Applicable Requirements

WAVY MEET is committed to complying with all applicable legal, regulatory, and contractual requirements related to information security, including those specified in the European Medical Device Regulation and ISO 27001.

5 Continual Improvement

WAVY MEET is dedicated to continually improving its information security management system (ISMS) to adapt to evolving threats and technological advancements. Regular assessments, reviews, and updates will be conducted at least once a year to enhance the effectiveness and efficiency of our security measures.

6 Documentation and Communication:

This Information Security Policy shall be documented and made available as a reference for all employees and relevant stakeholders. WAVY MEET will ensure effective communication of this policy to all employees, emphasizing their roles and responsibilities in safeguarding information security. The policy will also be made available to interested parties as appropriate, maintaining transparency in our commitment to information security.

7 Security Measures

WAVY MEET utilizes secure channels for all communications and enforces 2-factor authentication to enhance user authentication and access control.

8 Training and Awareness:

WAVY MEET establishes training and awareness programs to educate employees about information security practices and their roles in maintaining data confidentiality. These programs will emphasize the importance of protecting sensitive information and promote a culture of security within the organization.

9 Third-Party Service Providers:

WAVY MEET does not currently involve any third-party service providers in the operation of the WAVY MEET platform. However, should such partnerships arise in the future, WAVY MEET will ensure that these providers comply with information security requirements through appropriate contractual agreements and due diligence processes.