

POLICY
ON INFORMATION SECURITY
of “Antibiotic” Group*

1. INTRODUCTION

This policy should define practices for managing and maintaining information security in the companies of **“Antibiotic” Group**. The policy is based on regulatory requirements in the Republic of Bulgaria, as well as European legislation.

2. OBJECTIVES

- 2.1 Ensuring continuity of core business processes and services provided to customers;
- 2.2 Minimizing the risks causing damages to the information;
- 2.3 Reliable protection of the information during its creation, processing, storage, transfer and exchange;
- 2.4 Minimizing potential losses and damages from a breach.

3. TERMS AND DEFINITIONS

Information security – protection of information from unauthorized access, use, disclosure, alteration, recording or destruction

IT security - information security applied to computerized systems

Information protection- prevention of data loss in the event of natural disasters, accidents, theft, etc.

Security threat – software attacks; theft of intellectual property, identity, device; sabotage or manipulation.

4. BASIC PRINCIPLES

At the core of the dynamically developing technological environment, the activities of the companies of the group are faced with security threats. In order to respond to the risk of these threats, it is necessary to build a system to control

access and work with information, which minimizes and manages the risks that can lead to damage to assets - physical, intellectual, technical, etc. Information security is based on four fundamental principles:

4.1 Data availability - accessibility and usability upon request from an authorized entity;

4.2 Data integrity - data storage in full volume and accuracy;

4.3 Confidentiality - accessibility to authorized persons only;

4.4 Protection of employees and assets.

The management of "**Antibiotic**" **Group** is committed to develop, implement and maintain an information security management system for:

- ❖ Implementation of applicable regulatory requirements, international standards or contractual obligations;
- ❖ Continuous improvement in relation to changes in the legislation or business environment;
- ❖ Compliance of the system with risk management conditions.

5. SCOPE

The information security management system covers:

5.1 Technical means – equipment for creating, processing and transferring information, as well as the necessary infrastructure;

5.2 Software – operating systems and application programs;

5.3 Data - processed information, regardless of the form of storage, provision and exchange.

6. CHANGES

This policy may be updated, amended or changed to meet the requirements of the law, good practices, our partners and stakeholders.

Adopted by Protocol dated 08.11.2022. from a meeting of the Board of Directors of “Antibiotic – Razgrad” AD.