cybix.

COMPANY POLICY · FINAL

Information Security Policy.

How Cybix protects the confidentiality, integrity and availability of its information, and our commitments under ISO/IEC 27001:2022.

1 Introduction

1.1 As a modern, forward-looking business that handles sensitive information, we recognise at all levels the need to ensure that our business operates smoothly, without interruption and, above all, in a secure way for the benefit of our customers, shareholders and other stakeholders.

1.2 To provide such a level of continuous operation, we have implemented an Information Security Management System (ISMS) in line with ISO/IEC 27001:2022.

2 Purpose

2.1 The purpose of this policy is to protect all information assets within the company from all internal and external threats, whether deliberate or accidental. This policy aims to protect the confidentiality, integrity and availability of information in all forms, whether stored electronically, transmitted across networks, or printed on paper.

3 Scope

3.1 This policy applies to all systems, people and processes that constitute the company's information systems, including board members, employees, suppliers and other third parties who have access to company systems.

4 Confidentiality, Integrity and Availability

4.1 Throughout this policy and the ISMS, the protection of information is expressed through three properties:

(a) **Confidentiality:** information is accessible only to those authorised to access it, and is protected from disclosure to anyone else.

(b) **Integrity:** information is accurate and complete, and is protected from unauthorised or accidental modification, whether in storage, processing or transit.

(c) **Availability:** information and the systems that process it are accessible and usable by authorised users when required.

4.2 Every control we operate exists to protect one or more of these properties.

5 Policy Commitments

5.1 The company is committed to:

(a) Satisfying all applicable requirements related to information security.

(b) Continual improvement of the information security management system.

(c) Setting and achieving information security objectives through regular review of objectives at Management Review.

(d) The implementation and maintenance of an Information Security Management System (ISMS) that is independently certified as compliant with ISO/IEC 27001:2022.

(e) The systematic identification of security threats and the application of a risk assessment procedure that will identify and implement appropriate control measures.

(f) Regular monitoring of security threats and the testing/auditing of the effectiveness of control measures.

(g) The maintenance of a risk treatment plan that is focused on eliminating or reducing security threats.

(h) The clear definition of responsibilities and authorities for implementing the information security management system.

(i) The provision of appropriate information, instruction and training so that all employees are aware of their responsibilities and legal duties and can support the implementation of the ISMS.

(j) The implementation and maintenance of the sub-policies documented within the system.

6 Breaches of this Policy

6.1 Any contravention of this policy or other information security related policies and procedures will be dealt with under the appropriate procedures. This may involve the disciplinary procedure being invoked. Since this policy covers matters ranging from minor issues through to illegal activities, the sanctions for breaches may range from an informal warning to dismissal.