THE POLICY DISPLAYED WAS APPROVED BY THE ERSTWHILE BOARD OF DIRECTORS OF THE COMPANY IN ITS MEETING HELD ON 5TH DECEMBER 2024, THIS POLICY HAS BEEN PUBLISHED ON THE WEBSITE OF THE COMPANY TO COMPLY WITH REGULATION 46 OF THE SEBI (LODR) REGULATIONS, 2015. THE BOARD OF THE COMPANY MAY MODIFY, ADD, DELETE OR AMEND ANY OF THE PROVISIONS OF THIS POLICY TIME TO TIME.

ICODEX PUBLISHING SOLUTIONS LIMITED
IT and Cybersecurity Policy

1. Introduction

ICodex Publishing Solutions Limited ("the Company") recognizes the critical importance of information technology and cybersecurity in safeguarding its data assets, ensuring operational integrity, and protecting stakeholder interests. This IT and Cybersecurity Policy has been developed to establish a secure and resilient IT infrastructure that supports the Company's mission and objectives. This IT and Cybersecurity Policy serves as a foundation for ICodex Publishing Solutions Limited's commitment to protecting its digital assets, data from unauthorized access, and the organization against cyber threats while ensuring compliance with applicable regulatory standards. By fostering a secure environment, the Company aims to maintain the trust of its stakeholders and sustain its long-term operational success.

2. Objective

The primary objective of this policy is to outline the framework for effectively managing IT resources, safeguarding sensitive information, preventing unauthorized access to digital assets, and mitigating cyber risks. This framework is essential to ensure business continuity and protect the integrity of the Company's operations.

3. Scope

This policy applies to all employees, contractors, and third-party partners who have access to the Company's IT systems, networks, and data. It encompasses all digital assets, including IT infrastructure, software applications, data management processes, and cybersecurity protocols. Compliance with this policy is mandatory for all individuals with access to the Company's information systems.

4. IT Security Measures

The Company's approach to IT security is comprehensive and includes the following measures:

4.1 Access Control
Access to IT systems and data will be granted exclusively to authorized personnel based on role-specific requirements and minimum necessary access principles. User access will be regularly reviewed and adjusted as necessary.

4.2 Data Encryption
Sensitive data will be protected by implementing robust encryption protocols during both transmission and storage. This ensures that confidential information remains secure and inaccessible to unauthorized entities.

4.3 Network Security
The Company will establish and maintain firewalls, intrusion detection systems, and intrusion prevention systems to monitor and secure all network traffic. Network segmentation will be employed to further isolate sensitive systems.

4.4 Regular Audits
Regular security audits and vulnerability assessments will be conducted to evaluate the effectiveness of IT security controls, identify potential vulnerabilities, and implement corrective measures promptly.

5. Cybersecurity Practices

To effectively safeguard against cyber threats, the Company is committed to implementing the following practices:

5.1 Malware Protection
The Company will utilize up-to-date antivirus and anti-malware solutions to detect, prevent, and respond to malicious software attacks, ensuring the integrity of its IT systems.

5.2 Employee Training
Regular cybersecurity awareness training sessions will be provided to all employees to empower them to recognize potential cyber threats and respond appropriately, fostering a culture of security.

5.3 Incident Response
An incident response plan will be established to address cybersecurity breaches promptly. This plan will outline the procedures for identifying, containing, and mitigating the impact of cybersecurity incidents, including communication strategies with stakeholders.

6. Data Protection and Privacy

The Company is dedicated to protecting the privacy and security of both personal and business data. This commitment includes compliance with all relevant data protection laws and regulations, restricting access to sensitive data based on necessity, and ensuring that secure data storage and handling practices are in place.

7. Responsibilities

The governance of this policy is under the purview of the Board of Directors, in conjunction with the IT and Security teams, which are responsible for ensuring the effective implementation of the security measures outlined herein. All employees and contractors are expected to comply with established IT and cybersecurity protocols and are required to report any suspicious activities or security incidents immediately.

8. Review of the Policy

This policy shall be reviewed regularly to respond to evolving cybersecurity threats, changes in regulatory requirements, and advancements in technology. Any amendments to this policy must receive approval from the Board of Directors to ensure its ongoing relevance and effectiveness.