VIGILO

Cyber Security Policy

1. Introduction

VIGILO Solutions Ltd. ("the Company") is committed to protecting the confidentiality, integrity, and availability of its information assets. This Cybersecurity Policy provides the framework for managing and safeguarding the Company's digital infrastructure, data, and systems from internal and external cyber threats.

2. Purpose

The purpose of this policy is to:

- Protect company data and information assets from unauthorized access, disclosure, alteration, or destruction.
- Ensure compliance with applicable legal, regulatory, and contractual requirements.
- Promote a culture of cybersecurity awareness within the Company.
- Provide clear guidelines and procedures for managing cybersecurity risks.

3. Scope

This policy applies to:

- All employees, contractors, and third-party vendors who have access to the Company's IT systems, networks, and data.
- All devices (workstations, mobile devices, servers, etc.) connected to the Company's networks.
- All digital systems, applications, and software used by VIGILO Solutions Ltd.

4. Governance and Responsibilities

- Cybersecurity Team: The Cybersecurity Team is responsible for overseeing the implementation and enforcement of this policy, conducting risk assessments, and ensuring that the necessary resources are allocated to maintain a secure environment.
- Management: Senior management is responsible for ensuring that appropriate cybersecurity resources are in place, supporting training programs, and fostering a culture of security awareness.
- Employees and Contractors: All employees, contractors, and third parties are required to adhere to this policy and report any suspected security incidents or vulnerabilities.

5. Information Security Requirements

- Data Protection: All sensitive and confidential data must be classified, protected, and encrypted in accordance with the data protection regulations. Personal data must be handled securely and in compliance with applicable privacy laws.
- Access Control: Access to company systems and data is granted on a need-to-know basis. Role-based access control (RBAC) should be implemented to ensure that users can only access resources relevant to their roles.
- Authentication: Multi-factor authentication (MFA) is mandatory for accessing critical systems, applications, and sensitive data.
- Password Management: All users must adhere to the Company’s password policies, including using strong passwords and updating them regularly.

6. Network Security

- Firewall and Intrusion Detection Systems: Firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) must be implemented to protect the network from unauthorized access and threats.
- Encryption: All sensitive data transmitted over the network must be encrypted using industry-standard encryption protocols.
- Remote Access: Employees accessing company systems remotely must use secure VPN connections or other approved secure methods.

7. Threat Detection and Response

- Incident Reporting: Employees must immediately report any cybersecurity incidents (such as phishing attempts, malware infections, data breaches, or suspicious activities) to the Cybersecurity Team.
- Incident Response Plan: The Company will maintain and regularly update an Incident Response Plan to address potential cybersecurity incidents in a timely and effective manner. This includes identifying the threat, containing the damage, and recovering from the incident.
- Vulnerability Management: Regular vulnerability assessments and penetration tests should be conducted to identify potential weaknesses in the Company's systems and networks.

8. Data Backup and Recovery

- Data Backup: Regular backups of critical business data and systems must be performed and stored in a secure location. Backups should be tested periodically to ensure they are valid and can be restored in case of disaster.
- Disaster Recovery Plan: A disaster recovery plan will be maintained, and recovery procedures will be tested regularly to ensure that business operations can be restored with minimal disruption.

9. Security Awareness and Training

- Employee Training: All employees will undergo cybersecurity training during onboarding and participate in regular refresher courses to raise awareness about potential threats such as phishing, malware, and social engineering.
- Phishing Simulations: Regular phishing simulation exercises will be conducted to evaluate employees' ability to detect and respond to phishing attempts.

10. Vendor Management

- Third-Party Security: All third-party vendors with access to company systems or data must adhere to the Company's cybersecurity requirements. The Company will assess the security posture of third parties through periodic audits and assessments.
- Contracts and Agreements: The Company will establish clear cybersecurity requirements in contracts with vendors, ensuring they meet the necessary security standards.

11. Compliance and Legal Requirements

VIGILO Solutions Ltd. will comply with all relevant cybersecurity regulations, standards, and industry best practices, including but not limited to:

- GDPR (General Data Protection Regulation)
- CCPA (California Consumer Privacy Act)
- NIST Cybersecurity Framework
- ISO 27001

12. Monitoring and Auditing

- Continuous Monitoring: The Company will employ continuous monitoring of systems and networks to detect and mitigate cybersecurity risks.
- Audit and Reporting: Regular audits of cybersecurity practices and controls will be conducted. Audit logs must be maintained to ensure accountability.

13. Enforcement and Disciplinary Actions

- Policy Violations: Any violation of this policy may result in disciplinary actions, up to and including termination of employment or contract, in accordance with the Company's HR policies.
- Reporting Non-Compliance: Any employee who suspects a violation of this policy or has concerns about its enforcement should report it through the designated reporting channels.

14. Policy Review and Updates

This policy will be reviewed at least annually or whenever there are significant changes in the Company's operations or regulatory environment. Updates and revisions to this policy will be communicated to all employees and stakeholders.

Approval

This Cybersecurity Policy has been reviewed and approved by the management of VIGILO Solutions Ltd.

Edward Gilmour

Signed: Edward Gilmour
Name: Edward Gilmour
Title: Managing Director
Date: 12/09/24