Information Security Policy

Policy Objective:

Patrolsec Ltd's Information Security Policy is designed to ensure business continuity and minimize the risk of damage by preventing security incidents and reducing their potential impact. The overarching goal of this policy is to safeguard the organization's informational assets against all types of threats, whether internal, external, deliberate, or accidental, with the direct approval of the Managing Director (MD).

Key Policy Principles:

1. **Access Control:** Information will be protected against unauthorized access.
2. **Confidentiality:** The confidentiality of information will be assured.
3. **Integrity:** The integrity of information will be maintained.
4. **Availability:** Information necessary for business processes will be consistently available.
5. **Compliance:** All legislative and regulatory requirements will be met.
6. **Business Continuity:** Robust business continuity plans will be developed, maintained, and rigorously tested.
7. **Training:** Information security training will be made available to all employees.
8. **Incident Reporting:** Any actual or suspected information security breaches will be reported to the Information Security Manager and thoroughly investigated.

Supporting Measures:

To reinforce this policy, several measures will be implemented, including:

- **Virus Control Measures:** Implementing controls to prevent and address virus threats.
- **Password Security:** Ensuring secure password practices.
- **Continuity Plans:** Developing and maintaining plans to ensure business operations' continuity.

Responsibility and Oversight:

Patrolsec Ltd's top management bears the responsibility for maintaining and actively supporting the implementation of this policy. They will provide guidance and assistance to ensure the policy's effectiveness.

The Managing Director shall review this policy annually or following significant changes.

M. Naeem

Patrolsec Ltd.
Review date: 12/10/23