Information Security Policy

The objective of CAPITAL SHIELD SECURITY LTD information security policy is to ensure business continuity of company and to minimize the risk of damage by preventing security incidents and reducing their potential impact. The policy's goal is to protect the organization's informational assets against all internal, external, deliberate or accidental threats under the MD direct approval.

The security policy ensures that:

- Information will be protected against any unauthorized access;
- Confidentiality of information will be assured;
- Integrity of information will be maintained;
- Availability of information for business processes will be maintained;
- Legislative and regulatory requirements will met;
- Business continuity plans will be developed, maintained and tested;
- Information security training will be available for all employees;
- All actual or suspected information security breaches will be reported to the Information Security Manager and will be thoroughly investigated.

Measures will be taken to support the policy, including virus control measures, passwords and continuity plans.

Business requirements for availability of information and systems will be met. CAPITAL SHIELD SECURITY LTD top management is responsible for maintaining the policy and providing support and advice during its implementation.

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

CAPITAL SHIELD SECURITY LTD

This policy is reviewed on 01/01/2026

CSS-POL-08
Revision-01
Date 01-01-2026