Information Security Policy – SecureNet Ltd

Purpose:
This policy defines SecureNet Ltd's approach to protecting information assets against threats to confidentiality, integrity, and availability.

Scope:
Applies to all employees, contractors, and systems within SecureNet Ltd.

Key Policies:
- Access Control: Use of least privilege, strong password requirements.
- Data Classification: Public, Internal, Confidential.
- Device Security: All company laptops must be encrypted.
- Network Security: Firewalls and VPN required for remote access.
- Incident Reporting: All incidents must be reported within 24 hours to the Information Security Officer.

Responsibilities:
- The Information Security Officer maintains and updates this policy.
- All staff must complete annual cybersecurity training.
- Department heads ensure compliance within their teams.

Review:
This policy will be reviewed annually or after any major incident or system change.