**Risk Assessment Report – SecureNet Ltd**

Objective:  
To identify, assess, and manage potential information security risks within SecureNet Ltd.

Methodology:  
Risks are evaluated based on impact and likelihood, using qualitative analysis (High, Medium, Low).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Threat | Asset | Impact | Likelihood | Risk Level | Mitigation |
| Phishing attack | Employee email | High | Medium | High | Security awareness training, email filters |
| Data breach | Customer data | High | Low | Medium | Access control, encryption, regular audits |
| System downtime | Web servers | Medium | Medium | Medium | Regular patching, backup plan |

Summary:

Based on this assessment, SecureNet’s key risks relate to phishing and data protection. Mitigation controls are implemented through access policies and staff awareness training