Pinnacle Assurance Group – Scope, Information Security Policy, Security Objectives, and Roles/Key Duties

Scope
The Information Security Management System (ISMS) applies to all Pinnacle Assurance Group assets, processes, and people across situated in the physical location to safeguard client health data, support strategic growth, and meet all legal, and regulatory obligations.

Assets
Customer data, corporate network, endpoints, mobile devices, paper records, people, and software.

Exclusions
Personal devices for non-business activities,

Locations
Physical location – 12 Newark Street, Auckland, New Zealand, 0600.

Information Security Policy
Pinnacle Assurance Group will identify, assess, and treat information security. Controls selected in the Statement of Applicability (SoA) will be implemented, measured, and reviewed for continuous improvement. All employees and contractors, will be liable for this policy with written approval from the CISO.

Security Objectives
- Protect policy-holder medical and financial data from unauthorized access, alteration and destruction.
- Maintain continuous compliance with ISO 27001.
- Maintain > 95 % patching rate for both workstations and servers.
- Ensure that employees do atleast one week of security awareness training per month.
- Perform annual restore tests, and ensure documentation is updated accordingly.

Roles and Key Duties
GM – Provide resources, enforce disciplinary measures for non-compliance.
CISO – Own the ISMS, own the Information Security Committee, approve policies & exceptions.
Department Team Leads – Ensure team compliance, remediate audit findings.
All People – Follow policies, report incidents, complete mandatory training.
Third-Party Contractors – Agree to security requirements; undergo regular assessments by the SOC and NOC team.