ALTNETIX LLC
VitaAI Platform

RISK MANAGEMENT POLICY

Enterprise Risk Identification, Assessment, and Treatment

Control Reference	BIZOPS-1
Document Version	1.0
Effective Date	June 1, 2026
Next Review	June 1, 2027
Classification	Confidential – Internal & Customer Use
Maintained by	Altnetix LLC Security & Compliance Team
Contact	compliance@altnetix.com

1. Purpose and Scope

This Risk Management Policy establishes the framework for identifying, assessing, treating, and monitoring risks to the confidentiality, integrity, and availability of information systems and PHI at Altnetix LLC. It satisfies the HIPAA Security Rule requirement for a risk analysis (45 CFR §164.308(a)(1)(ii)(A)) and risk management program (§164.308(a)(1)(ii)(B)).

2. Risk Management Framework

The Company's risk management program is aligned with the NIST Risk Management Framework (NIST SP 800-37) and incorporates elements of the NIST Cybersecurity Framework (CSF). The program covers: Identify !’ Protect !’ Detect !’ Respond !’ Recover.

3. Risk Assessment Process

Step 1: Asset Inventory

All information assets that create, receive, maintain, or transmit PHI or sensitive data are inventoried annually, including systems, applications, cloud services, and workforce access points.

Step 2: Threat and Vulnerability Identification

Threats and vulnerabilities are identified through: automated vulnerability scanning, annual penetration testing, review of NIST NVD and HHS advisories, and incident analysis.

Step 3: Risk Scoring

Risks are scored using the formula: Risk Score = Likelihood (1-5) × Impact (1-5). Scores are mapped to: Low (1-5), Moderate (6-12), High (13-19), Critical (20-25).

Step 4: Risk Treatment Selection

- Accept — Low-risk items where controls cost exceeds potential impact
- Mitigate — Implement technical or administrative controls to reduce risk
- Transfer — Obtain cyber insurance or contractual risk transfer
- Avoid — Discontinue activity that creates unacceptable risk

4. Risk Monitoring and Review

The Risk Register is reviewed quarterly by the Security Officer. A comprehensive annual risk assessment is performed each calendar year and documented. Risk assessment findings drive the Company's security control roadmap and investment priorities.

5. Roles and Responsibilities

- Security Officer — owns the risk program, conducts assessments, maintains Risk Register
- CEO — approves risk acceptance decisions and resource allocation for mitigation
- Engineering — implements technical controls and remediates identified vulnerabilities
- All Workforce — report newly identified risks or security concerns to the Security Officer