ALTNETIX LLC
VitaAI Platform

SDLC SECURITY REVIEW PROCESS

Secure Software Development Lifecycle Standards

Control Reference	PDP-11
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 Overview

This document defines security review requirements at each phase of the VitaAI software development lifecycle (SDLC). Security is integrated from requirements through deployment — not added as a post-hoc review. The program is aligned with OWASP SAMM and NIST SP 800-64.

2. Security Requirements Phase

- All new features involving PHI storage, transmission, or display require explicit security requirements
- Authentication, authorization, and audit logging requirements are specified before design
- Regulatory requirements (HIPAA §164.312) are mapped to technical controls
- Threat modeling is performed for significant new features using STRIDE methodology

3. Design Review

- Architecture diagrams reviewed for attack surface minimization
- Data flow diagrams identify all PHI processing points
- Authentication and authorization designs verified against NIST 800-63B
- Cryptographic designs reviewed against Company encryption standards (this document)
- Infrastructure changes reviewed against CIS Azure Benchmark

4. Secure Coding Standards

All developers are required to follow OWASP Secure Coding Practices. Mandatory controls include:

- Input validation on all user-supplied data before processing
- Parameterized queries for all database operations (no string concatenation)
- HTTPS-only API communication; no HTTP endpoints in production
- No hardcoded credentials, API keys, or secrets in source code
- Dependencies scanned for CVEs before inclusion; high-severity CVEs block merge

5. Code Review Security Checklist

- Authentication: tokens validated, sessions expire, MFA enforced
- Authorization: all endpoints verify user permission before data access
- PHI: minimum necessary access, no unnecessary PHI in logs or error messages
- Crypto: approved algorithms only; no MD5, SHA-1, DES, RC4
- Error handling: no stack traces or internal details exposed to clients
- Secrets: no credentials in code; Key Vault references used
- Logging: audit events logged for all PHI access, modifications, and authentications

6. Pre-Release Security Testing

- Automated dependency scanning (Dependabot) on every pull request
- Static Application Security Testing (SAST) via GitHub Advanced Security
- OWASP ZAP scan on staging environment before each major release
- Annual third-party penetration test covering production API and infrastructure
- Penetration test findings remediated within SLA: Critical 7d, High 30d, Medium 90d

7. Security Training

All engineers complete OWASP Top 10 and secure coding training annually. New engineers complete security onboarding within 30 days of hire. Security briefings are provided following significant vulnerability disclosures or industry incidents relevant to the Company's technology stack.