Security Controls Overview

PHOCIS Tech maintains a robust set of technical and organizational security controls aligned with NIST CSF and SOC 2 Type II preparation. This document summarizes our current control environment and active security investments.

Access Control

- Role-based access control (RBAC) with least-privilege enforcement across all systems
- Multi-factor authentication (MFA) required for all administrative and cloud access
- Single sign-on (SSO) enforced via Google Workspace for internal applications
- Privileged access workstations (PAW) and just-in-time (JIT) access for production systems
- Quarterly access reviews with automatic de-provisioning on separation

Data Protection

- AES-256 encryption at rest for all borrower PII, loan data, and financial records
- TLS 1.3 in transit for all API communications and user-facing interfaces
- Database-level field encryption for SSNs, account numbers, and authentication tokens
- Automated key rotation every 90 days via AWS KMS / GCP Cloud KMS
- Data classification policy: Public / Internal / Confidential / Restricted

Network Security

- Zero-trust network architecture — no implicit trust based on network location
- Web Application Firewall (WAF) protecting all public endpoints
- Intrusion detection and prevention systems (IDS/IPS) with 24/7 alerting
- DDoS mitigation via Cloudflare Enterprise with automatic failover
- VPN-isolated development, staging, and production environments

Vulnerability Management

- Continuous vulnerability scanning via Tenable.io across all infrastructure
- SAST/DAST integrated into CI/CD pipeline — no critical-severity deployments permitted
- Penetration testing conducted annually by qualified third-party firm
- CVE patching SLAs: Critical ≤ 24 hrs, High ≤ 7 days, Medium ≤ 30 days
- Bug bounty program in scoping phase for Q3 2025 launch

Monitoring & Logging

- Centralized SIEM (Splunk / AWS Security Hub) with 12-month log retention
- Real-time alerting on anomalous access patterns, failed authentications, and data exfiltration indicators
- Immutable audit logs for all privileged actions and data access events

- API rate limiting and abuse detection across all integration endpoints

Current Control Maturity

Domain	Maturity Level	Status
Identity & Access Management	Managed	Active
Data Encryption	Defined	Active
Endpoint Security	Defined	Active
Network Controls	Managed	Active
Vulnerability Management	Repeatable	Active
Incident Response	Defined	In Progress
SOC 2 Type II Audit	Initiating	Q4 2025 Target