Information Security Policy Summary

PHOCIS Tech maintains a comprehensive information security policy framework governing all aspects of data handling, system access, and security operations. This summary provides an overview of our core policy documents, their scope, and review cadences.

Policy Framework Overview

Policy Document	Scope	Review Cycle
Information Security Policy	All systems, personnel, contractors	Annual
Acceptable Use Policy (AUP)	All employees, devices, and networks	Annual
Data Classification Policy	All data assets and repositories	Annual
Access Management Policy	All user, service, and admin accounts	Semi-Annual
Password & Authentication Policy	All authentication systems	Annual
Vendor & Third-Party Risk Policy	All external integrations and SaaS	Annual
Incident Response Policy	All security events and breaches	Bi-Annual
Business Continuity Policy	Critical systems and processes	Annual
Data Retention & Disposal Policy	All data stores and backups	Annual

Key Policy Highlights

- All employees complete mandatory security awareness training at onboarding and annually thereafter
- Background checks required for all hires with access to production systems or borrower data
- Contractor access governed by NDA, scoped credentials, and time-limited permissions
- Any security exception requires CISO approval and compensating control documentation
- Policy violations subject to disciplinary action up to and including termination

Third-Party Risk Management

- All vendors handling borrower or financial data undergo annual security review
- SOC 2 Type II reports, ISO 27001 certifications, or equivalent required for Tier 1 vendors
- Data processing agreements (DPAs) executed with all PII-handling third parties
- Vendor access monitored and revoked immediately upon contract termination

Compliance Attestation

PHOCIS Tech's security policies are reviewed by legal counsel and align with GLBA Safeguards Rule, FCRA, RESPA, and applicable state data protection statutes. Annual policy acknowledgment is required from all team members and tracked in our HR compliance system.