SECURITY POLICY SNAPSHOT

Information Security Program Overview

Aftershock Cyber Solutions

Version 2.1 | Effective Date: January 1, 2025

> **Document Purpose:** This snapshot provides an overview of Aftershock Cyber Solutions' information security policies and procedures. Full policy documentation is available to authorized personnel through our internal policy management system.

Compliance Framework Alignment

SOC 2 Type II **ISO 27001** **PCI DSS v4.0.1** **NIST CSF** **GDPR** **CCPA**

Our information security program is designed to meet or exceed industry standards and regulatory requirements. We maintain active compliance with multiple frameworks including PCI DSS v4.0.1 for payment card data security. We undergo regular third-party audits to validate our controls.

Policy Overview

1. Information Security Policy (ISP-001)

Last Updated: January 1, 2025 | **Review Cycle:** Annual

Establishes the foundation for our information security program, defining roles, responsibilities, and governance structure. All employees must acknowledge and comply with this policy annually.

Key Requirements:

- Annual security awareness training (100% completion required)
- Background checks for all employees with access to sensitive data
- Acceptable use of company resources
- Incident reporting obligations

2. Access Control Policy (ACP-002)

Last Updated: March 15, 2025 | **Review Cycle:** Semi-Annual

Defines how access to systems, applications, and data is granted, reviewed, and revoked. Implements principle of least privilege and separation of duties.

Key Controls:

- Multi-factor authentication (MFA) required for all accounts
- Role-based access control (RBAC) implementation
- Quarterly access reviews by data owners
- Automated deprovisioning within 24 hours of termination
- Privileged access management (PAM) for administrative accounts

3. Data Classification and Handling (DCH-003)

Last Updated: February 1, 2025 | **Review Cycle:** Annual

Establishes data classification levels and handling requirements to ensure appropriate protection based on sensitivity and business impact.

Classification	Description	Examples
Public	Information intended for public disclosure	Marketing materials, public documentation
Internal	Information for internal use only	Internal procedures, employee directory

Confidential	Sensitive business information	Financial data, customer information
Restricted	Highly sensitive, regulated data	PII, PHI, payment card data, credentials

4. Incident Response Policy (IRP-004)

Last Updated: April 1, 2025 | **Review Cycle:** Annual

Defines procedures for detecting, responding to, and recovering from security incidents. Includes escalation procedures and communication protocols.

Response Timeframes:

- Critical incidents: Initial response within 1 hour
- High severity: Initial response within 4 hours
- Medium severity: Initial response within 24 hours
- Low severity: Initial response within 72 hours

5. Change Management Policy (CMP-005)

Last Updated: January 15, 2025 | **Review Cycle:** Annual

Ensures all changes to production systems follow a controlled process with appropriate review, testing, and approval before implementation.

Key Requirements:

- Change requests documented in ticketing system
- Security review for all infrastructure changes
- Testing in non-production environment required
- Rollback plan documented before deployment
- Post-implementation review within 48 hours

6. Vulnerability Management Policy (VMP-006)

Last Updated: March 1, 2025 | **Review Cycle:** Annual

Establishes requirements for identifying, assessing, and remediating security vulnerabilities across our infrastructure and applications.

Remediation SLAs:

- Critical vulnerabilities: 7 days
- High vulnerabilities: 30 days
- Medium vulnerabilities: 90 days
- Low vulnerabilities: 180 days or next maintenance window

7. Backup and Recovery Policy (BRP-007)

Last Updated: February 15, 2025 | **Review Cycle:** Annual

Defines backup procedures, retention requirements, and recovery objectives to ensure business continuity.

Key Metrics:

- Recovery Time Objective (RTO): 4 hours for critical systems
- Recovery Point Objective (RPO): 1 hour for critical data
- Backup frequency: Daily incremental, weekly full
- Backup testing: Quarterly restoration tests

8. Payment Card Data Security Policy (PCI-008)

Last Updated: March 1, 2025 | **Review Cycle:** Annual

Establishes requirements for protecting payment card data in accordance with PCI DSS v4.0.1 standards. Applies to all systems that store, process, or transmit cardholder data.

Key Requirements:

- Cardholder data environment (CDE) network segmentation

- Encryption of cardholder data at rest and in transit (AES-256, TLS 1.2+)
- No storage of sensitive authentication data post-authorization
- Quarterly vulnerability scans by Approved Scanning Vendor (ASV)
- Annual penetration testing of CDE
- Multi-factor authentication for all CDE access
- Logging and monitoring of all access to cardholder data
- Annual PCI DSS compliance validation (SAQ or ROC)

PCI DSS v4.0.1 Compliance Status:

- Last Assessment: September 2025
- Attestation of Compliance (AOC): Valid through September 2026
- Next Assessment: September 2026
- Compliance Level: Service Provider Level 2

Security Controls Summary

Control Category	Implementation Status	Last Audit
Identity & Access Management	✅ Fully Implemented	September 2025
Network Security	✅ Fully Implemented	September 2025
Data Encryption	✅ Fully Implemented	September 2025
Logging & Monitoring	✅ Fully Implemented	September 2025
Vulnerability Management	✅ Fully Implemented	October 2025
Incident Response	✅ Fully Implemented	August 2025
Business Continuity	✅ Fully Implemented	September 2025
Security Awareness Training	✅ Fully Implemented	October 2025

PCI DSS Compliance Controls	✅ Fully Implemented	September 2025

Governance & Oversight

Security Steering Committee: Meets quarterly to review security posture, approve policy changes, and allocate resources for security initiatives.

Policy Review Schedule: All policies undergo formal review at least annually, with updates as needed based on regulatory changes, incidents, or business requirements.

Compliance Audits: Third-party audits conducted annually for SOC 2 Type II and ISO 27001 certification maintenance.

Training & Awareness

- Annual security awareness training required for all employees (100% completion in 2025)
- Quarterly phishing simulation exercises
- Role-specific security training for developers, IT staff, and management
- Monthly security newsletters and updates
- Incident response tabletop exercises conducted semi-annually

---

Document Classification: Internal Use - Public Trust Center Display

Policy Owner: Chief Information Security Officer (CISO)

Next Review Date: January 1, 2026