



Technical Vulnerability Management Policy

Control Page

ATTRIBUTE	DETAIL
Document Title	Technical Vulnerability Management Policy
Document ID	OG-SEC-008
Version	1.1
Effective Date	November 2, 2025
Next Review Date	November 2, 2026 (Annual)
Policy Owner	Chief Security & Compliance Officer (CSCO)
Approved By	Chief Executive Officer (CEO)
Classification	Confidential – Internal Use Only



Applicability	All systems, software, networks, cloud environments, and third-party integrations that process, store, or transmit cardholder data (CHD) or support Orchestrate Global's payment orchestration platform
Regulatory Alignment	PCI DSS v4.0.1 (Req 6.3, 11.2, 11.3), NIST SP 800-40 Rev. 4, ISO/IEC 27001:2022
Distribution List	Engineering, DevOps, IT, Security, Compliance, Product, Legal, C-Suite

Approvals

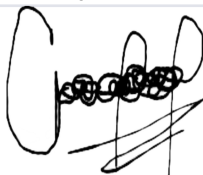
NAME	POSITION	SIGNATURE	DATE
Oleksii Bondarenko	Chief Security & Compliance Officer		1 November 2025
Charles Odhiambo	Technical Lead		1 November 2025
Kevin Kegera	Chief Commercial Officer		1 November 2025
Preston Obadan	Chief Executive Officer		1 November 2025

Table of Contents

1. Purpose
2. Scope
3. Definitions
4. Policy Statement
5. Roles and Responsibilities
6. Vulnerability Identification
7. Vulnerability Assessment & Prioritization
8. Remediation & Mitigation
9. Verification & Closure



- 10. Exception Management
- 11. Monitoring & Reporting
- 12. Training & Awareness
- 13. Policy Compliance
- 14. Review & Maintenance
- 15. Appendices

1. Purpose

This policy establishes a structured, risk-based approach to the proactive identification, assessment, prioritization, remediation, and reporting of technical vulnerabilities across Orchestrate Global's information systems, applications, networks, and supporting infrastructure. The objective is to reduce the organization's attack surface, protect cardholder data environments (CDE), and maintain compliance with applicable regulatory and industry standards.

2. Scope

This policy applies to all:

- On-premises and cloud-hosted systems
- Operating systems, databases, middleware, and runtime environments
- Custom-developed and third-party software (including open-source components)
- Network devices, security appliances, and virtualized infrastructure
- Containers, serverless functions, and orchestration platforms
- Employees, contractors, vendors, and third parties managing or accessing Orchestrate Global systems

Exclusions must be formally documented and approved through the Exception Management process (Section 10).

3. Definitions

- **Vulnerability:** A weakness in an information system, system security procedure, internal control, or implementation that could be exploited by a threat source.



- **Exploit:** A piece of software, data, or sequence of commands that takes advantage of a vulnerability.
- **CVSS (Common Vulnerability Scoring System):** An open framework for communicating the characteristics and severity of software vulnerabilities (v3.1 or later).
- **SLA (Service Level Agreement):** Defined timeframes for remediation based on vulnerability severity.
- **False Positive:** A reported vulnerability that does not exist or cannot be exploited in the target environment.
- **Compensating Control:** A security measure that reduces risk when primary remediation is not immediately feasible.

4. Policy Statement

Orchestrate Global shall:

- Proactively scan for and monitor technical vulnerabilities across its entire technology estate.
- Prioritize vulnerabilities based on risk, considering exploitability, asset criticality, and business impact.
- Remediate or mitigate all identified vulnerabilities within defined SLAs.
- Maintain an auditable record of vulnerability lifecycle activities.
- Ensure all vulnerability management activities align with PCI DSS Requirement 6 and other relevant standards.

Failure to comply with this policy may result in disciplinary action, including termination, and increased organizational risk exposure.

5. Roles and Responsibilities

ROLE	RESPONSIBILITIES
Chief Security & Compliance Officer	Overall policy ownership, strategic oversight, and compliance assurance.
IT & DevOps Teams	Execute scans, apply patches, implement mitigations, and validate fixes.



Security Operations Center (SOC)	Monitor threat intelligence feeds, correlate alerts, and escalate critical findings.
Engineering & Development Teams	Remediate vulnerabilities in custom code; integrate SCA/SAST/DAST into CI/CD pipelines.
Third-Party Vendors	Report and remediate vulnerabilities in their delivered products/services per contract.
All Personnel	Report suspected vulnerabilities and adhere to secure configuration standards.

6. Vulnerability Identification

Vulnerabilities shall be identified through:

- Automated Scanning: Weekly authenticated scans of internal systems; monthly external scans by PCI-Approved Scanning Vendors (ASVs).
- Threat Intelligence: Subscription to CVE, NVD, vendor advisories, and ISAC feeds.
- Code Analysis: Integration of SCA (Software Composition Analysis), SAST (Static Application Security Testing), and DAST (Dynamic Application Security Testing) tools in SDLC.
- Bug Bounty & Responsible Disclosure: Managed program for external researchers (if implemented).
- Manual Assessments: Periodic penetration tests by qualified internal or external parties.

All scanning tools must be maintained, calibrated, and validated to minimize false positives/negatives.

7. Vulnerability Assessment & Prioritization

- All vulnerabilities shall be scored using CVSS v3.1 or later.



- Risk rating = CVSS Base Score + Asset Criticality + Threat Context.
- Severity Tiers & SLAs:

SEVERITY	CVSS RANGE	REMEDiation SLA	EXAMPLES
Critical	9.0–10.0	7 calendar days	RCE, SQLi in CDE, unauthenticated access to admin interfaces
High	7.0–8.9	15 calendar days	Privilege escalation, XSS in authenticated apps
Medium	4.0–6.9	30 calendar days	Information disclosure, weak crypto
Low	0.1–3.9	90 calendar days or next maintenance window	Verbose error messages, missing HTTP security headers

Asset criticality is defined by data sensitivity (e.g., cardholder data), system function (e.g., CDE boundary), and availability requirements.

8. Remediation & Mitigation

- Remediation: Permanent fix (e.g., patch, code change, configuration update).
- Mitigation: Temporary control (e.g., WAF rule, network segmentation, access restriction) if remediation is delayed.
- All actions must be documented in the centralized vulnerability management platform.
- Compensating controls require formal risk acceptance (Section 10).

9. Verification & Closure

- Remediation must be verified via:
 - Rescanning
 - Manual validation by SOC or QA
 - Evidence of code commit or configuration change
- Only verified fixes may be marked “Closed” in the tracking system.



- Unverified or failed remediations re-enter the workflow with escalated priority.

10. Exception Management

- Exceptions require:
 - Business justification
 - Risk assessment
 - Compensating controls
 - Approval by CSO and CCO
- Maximum exception duration: 180 days (renewable only with C-level approval).
- All exceptions logged in the GRC system and reviewed quarterly.

11. Monitoring & Reporting

- Real-time dashboards for vulnerability status by system, team, and severity.
- Monthly reports to CSO, CCO, and IT leadership including:
 - Open vulnerabilities by severity
 - SLA compliance rate
 - Top vulnerable assets
 - Trend analysis
- Annual attestation of policy effectiveness for PCI DSS and ISO 27001 audits.

12. Training & Awareness

- Annual training for IT, DevOps, and Engineering staff on:
 - Secure coding practices
 - Vulnerability scanning tools
 - Patch deployment procedures
- New hires complete training within 30 days of onboarding.

13. Policy Compliance

- Non-compliance may result in:
 - Access revocation
 - Project delays
 - Disciplinary action per HR policy
- Audit logs of vulnerability activities retained for minimum 1 year (3 years for PCI DSS).



14. Review & Maintenance

- Reviewed annually or after:
 - Major security incident
 - Significant infrastructure change
 - New regulatory requirement
- Updates approved by CSO and CEO.

15. Appendices

- Appendix A: Approved Scanning Tools List
- Appendix B: CVSS Scoring Guide
- Appendix C: Vulnerability Ticket Template
- Appendix D: Exception Request Form

This document is the property of Orchestrate Global. Unauthorized distribution is prohibited.