



Operating Procedure

Version: 2.0

Effective Date: 1 November 2025

Next Scheduled Review: 1 November 2026

Document Owner: Chief Security & Compliance Officer (CSCO)

Distribution: All Employees, Contractors, and Third Parties with access to systems impacting the Cardholder Data Environment (CDE)

Document Review

Name	Title
All Employees	Staff with system access responsibilities
Contractors	Infrastructure or security-related tasks
Third-Party Vendors	Configurations or shared CDE responsibility

Approval

Name	Position	Signature	Date
Oleksii Bondarenko	Chief Security & Compliance Officer		1 November 2025
Kevin Kegera	Chief Commercial Officer		1 November 2025



Preston Obadan

Chief Executive Officer

1 November 2025

Revision History

Version	Date	Change Number	Summary of Changes
1.0	24 October 2025	001	Initial draft aligned to PCI DSS 4.0
2.0	1 November 2025	002	Full restructuring, expanded scope, asset table integration

Table of Contents

1. Introduction
2. Risks Addressed
3. Asset Inventory and Control Scope
4. Operating Procedure
 - 4.1 Access Control
 - 4.2 Data Encryption
 - 4.3 Security Awareness and Training
 - 4.4 Incident Response
 - 4.5 Vulnerability and Patch Management
 - 4.6 Network Security
 - 4.7 Physical Security
 - 4.8 Secure Disposal
5. Scope of Procedure
6. Prerequisites
7. Timing and Scheduling
8. Step-by-Step Instructions



9. Output and Media Handling
10. Backup and Recovery
11. Error Handling
12. Support and Escalation
13. Auditing and Logging
14. Monitoring
15. End of Procedure

1. Introduction

This Operating Procedure defines the formal processes, roles, and controls implemented by Orchestrate Global Inc. to achieve and maintain compliance with PCI DSS v4.0. These procedures ensure the secure handling, transmission, processing, and storage of Cardholder Data (CHD) and Sensitive Authentication Data (SAD). All employees, contractors, and authorized service providers interacting with payment systems are required to follow this document.

2. Risks Addressed

This document defines controls addressing the following risks from the Information Security Risk Treatment Plan:

Reference	Risk Description
PCI-001	Unauthorized logical or physical access to cardholder data
PCI-002	Leakage or exposure of cardholder data during transmission
PCI-003	System compromise due to unpatched software vulnerabilities



3. Asset Inventory and Control Scope

In accordance with PCI DSS Requirement 2.4, Orchestrate Global maintains a comprehensive asset inventory for all systems within or connected to the CDE. This inventory is maintained within the SmartComply platform and reviewed quarterly.

Asset Inventory Table

Asset ID	Asset Name	Type	Environment	Owner	Role in CDE	Criticality	PCI Mapping
A-001	Payment Gateway API	Microservice	AWS Production	Charles Odhiambo	Processes card transactions and tokens	High	1, 2, 6, 10
A-002	CHD PostgreSQL Database	Database Server	AWS Production	Charles Odhiambo	Stores encrypted PAN data	High	3, 4, 7
A-003	Web Application Firewall	Network Security	Cloud/Edge	IT Security Team	Filters traffic, prevents OWASP Top 10	High	1, 6, 11
A-004	Bastion Host	Secure Access Server	AWS	IT Infrastructure Team	Controlled administrative access to CDE	High	7, 8



A-005	Centralized Logging Server	SIEM	On-Premise	IT Security Team	Aggregates logs for monitoring and forensics	Medium	10, 12
A-006	Finance Department Laptops	Endpoint Devices	Hybrid	Finance Lead	Access financial dashboards and reports	Medium	2, 8
A-007	Encrypted Backup Vault	Object Storage	AWS S3/Glacier	DevOps Team	Retains encrypted backups of CHD databases	High	3, 9
A-008	Vendor API Portal	Web Application	Azure	Kevin Kegera	Transmits card tokenized data to partners	Medium	4, 12

Control Scope applies to all listed assets and any system with logical or physical connectivity to the CDE.

4. Operating Procedure

4.1 Access Control

User Account Management

- All user accounts require written approval by the Chief Security & Compliance Officer (CSCO).
- Access follows least privilege and role-based access control (RBAC) principles.
- User access is reviewed quarterly; inactive accounts are disabled after 90 days.

Access Restrictions



- Multi-factor authentication (MFA) is mandatory for access to CDE resources.
- VPN and firewall segmentation must restrict network access to authorized personnel only.

Authentication

- Passwords must be at least 12 characters with upper/lowercase, numeric, and special characters.
- Password rotation every 90 days.
- Five failed login attempts trigger lockout.

4.2 Data Encryption

Encryption in Transit

- All externally transmitted CHD must use TLS 1.2 or higher.
- Certificates are monitored and renewed at least annually.

Encryption at Rest

- CHD must be encrypted using AES-256 or stronger.
- Encryption keys stored in AWS KMS and rotated annually or upon compromise.

Key Management

- Keys accessible only to authorized personnel.
- All key lifecycle events logged and reviewed quarterly.

4.3 Security Awareness and Training

- Mandatory PCI DSS training at onboarding and every 6 months.
- Developers and IT staff undergo secure coding and CHD handling training.
- Training completion monitored by Compliance.

4.4 Incident Response

- All security events reported to incident@orchestrate.global.
- Incident Response Team consists of CSCO, CTO, and IT Lead.
- Incidents logged; Root Cause Analysis completed within 5 business days.

4.5 Vulnerability and Patch Management



- Internal and external vulnerability scans conducted quarterly and post-changes.
- Critical vulnerabilities remediated within 30 days; medium within 90 days.
- Annual penetration tests conducted.

4.6 Network Security

- CDE segmented from corporate networks.
- Firewalls deny all traffic by default; only approved ports enabled.
- Firewall rules reviewed quarterly.
- Logs retained securely for 12 months minimum.

4.7 Physical Security

- Data center access controlled using biometric and keycard entry.
- Visitor logs maintained; escorts required at all times.
- CCTV recordings retained for a minimum of 90 days.

4.8 Secure Disposal

- CHD on physical media destroyed using shredding or degaussing.
- Certificates of destruction retained for 2 years.
- E-waste processed by approved, certified vendors.

5. Scope of Procedure

This procedure applies during:

- New employee onboarding
- Scheduled compliance reviews
- Incident investigations
- Security audits
- System deployments or upgrades involving CDE

6. Prerequisites

Knowledge

Personnel must understand PCI DSS v4.0, encryption standards, access control policies, and incident escalation processes.

Access



- Administrator or privileged access to staging/production CDE.
- Secure VPN with MFA.
- Physical access authorization (if required).

Materials

- Encrypted company laptop
- MFA token device
- Access to Change Management System, SIEM, vulnerability scanner

7. Timing and Scheduling

- Performed outside business hours if changes impact live services.
- Quarterly during audits and access reviews.
- Immediately after critical infrastructure or application changes.

8. Instructions

- Validate access controls and MFA enforcement.
- Check TLS encryption and certificate validity.
- Review firewall and segmentation policies.
- Conduct vulnerability scans.
- Document findings and remediation steps.

9. Output and Media Handling

- All reports stored under "Compliance/PCI_Reports".
- Printed materials shredded immediately.
- Electronic media encrypted at rest.

10. Backup and Recovery

- Daily backups using AES-256 encryption.
- Offsite backups in AWS Glacier.
- Quarterly restoration tests conducted.

11. Error Handling



Error Type	Cause	Corrective Action
Authentication Failure	Incorrect credentials	Reset via MFA and compliance validation
Key Expiration	Expired key	Rotate key and re-encrypt affected data
TLS Misconfiguration	Weak cipher detected	Update TLS config and re-scan
PAN Exposure	Logging misconfig	Stop logging, sanitize logs, file incident

12. Support and Escalation

Name	Role	Email	Availability
Oleksii Bondarenko	CSCO	compliance@orchestrate.global	9am–5pm weekdays
Charles Odhiambo	Technical Lead	charlie@orchestrate.global	9am–5pm weekdays
Preston Obadan	CEO	preston@orchestrate.global	9am–5pm daily
Kevin Kegera	Chief Commercial Officer	kevin@orchestrate.global	9am–5pm daily



13. Auditing and Logging

- Logs retained for a minimum of 12 months.
- Quarterly audit trail reviews conducted by CSCO.
- Non-compliance incidents documented and resolved within 30 days.

14. Monitoring

- SIEM continuously monitors system logs and alerts.
- Anomalies escalated to Incident Response Team.
- Monthly security metrics reported to executives.