



Access Control Policy

Control Page

ATTRIBUTE	DETAIL
Document Title	Access Control Policy
Document ID	OG-ACP-001
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	Applies to all employees, contractors, third-party vendors, and service providers who access Orchestrate Global's systems, networks, physical facilities, or cardholder data



	environments. It covers all technologies, applications, infrastructure, and physical locations that store, process, transmit, or secure sensitive or confidential information. Compliance with this policy is mandatory for all internal and external personnel granted access to company resources.
Compliance Frameworks	PCI DSS v4.0
Distribution List	All Employees, Board of Directors, Audit Committee, Key Merchant Partners, Compliance Team

Approvals

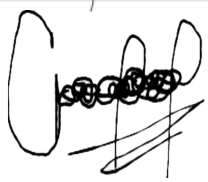
NAME	POSITION	SIGNATURE	DATE
Oleksii Bondarenko	Chief Security & Compliance Officer		1 November 2025
Charles Odhiambo	Technical Lead		1 November 2025
Kevin Kegera	Chief Commercial Officer		1 November 2025
Preston Obadan	Chief Executive Officer		1 November 2025

Table of Contents

1. Purpose and Scope
 - 1.1 Purpose
 - 1.2 Scope
2. Regulatory Compliance
 - 2.1 PCI DSS Requirements
 - 2.2 Additional Standards
3. Access Control Principles
 - 3.1 Least Privilege
 - 3.2 Need-to-Know Basis



- 3.3 Segregation of Duties
 - 3.4 Defense in Depth
- 4. User Classification and Roles
 - 4.1 Internal User Roles
 - 4.2 External User Roles
- 5. Access Provisioning and Deprovisioning Process
 - 5.1 New User Access Request
 - 5.2 Access Modification Process
 - 5.3 Access Removal Process
- 6. Physical Access Control Policy
- 7. Authentication Requirements
 - 7.1 Internal Users
 - 7.2 External Users
- 8. Authorization Controls
 - 8.1 Role-Based Access Control (RBAC)
 - 8.2 Attribute-Based Access Control (ABAC)
 - 8.3 Data Classification Access Rules
- 9. System-Specific Access Controls
 - 9.1 Cardholder Data Environment (CDE)
 - 9.2 Payment APIs
 - 9.3 Administrative Systems
- 10. Access Monitoring and Auditing
 - 10.1 Access Logging Requirements
 - 10.2 Real-Time Monitoring
 - 10.3 Access Reviews and Audits
- 11. Special Access Scenarios
 - 11.1 Emergency Access Procedures
 - 11.2 Third-Party Access
 - 11.3 Remote Access Controls
- 12. Access Control Violations
 - 12.1 Violation Categories
 - 12.2 Incident Response
- 13. Training and Awareness
 - 13.1 Security Awareness Training
 - 13.2 Ongoing Awareness
- 14. Technology Controls
 - 14.1 Identity and Access Management (IAM)
 - 14.2 Privileged Access Management (PAM)
 - 14.3 Application Security Controls
- 15. Compliance Monitoring
 - 15.1 Key Performance Indicators (KPIs)
 - 15.2 Reporting Requirements
- 16. Policy Maintenance
 - 16.1 Policy Review and Updates
 - 16.2 Related Documentation
- 17. Definitions and Acronyms



1. Purpose and Scope

1.1 Purpose

This Access Control Policy establishes requirements for managing user access to Orchestrate Global's payment orchestration platform, ensuring compliance with PCI DSS Requirement 7 and protecting cardholder data through implementation of least privilege principles and role-based access controls.

1.2 Scope

This policy applies to all access to systems, applications, and data within Orchestrate Global's environment, including:

Internal Users:

- Employees (full-time, part-time, contractors)
- System administrators and developers
- Support and operations staff
- Management and executives

External Users:

- Merchant customers using payment APIs
- Partner organizations (banks, processors, vendors)
- Third-party service providers
- Auditors and compliance assessors

Systems Covered:

- Cardholder Data Environment (CDE) systems
- Payment processing infrastructure
- API gateways and merchant portals
- Administrative and monitoring systems
- Development and testing environments

2. Regulatory Compliance



2.1 PCI DSS Requirements

This policy addresses PCI DSS v4.0.1 requirements:

- Requirement 7.1: Limit access to cardholder data by business need-to-know
- Requirement 7.2: Access control systems assign access based on job classification
- Requirement 7.3: Default "deny-all" setting implemented

2.2 Additional Standards

- SOX compliance for financial controls
- GDPR for data privacy requirements
- ISO 27001 access management principles
- FFIEC guidelines for financial institutions

3. Access Control Principles

3.1 Least Privilege

- Users granted minimum access required for job functions
- Default deny-all policy with explicit allow permissions
- Regular review and removal of unnecessary access
- Temporary access automatically expires

3.2 Need-to-Know Basis

- Access limited to data required for specific business functions
- Cardholder data access restricted to authorized personnel only
- Cross-functional access requires additional approval
- Data access logged and monitored

3.3 Segregation of Duties

- Critical functions require multiple approvals
- No single individual has complete control over payment processes
- Development and production access segregated
- Financial and operational controls separated



3.4 Defense in Depth

- Multiple layers of access controls
- Authentication, authorization, and audit controls
- Network, application, and data-level restrictions
- Continuous monitoring and alerting

4. User Classification and Roles

4.1 Internal User Roles

4.1.1 Executive Management

Access Level: Strategic oversight, no direct system access

- Dashboard and reporting access only
- No direct cardholder data access
- Quarterly access reviews
- Systems: Executive dashboards, financial reports

4.1.2 System Administrators

Access Level: High privilege for infrastructure management

- Multi-factor authentication required
- All actions logged and monitored
- Quarterly privileged access review
- Systems: CDE infrastructure, network devices, security tools

4.1.3 Application Developers

Access Level: Development environment access, no production CHD

- Read-only production access for troubleshooting
- Full access to development and testing environments
- Code deployment through automated pipelines only
- Systems: Development environments, code repositories, testing tools



4.1.4 Operations Staff

Access Level: Production monitoring and maintenance

- Read-only access to production systems
- Incident response and troubleshooting capabilities
- No direct cardholder data access
- Systems: Monitoring tools, log analysis, alert management

4.1.5 Customer Support

Access Level: Limited merchant account management

- Access to merchant account information (non-CHD)
- Transaction status and troubleshooting tools
- No access to cardholder data or payment details
- Systems: Customer support portal, transaction logs (sanitized)

4.1.6 Compliance and Security

Access Level: Audit and security monitoring access

- Read-only access to all systems for compliance monitoring
- Security tool configuration and management
- Incident investigation capabilities
- Systems: SIEM, vulnerability scanners, audit logs

4.2 External User Roles

4.2.1 Merchant Customers

Access Level: API access for payment processing

- API key-based authentication with rate limiting
- Access limited to own merchant data only
- Real-time transaction processing capabilities
- Systems: Payment APIs, merchant portal, transaction reporting

4.2.2 Integration Partners



Access Level: Specific API endpoints for partner functions

- Certificate-based authentication for system-to-system connections
- Limited to specific data sets and functions
- Dedicated network connections where possible
- Systems: Partner APIs, data exchange interfaces

4.2.3 Third-Party Vendors

Access Level: Minimal access for specific services

- Time-limited access for specific projects
- Escorted access for sensitive systems
- All activities monitored and logged
- Systems: Determined case-by-case with security approval

4.2.4 Auditors and Assessors

Access Level: Read-only access for compliance validation

- Temporary access for audit periods only
- Access to compliance documentation and evidence
- Supervised access to sensitive systems
- Systems: Compliance systems, audit logs, documentation

5. Access Provisioning Process

5.1 New User Access Request

5.1.1 Internal Users

1. Request Initiation: Manager submits access request form
2. Business Justification: Detailed explanation of access requirements
3. Role Assignment: HR assigns appropriate role based on job function
4. Security Review: Security team reviews access requirements
5. Approval: Department head and security team approval required
6. Provisioning: IT provisions access based on approved role
7. Verification: User confirms access works as intended
8. Documentation: Access recorded in access management system



5.1.2 External Users (Merchants)

1. Account Registration: Merchant completes registration process
2. Identity Verification: KYC/AML verification procedures
3. Contract Execution: Merchant agreement signed
4. Risk Assessment: Merchant risk profile evaluation
5. API Key Generation: Unique API credentials generated
6. Access Provisioning: API access activated with appropriate limits
7. Testing: Merchant tests integration in sandbox environment
8. Production Activation: Live access enabled after successful testing

5.2 Access Modification Process

1. Change Request: Formal request for access changes
2. Business Justification: Reason for access modification
3. Impact Assessment: Security impact analysis
4. Approval: Same approval process as new access
5. Implementation: Changes implemented by IT
6. Verification: Access changes verified and documented

5.3 Access Removal Process

1. Trigger Events: Termination, role change, project completion
2. Immediate Suspension: Access suspended within 24 hours
3. Asset Recovery: Return of company devices and credentials
4. Access Verification: Verification that all access is removed
5. Documentation: Removal documented in access management system

Justification: This aligns with PCI DSS Requirement 8.1.4 (“Immediately revoke access for terminated users”) and ISO 27001 A.9.2.6 (“Removal of access rights”). Failure to recover credentials creates persistent attack vectors. Automated deprovisioning integrated with HR offboarding workflows ensures compliance and reduces insider threat risk.

6. Authentication Requirements

6.1 Internal Users

6.1.1 Standard Authentication



- Password Requirements: Minimum 12 characters, complexity rules
- Password Expiry: 90-day maximum password age
- Account Lockout: 10 failed attempts trigger 30-minute lockout
- Session Timeout: 15 minutes inactivity timeout

6.1.2 Multi-Factor Authentication (MFA)

Required for:

- All CDE access
- Administrative access
- VPN connections
- Privileged accounts

Approved MFA Methods:

- Hardware security keys (preferred)
- Mobile authenticator apps
- SMS codes (backup only)
- Biometric authentication

6.1.3 Privileged Account Management

- Dedicated Accounts: Separate accounts for administrative functions
- Just-in-Time Access: Temporary elevation for specific tasks
- Session Recording: All privileged sessions recorded
- Approval Workflows: Additional approval for high-risk actions

6.2 External Users

6.2.1 API Authentication

- API Keys: Unique keys for each merchant
- Key Rotation: Quarterly key rotation recommended
- Rate Limiting: Transaction and request rate limits
- IP Whitelisting: Restrict access to approved IP addresses

6.2.2 Merchant Portal Authentication



- Username/Password: Strong password requirements
- MFA Required: For all merchant portal access
- Session Management: Secure session handling
- Device Management: Register and manage trusted devices

7. Authorization Controls

7.1 Role-Based Access Control (RBAC)

7.1.1 Role Definition

- Predefined Roles: Standard roles for common job functions
- Custom Roles: Special roles for unique requirements
- Role Inheritance: Hierarchical role structures where appropriate
- Role Documentation: Clear documentation of role permissions

7.1.2 Permission Matrix

User Role	CHD Access	Production systems	Admin Functions	API Access
Executive	Dashboard Only	Read-Only Reports	None	None
SysAdmin	Emergency Only	Full Admin	Full	Config Only
Developer	None	Read-Only	Dev Env Only	Dev APIs
Operations	None	Monitoring	Limited	Status APIs
Support	None	Customer Portal	None	Support APIs
Merchant	None	Own Data Only	None	Payment APIs

7.2 Attribute-Based Access Control (ABAC)

- Context-Aware: Access decisions based on multiple attributes
- Time-Based: Access restrictions based on time of day/week



- Location-Based: Geographic restrictions where appropriate
- Risk-Based: Dynamic access based on risk assessment

7.3 Data Classification Access Rules

7.3.1 Cardholder Data (Restricted)

- Access Requirement: Explicit business need and management approval
- Authorized Roles: Payment processing staff, authorized developers
- Access Controls: Encryption, masking, tokenization
- Monitoring: All access logged and monitored in real-time

7.3.2 Merchant Data (Confidential)

- Access Requirement: Business need-to-know
- Authorized Roles: Customer support, operations, authorized management
- Access Controls: Role-based restrictions, data masking
- Monitoring: Access logged and reviewed monthly

7.3.3 Transaction Data (Internal)

- Access Requirement: Job function requirement
- Authorized Roles: Operations, reporting, compliance
- Access Controls: Aggregated/anonymized data preferred
- Monitoring: Access patterns monitored for anomalies

8. System-Specific Access Controls

8.1 Cardholder Data Environment (CDE)

8.1.1 Access Requirements

- Pre-Authorization: Security team pre-approval required
- Business Justification: Documented business need
- Time Limits: Maximum 8-hour access sessions
- Monitoring: Real-time monitoring and alerting
- Logging: All actions logged with full audit trail

8.1.2 CDE Access Procedures



1. Access Request: Submit request 24 hours in advance
2. Justification Review: Security team reviews business need
3. Approval: CISO or designee approval required
4. Access Provisioning: Temporary access granted
5. Activity Monitoring: Real-time monitoring during access
6. Session Termination: Automatic termination after time limit
7. Review: Post-access review of all activities

8.2 Payment APIs

8.2.1 Merchant API Access

- Authentication: API key + optional certificate authentication
- Authorization: Merchant can only access own data
- Rate Limiting: Configurable transaction and request limits
- IP Restrictions: Optional IP whitelisting
- Monitoring: Real-time fraud and abuse monitoring

8.2.2 Partner API Access

- Authentication: Mutual TLS certificate authentication
- Authorization: Function-specific access permissions
- Dedicated Connections: VPN or dedicated circuit preferred
- Data Restrictions: Limited to agreed data sets
- SLA Monitoring: Performance and availability monitoring

8.3 Administrative Systems

8.3.1 Network Infrastructure

- Console Access: Physical security required
- Remote Access: VPN + MFA required
- Emergency Access: Emergency procedures documented
- Change Control: All changes through formal process
- Backup Access: Secure backup authentication methods

8.3.2 Database Systems

- Database Access: Application service accounts only



- Direct Access: Emergency procedures with dual approval
- Query Monitoring: All queries logged and monitored
- Data Export: Special approval required for data exports
- Backup Access: Encrypted backups with secure key management

9. Access Monitoring and Auditing

9.1 Access Logging Requirements

9.1.1 Log Collection

- All Access Attempts: Successful and failed access logged
- User Identification: Unique user identification in all logs
- Timestamp: Accurate timestamps with timezone information
- Source Information: Source IP, device, and location data
- Action Details: Specific actions performed and data accessed

9.1.2 Log Protection

- Centralized Logging: All logs sent to central SIEM system
- Log Integrity: Cryptographic protection against tampering
- Retention: 12-month minimum retention period
- Access Controls: Limited access to audit logs
- Backup: Secure backup of all audit logs

9.2 Real-Time Monitoring

9.2.1 Automated Alerts

- Failed Authentication: Multiple failed login attempts
- Privilege Escalation: Attempts to gain elevated access
- Unusual Patterns: Access outside normal patterns
- Policy Violations: Access that violates security policies
- Critical Actions: High-risk administrative actions

9.2.2 Monitoring Dashboard

- Real-Time View: Current access sessions and activities
- Risk Indicators: Visual indicators of high-risk activities



- Alert Management: Centralized alert management and response
- Trending Analysis: Historical trends and pattern analysis
- Executive Reporting: Summary reports for management

9.3 Access Reviews and Audits

9.3.1 Regular Access Reviews

- Quarterly Reviews: All user access reviewed quarterly
- Annual Certification: Annual manager certification of team access
- Role-Based Reviews: Systematic review of role permissions
- Exception Reviews: Review of any access exceptions or violations

9.3.2 Audit Procedures

- Internal Audits: Semi-annual internal access control audits
- External Audits: Annual third-party access control assessments
- Compliance Audits: PCI DSS and other regulatory audits
- Penetration Testing: Annual testing of access controls

10. Special Access Scenarios

10.1 Emergency Access Procedures

10.1.1 Emergency Access Criteria

- System Outages: Critical system failures affecting payments
- Security Incidents: Active security breaches or attacks
- Compliance Issues: Urgent compliance or regulatory requirements
- Business Continuity: Disaster recovery and business continuity

10.1.2 Emergency Access Process

1. Declaration: Incident commander declares emergency
2. Authorization: Emergency access authorization by CISO or CEO
3. Access Provisioning: Temporary elevated access granted
4. Activity Monitoring: Enhanced monitoring during emergency access
5. Documentation: All emergency actions documented
6. Review: Post-incident review and access revocation



10.2 Third-Party Access

10.2.1 Vendor Access Management

- Due Diligence: Security assessment before granting access
- Contractual Controls: Security requirements in vendor contracts
- Limited Access: Minimal access required for services
- Monitoring: Enhanced monitoring of vendor activities
- Termination: Immediate access revocation upon contract end

10.2.2 Auditor Access

- Temporary Access: Limited-time access for audit periods
- Supervised Access: Supervised access to sensitive systems
- Read-Only Access: No modification of systems or data
- NDA Requirements: Non-disclosure agreements required
- Access Logging: All auditor activities logged and reviewed

10.3 Remote Access Controls

10.3.1 VPN Access

- Multi-Factor Authentication: Required for all VPN connections
- Split Tunneling: Prohibited for CDE-connected sessions
- Session Monitoring: All VPN sessions monitored
- Geographic Restrictions: VPN access from approved countries only
- Device Management: Managed devices preferred for VPN access

10.3.2 Remote Work Considerations

- Secure Devices: Company-managed devices required for CHD access
- Network Security: Secure home network requirements
- Physical Security: Secure workspace requirements
- Data Handling: Restrictions on local data storage
- Incident Reporting: Enhanced incident reporting requirements

11. Access Control Violations

11.1 Violation Categories



11.1.1 Policy Violations

- Unauthorized Access: Accessing systems without authorization
- Privilege Abuse: Using access beyond authorized scope
- Password Sharing: Sharing credentials with others
- Bypass Attempts: Attempting to circumvent access controls
- Data Misuse: Inappropriate use of accessed data

11.1.2 Security Incidents

- Account Compromise: Compromised user accounts
- Insider Threats: Malicious insider activities
- External Attacks: External attempts to gain unauthorized access
- Data Breaches: Unauthorized disclosure of sensitive data
- System Intrusions: Unauthorized system modifications

11.2 Incident Response

11.2.1 Detection and Response

- Automated Detection: SIEM alerts for policy violations
- Investigation: Security team investigation of incidents
- Containment: Immediate containment of security threats
- Evidence Collection: Preservation of incident evidence
- Reporting: Incident reporting to management and authorities

11.2.2 Disciplinary Actions

- Warning: Verbal or written warnings for minor violations
- Access Suspension: Temporary suspension of access privileges
- Termination: Employment termination for serious violations
- Legal Action: Legal prosecution for criminal activities
- Recovery: Efforts to recover any damages or losses

12. Training and Awareness

12.1 Security Awareness Training

12.1.1 General Training



- Annual Training: Mandatory annual security awareness training
- Access Control Focus: Specific training on access control policies
- Role-Specific Training: Training tailored to specific job roles
- Update Training: Training on policy and procedure updates
- Compliance Training: Training on regulatory requirements

12.1.2 Specialized Training

- Privileged User Training: Additional training for privileged users
- Developer Training: Secure coding and access control training
- Manager Training: Training for managers on access approval
- Incident Response: Training on security incident procedures
- New Hire Training: Access control training for new employees

12.2 Ongoing Awareness

12.2.1 Communication

- Policy Updates: Communication of policy changes
- Security Alerts: Alerts about new threats and vulnerabilities
- Best Practices: Sharing of access control best practices
- Lessons Learned: Sharing lessons from security incidents
- Recognition: Recognition of good security practices

13. Technology Controls

13.1 Identity and Access Management (IAM)

13.1.1 IAM System Requirements

- Centralized Management: Single system for identity management
- Role-Based Provisioning: Automated role-based access provisioning
- Workflow Management: Approval workflows for access requests
- Integration: Integration with all business systems
- Reporting: Comprehensive access reporting capabilities

13.1.2 Single Sign-On (SSO)

- SSO Implementation: SSO for all compatible business applications



- SAML/OAuth: Standard protocols for authentication
- Session Management: Secure session management across applications
- Logout Procedures: Secure logout from all applications
- Federation: Identity federation with trusted partners

13.2 Privileged Access Management (PAM)

13.2.1 PAM System Features

- Password Vaulting: Secure storage of privileged passwords
- Session Recording: Recording of all privileged sessions
- Just-in-Time Access: Temporary elevation of privileges
- Approval Workflows: Multi-level approval for privileged access
- Risk Scoring: Risk-based access decisions

13.2.2 Privileged Account Controls

- Shared Account Management: Secure management of shared accounts
- Service Account Management: Automated service account management
- Emergency Access: Emergency break-glass procedures
- Account Discovery: Automated discovery of privileged accounts
- Compliance Reporting: Detailed compliance reporting

13.3 Application Security Controls

13.3.1 API Security

- OAuth 2.0: Industry standard for API authorization
- Rate Limiting: Protection against abuse and attacks
- Input Validation: Validation of all API inputs
- Output Encoding: Secure encoding of API outputs
- Error Handling: Secure error handling and logging

13.3.2 Web Application Security

- Session Management: Secure web session management
- CSRF Protection: Cross-site request forgery protection
- XSS Prevention: Cross-site scripting prevention
- SQL Injection Prevention: Parameterized queries and validation



- Security Headers: Implementation of security headers

14. Compliance Monitoring

14.1 Key Performance Indicators (KPIs)

14.1.1 Access Metrics

- Access Request Processing Time: Average time to process requests
- Policy Compliance Rate: Percentage of compliant access
- Review Completion Rate: Percentage of reviews completed on time
- Violation Rate: Number of access control violations
- Training Completion Rate: Percentage of users trained

14.1.2 Security Metrics

- Failed Authentication Rate: Rate of failed login attempts
- Privileged Access Usage: Usage patterns of privileged accounts
- Emergency Access Frequency: Frequency of emergency access usage
- Incident Response Time: Time to respond to access incidents
- Audit Finding Remediation: Time to remediate audit findings

14.2 Reporting Requirements

14.2.1 Regular Reports

- Monthly Access Reports: Summary of access activities and metrics
- Quarterly Review Reports: Results of quarterly access reviews
- Annual Compliance Reports: Comprehensive compliance status
- Incident Reports: Detailed reports on security incidents
- Audit Reports: Results of internal and external audits

14.2.2 Executive Reporting

- Dashboard Metrics: Real-time security dashboard for executives
- Risk Reports: Summary of access-related risks
- Compliance Status: Current compliance status and issues
- Investment Recommendations: Recommendations for security investments
- Trend Analysis: Analysis of security trends and patterns



15. Policy Maintenance

15.1 Policy Review and Updates

15.1.1 Review Schedule

- Semi-Annual Reviews: Policy reviewed every 6 months
- Triggered Reviews: Reviews triggered by incidents or changes
- Regulatory Updates: Updates for new regulatory requirements
- Technology Changes: Updates for new technology implementations
- Business Changes: Updates for business process changes

15.1.2 Update Process

- Change Proposal: Formal process for proposing changes
- Impact Assessment: Assessment of change impacts
- Stakeholder Review: Review by affected stakeholders
- Approval Process: Formal approval by management
- Implementation: Controlled implementation of changes
- Communication: Communication of changes to all users

15.2 Related Documentation

- Access Control Procedures: Detailed step-by-step procedures
- Role Definitions: Detailed definitions of all user roles
- System Documentation: Documentation of access control systems
- Training Materials: Materials for access control training
- Audit Procedures: Procedures for access control audits

16. Definitions and Acronyms

- Access Control: Security features that control which users can access which resources
- API: Application Programming Interface
- CHD: Cardholder Data
- CDE: Cardholder Data Environment
- IAM: Identity and Access Management
- MFA: Multi-Factor Authentication
- PAM: Privileged Access Management



ORCHESTRATE

- RBAC: Role-Based Access Control
- SIEM: Security Information and Event Management
- SSO: Single Sign-On

END OF POLICY

Document Version 1.0 – Effective 1 September 2025

Prepared in accordance with PCI DSS v4.0.1, ISO/IEC 27001:2022, and internal governance standards.