



User Access Management Process

Control Page

ATTRIBUTE	DETAIL
Document Title	<i>User Access Management Process</i>
Document ID	OG-PROC-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	All Orchestrate Global employees, contractors, third-party vendors, and system users who require access to corporate systems, applications, infrastructure, or cardholder data environments (CDE). Any individual or entity accessing Orchestrate Global systems must comply with this policy, regardless of role, location, or employment status.
Compliance Frameworks	PCI DSS v4.0
Distribution List	All Employees, Board of Directors, Audit Committee, Key Merchant Partners, Compliance Team

Approvals

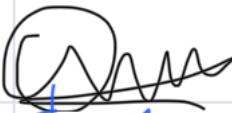
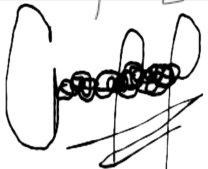
NAME	POSITION	SIGNATURE	DATE
Oleksii Bondarenko	Chief Security & Compliance Officer		1 November 2025
Charles Odhiambo	Technical Lead		1 November 2025
Kevin Kegera	Chief Commercial Officer		1 November 2025
Preston Obadan	Chief Executive Officer		1 November 2025

Table of Contents

1. Introduction

- 1.1 Purpose
- 1.2 Scope
- 1.3 Applicability

2. Control Page Information

- 2.1 Control Objective
- 2.2 Regulatory and Standards Alignment



- 2.3 Risk-Based Justification
- 2.4 Roles and Responsibilities
- 2.5 Review and Maintenance

3. Access Management Lifecycle

- 3.1 Lifecycle Phases
- 3.2 User Categories and Access Levels

4. User Onboarding and Access Provisioning

- 4.1 Access Request Process
- 4.2 Access Approval Matrix
- 4.3 Account Creation Procedures

5. Access Modification and Role Changes

- 5.1 Access Modification Request
- 5.2 Enforcing the Principle of Least Privilege

6. Access Review and Recertification

- 6.1 Access Review Schedule
- 6.2 Access Review Procedures
- 6.3 Inactive Account Management

7. User Offboarding and Access Revocation

- 7.1 Employee Termination Process
- 7.2 Access Revocation Checklist
- 7.3 Merchant and Third-Party Account Closure

8. Emergency and Privileged Access Management

- 8.1 Emergency Access Procedures
- 8.2 Break-Glass Account Management
- 8.3 Privileged Access Management (PAM)

9. Third-Party and Vendor Access Management

- 9.1 Vendor Access Request Process
- 9.2 Vendor Access Controls
- 9.3 Contractor and Consultant Access

10. Monitoring, Logging, and Audit

- 10.1 Access Monitoring and Alerting
- 10.2 Access Audit Logs
- 10.3 Compliance Reporting

11. Password Management Policy

- 11.1 Password Complexity Requirements
- 11.2 Password Expiration and Rotation
- 11.3 Secure Storage and Transmission
- 11.4 Prohibited Practices
- 11.5 Password Recovery and Reset



12. Exception Management

- 12.1 Access Policy Exceptions
- 12.2 Exception Documentation and Approval

13. Training and Awareness

- 13.1 Role-Based Training
- 13.2 User Responsibilities and Accountability

14. Metrics and Key Performance Indicators (KPIs)

15. Roles and Responsibilities Summary

16. Contact Information

1. Introduction

1.1 Purpose

This document defines Orchestrate Global's formal User Access Management (UAM) Process to ensure secure, auditable, and compliant control over logical access to all system components—particularly those within the Cardholder Data Environment (CDE). It establishes procedures for provisioning, modifying, reviewing, and revoking access throughout the user lifecycle.

1.2 Scope

Applies to all internal personnel (employees, contractors), external entities (merchants, partners, vendors), and emergency/privileged users requiring access to Orchestrate Global's payment orchestration platform, supporting infrastructure, APIs, databases, and CDE systems.

1.3 Applicability

Mandatory for all individuals and roles interacting with Orchestrate Global systems. Non-compliance may result in disciplinary action, contract termination, or regulatory penalties.



2. Control Page Information

2.1 Control Objective

To enforce a risk-based, policy-driven access control framework that ensures only authorized, authenticated, and justified users can access systems or data—minimizing exposure of cardholder data and maintaining system integrity through continuous monitoring, least privilege, and timely deprovisioning.

2.2 Regulatory and Standards Alignment

This process directly implements controls required by:

- PCI DSS v4.0.1:
 - Requirement 7.1–7.3: Restrict access based on need-to-know; implement access control systems; manage user access lifecycle
 - Requirement 8.2–8.6: Strong authentication, unique IDs, password policies, account management
- SOX Section 404: Enforces segregation of duties and auditability of IT access
- ISO/IEC 27001:2022: A.8.2 (User Access Management), A.8.3 (Authentication Information)
- NIST SP 800-53 Rev. 5: AC-2 (Account Management), IA-5 (Authenticator Management)

This alignment is validated quarterly via internal audits and continuously through automated compliance dashboards.

2.3 Risk-Based Justification

Unauthorized or excessive access poses critical risks to cardholder data confidentiality and system availability. This process mitigates such risks by embedding:

- Least privilege at provisioning
- Multi-factor authentication for all CDE and privileged access
- Automated deprovisioning upon role change or termination



- Continuous monitoring for anomalous behavior
These controls reduce attack surface, support forensic readiness, and satisfy auditor expectations.

2.4 Roles and Responsibilities

- Chief Security & Compliance Officer (CSCO): Policy ownership, exception approval, compliance validation
- Chief Technology Officer (CTO): Technical implementation oversight, emergency access authorization
- IT/Operations Team: Execute provisioning/deprovisioning per approved workflows
- Department Managers: Approve and recertify team access quarterly
- Security Team: Monitor logs, conduct access reviews, investigate anomalies
- HR: Trigger offboarding workflows and validate employment status

2.5 Review and Maintenance

Reviewed quarterly or after material changes (e.g., new CDE systems, breaches, regulatory updates). Revisions require CSCO and CTO approval. Version history maintained in Section 16.

3. Access Management Lifecycle

3.1 Lifecycle Phases

Access management is governed by an eight-phase lifecycle:

1. Request: Initiated by user or manager with business justification
2. Review: Security team validates compliance and risk posture
3. Approval: Authorized by appropriate management tier
4. Provisioning: IT creates accounts and assigns permissions
5. Validation: User and security team confirm correct access
6. Monitoring: Continuous oversight of access usage
7. Modification: Adjustments due to role changes or project needs
8. Deprovisioning: Full revocation upon termination or role change

Each phase includes defined timelines, responsibilities, and documentation requirements to ensure accountability.



3.2 User Categories and Access Levels

Access is tiered based on user function and sensitivity of systems:

- System Administrators: Full infrastructure access; monthly review
- Security Team: Monitoring and security tool access; monthly review
- Developers: Staging and development environments; quarterly review
- Operations Team: Production read-only with limited write; quarterly review
- Merchant Admins: Manage merchant accounts; semi-annual review
- Merchant Users: View transactions and reports; annual review
- Support Team: Customer support tools; quarterly review
- Finance Team: Settlement and reporting data; quarterly review

Each category has defined approval chains and review frequencies to enforce accountability.

4. User Onboarding and Access Provisioning

4.1 Access Request Process

All access requests must include:

- Full name and unique identifier (employee or merchant ID)
- Official email address
- Department or organization
- Job title or role
- Direct manager or supervisor
- Business justification
- Specific systems or applications required
- Required access level (read-only, read-write, admin)
- Duration (permanent, temporary, or project-based)

Requests are submitted via the IT service desk ticketing system, a standardized electronic form, or designated secure email address.

4.2 Access Approval Matrix

Approval authority is determined by access type:



- Standard Employee Access: Direct manager + department head
- Privileged Access: Department head + CTO + CSCO security review
- CDE Access: Department head + CSCO with formal risk acceptance
- Database Access: Database manager + CTO + CSCO
- Production Access: Operations manager + CTO + security clearance
- Emergency Access: On-call manager + CTO/CSCO with post-use review
- Vendor Access: Business owner + CTO + vendor security assessment

All approvals are documented and retained for audit purposes.

4.3 Account Creation Procedures

Internal email accounts follow the format firstname@orchestrate.global. Security policies applied include mandatory multi-factor authentication, email encryption, and blocked external forwarding.

Application access is primarily granted via magic link authentication, eliminating static passwords for user-facing systems. Upon provisioning:

- User email is added to the authentication database
- Role is assigned (e.g., Merchant User, Internal Admin)
- Magic link expiration is configured based on role sensitivity
- MFA is enforced where required
- Welcome email with login instructions is sent
- First login is verified, and user acceptance is captured

Access rights are assigned via role-based groups for dashboards, staging environments, APIs, and databases, with validation performed through functional tests.

5. Access Modification and Role Changes

5.1 Access Modification Request

Modifications are triggered by role changes, promotions, transfers, project assignments, or temporary needs. The process includes:



1. Submission of modification request
2. Review of current access by security
3. Assessment of new requirements
4. Approval by appropriate manager
5. Implementation of changes by IT
6. Removal of obsolete permissions
7. Validation by security
8. Documentation of all changes

5.2 Principle of Least Privilege Enforcement

All modifications adhere to least privilege:

- Old access is removed before new access is granted
- Permissions are limited to the minimum necessary
- Temporary access includes automatic expiration
- Business justification is documented
- Access is re-evaluated after 90 days

Common scenarios include promotions (adding management tools), department transfers (swapping dashboards), and role reductions (downgrading admin rights).

6. Access Review and Recertification

6.1 Regular Access Review Schedule

- Privileged/CDE Access: Monthly
- Employee Access: Quarterly
- Merchant Access: Semi-annually
- Vendor Access: Quarterly
- Dormant Accounts: Monthly (after 30+ days inactive)

6.2 Access Review Procedures

Reviews are conducted in three phases:

- Preparation: Security generates user access reports by department



- Review: Managers verify alignment with current roles and flag unnecessary access
- Remediation: IT implements removals; security validates and reports compliance

A standardized certification form captures approvals, required actions, and notes, signed by the reviewing manager.

6.3 Inactive Account Management

Accounts inactive for 30 days (internal) or 90 days (merchant) are flagged. At 60 days, internal accounts are disabled; at 90 days, deactivated. API accounts inactive for 180 days are archived. Automated notifications are sent at 30, 45, and 60 days.

7. User Offboarding and Access Revocation

7.1 Employee Termination Process

- Planned Termination: Full access revocation begins 2 hours before the last working day
- Immediate Termination: All systems disabled within 15 minutes (email, magic links, VPN, APIs, cloud consoles, databases)

7.2 Access Revocation Checklist

Includes deactivation of:

- Email and magic link authentication
- MFA enrollment
- Network and cloud platform access (AWS/Azure/GCP)
- Application, database, and repository permissions
- API and SSH keys
- Collaboration tools (Slack/Teams)
- Physical access badges and company devices
- Shared credentials (rotated if exposed)

Final verification is performed by the security team.



7.3 Merchant Account Closure

Process includes:

1. Closure request acknowledgment
2. Financial reconciliation and final settlements
3. Data retention notification
4. Dashboard and API access revocation on Day 7
5. Data archival on Day 30
6. Seven-year retention for compliance

8. Emergency and Privileged Access Management

8.1 Emergency Access Procedures

Granted for production outages, security incidents, or critical bugs. Requires verbal CTO/CISO approval, with access provisioned within 30 minutes. All actions are logged in real time, and full documentation is submitted within 24 hours.

8.2 Break-Glass Account Management

Break-glass accounts are secured physically (sealed envelopes in safes) and digitally (encrypted with multi-party decryption). Usage requires dual authorization, triggers real-time SIEM alerts, expires after 4 hours, and mandates post-use executive review.

8.3 Privileged Access Management (PAM)

Privileged accounts are never shared. Access is logged, monitored, and recorded. Just-in-time provisioning is preferred. Monthly reviews, mandatory MFA, and segregation of duties are enforced.

9. Third-Party and Vendor Access Management

9.1 Vendor Access Request Process



Requires:

- Formal request
- Security questionnaire
- Risk assessment
- Signed NDA
- CTO/CSCO approval
- Limited, time-bound provisioning
- Monitoring setup

9.2 Vendor Access Controls

- Maximum 12-month duration (renewable)
- Network isolation
- No CDE access without explicit approval
- Mandatory MFA and VPN
- All actions logged and monitored

Access levels include read-only, limited write, administrative (scoped), and support (read-only customer data).

9.3 Contractor and Consultant Access

Duration-based approval:

- <30 days: Manager approval
- 30–90 days: Department head + monthly review
- 90 days: CTO approval + monthly review
- 6 months: Executive approval + bi-weekly review

Automatic expiration and 24-hour offboarding audit ensure accountability.

10. Monitoring, Logging, and Audit

10.1 Access Monitoring and Alerting

Real-time alerts for:



- 5 failed logins in 5 minutes
- Off-hours privileged access
- New CDE access grants
- Mass access changes (>10/hour)
- Logins from new countries (blocked + alerted)
- Activity on disabled accounts

10.2 Access Audit Logs

Logs retained as follows:

- Provisioning/modification/removal/reviews: 7 years
- Login events: 12 months
- Privileged actions: 24 months

All logs are immutable and accessible only to security and audit personnel.

10.3 Compliance Reporting

Weekly/monthly reports cover:

- New accounts and terminations
- Privileged access usage
- Review completion status
- Dormant accounts
- Failed logins
- Real-time executive compliance dashboard

11. Password Management Policy

11.1 Password Complexity Requirements

- Minimum 12 characters
- Uppercase, lowercase, numeric, and special characters
- Not based on dictionary words, usernames, or repeated patterns
- Unique across all corporate systems

11.2 Password Expiration and Rotation



- Standard accounts: 90-day rotation
- Privileged accounts: 60-day rotation
- No reuse of last 24 passwords

11.3 Secure Storage and Transmission

- Stored using adaptive hashing (Argon2id or PBKDF2 $\geq 100,000$ iterations)
- Transmitted only over TLS 1.2 or higher
- Never logged, cached, or stored in plaintext

11.4 Prohibited Practices

- Sharing credentials
- Writing passwords on paper or unsecured digital notes
- Using personal password managers for corporate credentials
- Bypassing MFA

11.5 Password Recovery and Reset

- Self-service reset requires MFA verification
- Helpdesk resets require two-factor identity confirmation
- All resets logged and monitored for abuse

12. Exception Management

12.1 Access Policy Exceptions

Permitted only for legal, critical business, or technical reasons—with compensating controls (e.g., enhanced logging, time limits).

12.2 Exception Documentation

Requires:

- Business justification
- Risk assessment
- Compensating controls
- Exception duration



- Review frequency
- CISO/CTO risk acceptance signature
- Remediation plan

Exceptions are reviewed monthly.

13. Training and Awareness

13.1 Role-Based Training

- All Users: Annual security awareness + quiz
- Managers: Semi-annual access review training + certification
- IT/Security: Quarterly hands-on assessments
- HR: Semi-annual onboarding/offboarding coordination training

13.2 User Responsibilities

Users must:

- Protect authentication credentials
- Report suspicious activity
- Avoid sharing accounts
- Use access appropriately
- Report role changes
- Complete training
- Participate in access reviews

14. Metrics and KPIs

METRIC	TARGET	MEASUREMENT	FREQUENCY
Access Provisioning Time	<3 business days	Ticket resolution time	Weekly
Access Review Completion	100% on-time	Completion rate	Monthly



Dormant Account Rate	<5%	Inactive/total accounts	Monthly
Access Removal Upon Termination	<4 hours	Time to full revocation	Weekly
Failed Access Attempts	Trending down	Failed login rate	Daily
Privileged Access Review	100% monthly	On-time completion	Monthly

15. Roles and Responsibilities

- CSCO: Policy oversight, exception approval, compliance verification
- CTO: Technical implementation, emergency access authorization
- IT Manager: Provisioning, system maintenance
- Security Manager: Monitoring, reviews, audit support
- Department Managers: Approvals, quarterly reviews
- HR Manager: Onboarding/offboarding coordination
- Help Desk: Request intake, ticket management
- Compliance Officer: Audit coordination, documentation

16. Contact Information

- Access Requests: access-management@orchestrate.global (Business hours)
- IT Help Desk: helpdesk@orchestrate.global (24/7)
- Security Team: security@orchestrate.global (24/7)