



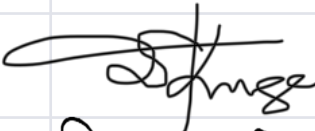
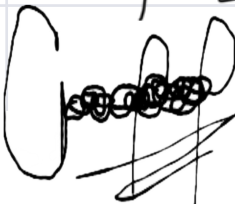
Release and Deployment Management Policy

Document Control

FIELD	DETAILS
Document Title	Release and Deployment Management Policy
Document Number	OG-RDM-POL-004
Version	1.0
Effective Date	1 November 2025
Next Review Date	1 November 2026
Policy Owner	Chief Security & Compliance Officer (CSCO)
Classification	Confidential – Internal Use Only
Distribution	All Engineering, IT, DevOps, Security Teams, and Approved Vendors



Approvals

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

1. Purpose and Scope

This policy establishes a secure, auditable, and resilient release and deployment management framework that ensures all changes to Orchestrate Global's payment orchestration platform are introduced in a manner that:

- Preserves the confidentiality, integrity, and availability of cardholder data (CHD);
- Maintains continuous, uninterrupted payment processing;
- Enforces least-privilege access and separation of duties;
- Embeds security and compliance into every phase of the SDLC;
- Provides full traceability from requirement to production deployment.

Scope Includes:

- All code, configuration, infrastructure, and data changes affecting the Cardholder Data Environment (CDE);
- Internal and third-party software components;
- CI/CD pipelines, deployment tooling, and automation scripts;
- Mobile, web, API, and backend services;
- Monitoring, logging, and observability systems.



2. Foundational Principles

Orchestrate Global adheres to the following core principles in release and deployment management:

1. **Security by Default:** All environments, artifacts, and configurations are secure unless explicitly and justifiably relaxed under controlled conditions.
2. **Immutable Artifacts:** Once built, deployment artifacts are never modified; all changes require a new build and validation cycle.
3. **Zero Trust Deployment:** No implicit trust is granted to any component, environment, or user—continuous validation is required.
4. **Shift Left Security:** Security controls are integrated early and continuously throughout the SDLC.
5. **Observability-Driven Releases:** Deployment decisions are informed by real-time telemetry and risk signals.

3. Release Types, Risk Classification, and Governance

RELEASE TYPE	FREQUENCY	RISK LEVEL	APPROVAL AUTHORITY	SECURITY AND COMPLIANCE REQUIREMENTS
Major Release	Quarterly	HIGH	CEO, CTO, CSCO	Full PCI DSS validation, penetration test, architecture review, threat modeling
Minor Release	Bi-weekly	MEDIUM	CTO, Product Owner	SAST/DAST, dependency scan, UAT, performance baseline validation
Patch Release	Weekly	LOW	Development Manager	Targeted testing, vulnerability remediation verification
Hotfix Release	As needed	HIGH	CTO, CSCO (written or recorded verbal)	Critical path testing, security validation, rollback rehearsal



Emergency Release	Immediate	CRITICAL	CTO (verbal), with CSCO notified within 15 minutes	Post-deployment forensic review, incident linkage, mandatory post-mortem within 48 hours
-------------------	-----------	----------	--	--

Note: All releases—regardless of type—must pass automated policy gates in the CI/CD pipeline before promotion.

4. Secure SDLC Integration

4.1 Requirements & Design Phase

- All features impacting CHD or payment flows undergo threat modeling (using STRIDE or PASTA).
- Security and privacy requirements are documented in user stories and tracked in Jira/ALM.
- Architecture diagrams are reviewed by the Security Lead for CDE boundary integrity.

4.2 Development Phase

- Developers use pre-approved, hardened base images and secure coding standards (OWASP ASVS Level 2+).
- Branch protection rules enforce:
 - Mandatory pull requests;
 - ≥2 peer reviews (one from Security or DevOps);
 - Signed commits (GPG or S/MIME);
 - No direct pushes to `main` or `release/*` branches.

4.3 Build & Test Phase

- Immutable, signed artifacts are generated with SBOMs (Software Bill of Materials).
- Automated SAST, SCA, and IaC scanning block builds with:
 - Any critical vulnerabilities;
 - 5 high severity issues;
 - Hardcoded secrets or non-compliant configurations.



- Dynamic testing (DAST/IAST) runs against staging with production-like traffic patterns.

4.4 Pre-Production Validation

- Pre-Prod is a full replica of Production (network topology, data volume, encryption settings).
- Red team validation is required for any change affecting authentication, authorization, or CHD handling.
- Performance and chaos testing simulate peak load and failure scenarios (e.g., database failover, network partition).

5. Deployment Security Controls

5.1 Environment Isolation & Data Handling

- No production CHD is permitted in Dev, Integration, or Staging.
- Synthetic data generators produce PCI-compliant test datasets with realistic distributions.
- Data masking/anonymization is applied to any production-derived data used in Pre-Prod.

5.2 Deployment Execution

- All deployments use idempotent, declarative IaC (Terraform with OPA policies).
- Blue-green or canary strategies are mandatory for all CDE-impacting changes.
- Zero-downtime is enforced via:
 - Health probes before traffic shift;
 - Automatic rollback on error rate >0.5%;
 - Transaction replay validation for database migrations.

5.3 Secrets & Credentials

- No secrets in code, configs, or logs.
- Runtime secrets are injected via HashiCorp Vault or AWS Secrets Manager with short TTLs.



- Audit logs capture all secret access during deployment.

6. Audit, Compliance, and Evidence Retention

ARTIFACT	RETENTION PERIOD		
Deployment Logs	7 years	Security, Audit, CSCO	PCI DSS 10.2, SOX
Code & Configuration Changes	7 years	Dev, Ops, Security	Change traceability
Security Scan Reports	3 years	Security Team	Vulnerability trend analysis
Approval Records	7 years	Governance, Legal	Accountability & compliance evidence
Rollback & Incident Logs	7 years	Incident Response Team	Post-mortem & regulatory reporting

All logs are immutable, time-synchronized (NTP), and shipped to a SIEM with tamper-evident storage.

7. Roles, Responsibilities, and Accountability

ROLE	KEY RESPONSIBILITIES
Chief Technology Officer (CTO)	Final approval for high-risk releases; resource allocation; policy enforcement oversight
Chief Security & Compliance Officer (CSCO)	Validate PCI DSS/SOX alignment; approve security overrides; lead compliance audits



Release Manager	End-to-end coordination; risk register maintenance; stakeholder communication
Security Lead	Enforce security gates; conduct threat modeling; approve emergency overrides
DevOps Engineer	Maintain secure CI/CD pipeline; manage IaC; ensure artifact integrity
Database Administrator	Validate schema changes; ensure zero data loss; manage encrypted backups

Separation of Duties: No single individual may approve, deploy, and validate a production change.

8. Continuous Improvement & Innovation

Orchestrate Global commits to evolving its deployment maturity through:

- Quarterly red team exercises simulating supply chain and deployment pipeline attacks;
- Automated policy-as-code (e.g., Open Policy Agent) to enforce compliance in pipelines;
- GitOps adoption by Q2 2026 for declarative, auditable deployments;
- AI-assisted anomaly detection in deployment telemetry to predict failures.

9. Policy Enforcement

- Non-compliance with this policy constitutes a material control failure and may result in:
 - Suspension of deployment privileges;
 - Escalation to Executive Leadership;
 - Disciplinary action per HR policy.
- Exceptions require written justification, risk acceptance by CSCO and CTO, and time-bound remediation.



ORCHESTRATE

This policy is reviewed semi-annually or after any material security incident, regulatory change, or significant architectural evolution.