



Cryptographic Policy

Document Number: OG-CRYPTO-POL-001

Version: 1.0

Effective Date: 1 November 2025

Next Scheduled Review: 1 November 2026

Policy Owner: Chief Security & Compliance Officer (CSCO)

1. Document Review

This policy applies to:

- All Employees
- IT, Security, Engineering, Finance, and Operations Teams
- Contractors involved in infrastructure, development, or security tasks involving sensitive or cardholder data
- Third-Party Vendors and Service Providers with access to encrypted data, encryption keys, or cardholder systems (Cloud, MSPs, Payment Processors)

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



2. Table of Contents

1. Document Review & Approvals
2. Purpose
3. Scope
4. Compliance & Policy Alignment
5. Definitions & Terminology
6. Roles and Responsibilities
7. Approved Cryptographic Algorithms & Key Lengths
8. Key Management Lifecycle
9. Protection of Cardholder Data in Transit
10. Protection of Cardholder Data at Rest
11. Tokenization, Hashing, and PAN Truncation
12. Cryptographic Key Storage & Access Control
13. Key Rotation, Revocation, Destruction
14. Cryptographic Incident Response
15. Logging, Monitoring & Audit Requirements
16. Third-Party Cryptography Requirements
17. Policy Maintenance, Exceptions & Violations
18. Revision History

3. Purpose

This policy establishes the mandatory requirements for the use of cryptography to protect sensitive information at Orchestrate Global Inc., with emphasis on:

- Ensuring **confidentiality and integrity** of Cardholder Data (CHD) and Sensitive Authentication Data (SAD)
- Implementing and maintaining **robust cryptographic controls** during **storage, transmission, backup, and disposal**
- Defining procedures for **key generation, use, storage, distribution, rotation, and destruction**
- Meeting corporate, legal, and regulatory requirements, including **PCI DSS v4.0 requirements 3, 4, and 12**



4. Scope

This policy applies to all:

Data Types:

- Cardholder Data (PAN, cardholder name, expiry date, service code)
- Sensitive Authentication Data (CVV, full track data, PINs) – stored only until authorization is complete
- Encryption keys, API secrets, TLS certificates, HSM/KMS master keys
- System credentials, tokens, password vaults, SSH keys

Systems & Technologies:

- Databases, application servers, cloud deployments, encryption libraries
- AWS KMS, Azure Key Vault, HSMs, secure enclaves
- Network encryption protocols (TLS, VPN, IPSec, SSH)

Environments Covered:

- Production, Staging, Development, Testing (where test data contains real CHD)
- On-premises infrastructure and all cloud environments
- Third-party service providers processing data on behalf of Orchestrate Global

5. Compliance & Policy Alignment

This policy supports and aligns with the following:

Standard / Framework	Relevant Sections Covered
PCI DSS v4.0	Req. 3 (Protect Stored Data), Req. 4 (Encrypt Transmission), Req. 12 (Policies & Governance)
NIST SP 800-57	Key Management Best Practices
NIST SP 800-52	TLS Configuration Guidelines



6. Definitions & Terminology

Term	Definition
Cardholder Data (CHD)	Primary Account Number (PAN), cardholder name, service code, and expiration date
Sensitive Authentication Data (SAD)	Full track data, CVV2/CVC2, PINs — must never be stored post-authorization
Cryptographic Key	A value used in encryption, decryption, digital signatures, or hashing
Tokenization	Replacing a PAN with a non-sensitive surrogate token
PAN Truncation	Displaying/storing only the first 6 and last 4 digits of a PAN
HSM (Hardware Security Module)	Tamper-resistant hardware for secure key management
KMS (Key Management Service)	AWS KMS, Azure Key Vault — centralized key storage/control
PFS (Perfect Forward Secrecy)	Ensures session keys cannot be derived from long-term private keys



Split Knowledge & Dual Control

Key custodians each hold partial key knowledge; no single individual can access full keys

7. Roles and Responsibilities

Role

Responsibilities

Chief Security & Compliance Officer (CSCO)

Owns this policy; approves cryptographic standards; authorizes key custodians; approves key rotations, revocations, emergency decryption procedures.

Chief Technology Officer (CTO)

Ensures alignment of cryptographic architecture with engineering standards; approves use of cryptographic libraries and protocols across systems.

DevOps / Infrastructure Teams

Implement encryption services; manage AWS KMS/Azure Key Vault; enforce TLS configurations; deploy HSM where applicable.

Security Engineering Team

Conducts cryptographic risk assessments; reviews API encryption; manages key lifecycle automation; performs penetration testing of encryption implementations.

System Administrators

Ensure encrypted backups, secure certificate deployment, patch management for cryptographic services, rotate expired TLS certificates.

Application Developers

Use approved cryptographic libraries; avoid custom encryption; ensure no storage of SAD post-authorization; secure API endpoints using TLS 1.2 or higher.



Internal Audit & Compliance Team

Reviews cryptographic key logs quarterly; verifies proper rotations, expirations, disposal; documents any deviations or compensating controls.

Third-Party Service Providers

Must use equivalent or stronger encryption and key management controls; subject to due diligence, contract clauses, and audit rights.

8. Approved Cryptographic Algorithms and Key Strengths

Only the following algorithms and key lengths are permitted for protecting cardholder and sensitive data:

Symmetric Encryption (Data-at-Rest)

Algorithm	Minimum Key Size	Use Case
AES (GCM/CBC)	256-bit	Database encryption, backups, file system encryption
AES-XTS	256-bit	Disk/volume encryption (e.g., BitLocker, LUKS)

Asymmetric Encryption (Keys, TLS Handshakes, Certificates)

Algorithm	Minimum Key Size	Use Case
RSA	2048-bit (preferred 3072)	TLS certificates, key exchanges



ECC (Elliptic Curve)

P-256 (or higher)

TLS key exchange, JWT signing

ECDSA

P-256 or P-384

Digital signatures, HSM-stored certs

Hashing & Integrity

Algorithm	Minimum Standard	Use Case
SHA-256	Required	Digital signatures, checksum validation
HMAC-SHA-256	Required	API authentication, payload integrity
SHA-1 & MD5	DISALLOWED	Must not be used in any capacity

Key Derivation & Password Storage

Method	Description
PBKDF2, Argon2id, or bcrypt	Salted with minimum 10,000 iterations for authentication systems
HKDF	For deriving session keys from master keys

Transport Layer Security (TLS)

Control	Requirement
---------	-------------



Protocols	Allow: TLS 1.2 or TLS 1.3 only ; Disable SSL, TLS 1.0/1.1
Cipher Suites	Use ECDHE + AES-256-GCM; enforce Forward Secrecy
Certificate Authority	Use publicly trusted CAs or enterprise CA with CRL/OCSP

9. Key Management Lifecycle

Cryptographic keys must go through a controlled lifecycle consisting of:

9.1 Key Generation

- Keys generated using FIPS 140-2 compliant modules (AWS KMS, Azure Key Vault, HSMs)
- Must use true cryptographically secure random number generators (CSPRNG)

9.2 Key Distribution

- Keys are never transmitted in plaintext
- Symmetric keys distributed via secure channel (TLS 1.2+, SSH) or KMS API
- Asymmetric keys stored and accessed only via HSM or vaults

9.3 Key Storage

- Store master encryption keys in AWS KMS or HSM only
- Application keys stored in Vault, Parameter Store, or encrypted environment variables—never in code repositories or plaintext files

9.4 Key Rotation

- AES and RSA keys rotated **every 12 months**, or immediately if compromise is suspected
- TLS certificates renewed **every 12 months** or before expiry



- Key version control maintained, old keys archived securely for decryption needs

9.5 Key Revocation and Destruction

- Keys must be revoked if suspected of compromise, personnel departure, or system decommissioning
- Destroyed using cryptographic erase or HSM key purge mechanisms
- Destruction events must be logged and approved by CSCO

10. Protection of Cardholder Data in Transit

There is a mechanism to protect cardholder data during transmission over open, public networks, ensuring confidentiality, integrity, and protection from interception or tampering.

10.1 Approved Transmission Methods

Cardholder Data (CHD) and Sensitive Authentication Data (SAD) must only be transmitted using secure protocols:

Network Type	Approved Protocols	Disallowed Protocols
Public Internet	HTTPS (TLS 1.2/1.3), Secure WebSockets (WSS), SFTP, FTPS	HTTP, FTP, Telnet, SMTP without TLS
Remote Admin Access	SSH v2 with key-based auth, VPN with AES-256	Telnet, RDP without TLS
API Communication	Mutual TLS, OAuth 2.0 with JWT (signed), HMAC-SHA256	Plaintext tokens, Basic Auth without TLS

10.2 Required Security Controls

- TLS connections must be configured with:
 - **Minimum TLS 1.2**, TLS 1.3 preferred
 - **Forward secrecy** (ECDHE key exchange)



- Strong cipher suites (e.g., ECDHE-ECDSA-AES256-GCM-SHA384)
- Certificates must:
 - Be issued by a trusted Certificate Authority
 - Be renewed before expiration
 - Be monitored and auto-rotated via ACME, Certbot, or AWS Certificate Manager
- Public-facing services must enforce **HSTS (HTTP Strict Transport Security)**

11. Protection of Cardholder Data at Rest

All stored cardholder data must be encrypted to ensure confidentiality if unauthorized access occurs.

11.1 Storage Requirements

- Primary Account Numbers (PANs)** must be:
 - Encrypted using AES-256 or stronger
 - Tokenized wherever possible
 - Displayed only in truncated form (first 6, last 4 digits)
- SAD (e.g., CVV, PINs)** must **never be stored post-authorization**
- Logs, exports, memory dumps, debug data** must never contain unmasked or unencrypted PAN

11.2 Storage Locations & Controls

Storage Location	Encryption Method	Control
Databases (RDS, PostgreSQL, MySQL)	AES-256 Transparent Data Encryption (TDE)	Managed via AWS KMS key policy
File Systems / Application Servers	LUKS / BitLocker (AES-256)	Full disk encryption
Backups & Snapshots	AES-256 with KMS keys	Auto-deletion via lifecycle policies



Cloud Storage (S3, Azure Blob)

SSE-KMS or CMK encryption

Access restricted via IAM

12. Tokenization & Data Minimization

Orchestrate Global uses tokenization to avoid storing raw PANs in most environments.

Element	Description
Tokenization Service	Exchanges PAN for a token; PAN stored only in the token vault
Token	Random, irreversible reference to PAN; unusable outside token service
Token Vault	Encrypted at rest, hosted in isolated segment of CDE
Logging Rules	Logs never store PAN; only masked or tokenized values allowed
Data Minimization	Collect only the minimum account data necessary for operational or legal needs

13. Cryptographic Key Custodians & Segregation of Duties

To prevent abuse or collusion, cryptographic responsibilities are segregated:



Role	Access Limitation
Key Generator (DevOps)	Can generate KMS keys but cannot decrypt data
Key Custodian (Security Team)	Can request key revocation/rotation; cannot view raw keys
System Administrator	Can deploy applications but cannot access cryptographic keys
Auditor	Can review logs and key lifecycle reports but cannot modify configurations

No single individual should ever have end-to-end control of cryptographic creation, storage, and usage.

14. Cryptographic Failure Handling

When cryptographic controls fail or degrade:

Incident Type	Response
Certificate expired	Auto-renew via ACM or Let's Encrypt; service restart
Weak cipher suite detected	Disable via web server config; validate via SSL Labs
KMS/HSM outage	Failover to secondary KMS region; audit recoveries
Suspected key compromise	Immediate key revocation and rotation; forensic analysis



15. Cryptographic Hardware & Secure Key Storage

15.1 Approved Cryptographic Devices

All cryptographic operations involving sensitive keys must be performed using secure, tamper-resistant hardware wherever feasible.

Device Type	Purpose	Compliance Level
Cloud HSMs (e.g., AWS CloudHSM, Azure Managed HSM)	Secure generation and storage of master keys	FIPS 140-2 Level 3
AWS KMS / Azure Key Vault	Key management for application-level encryption	FIPS 140-2 Level 2
HSM-backed Token Vaults	Stores PAN mapping and token references	Segmented CDE environment
Hardware Security Tokens	Admin MFA and root key operations	FIDO2-certified

15.2 Physical & Logical Protection of HSMs

- HSM access requires MFA and dual authorization.
- HSM devices are geographically distributed across **at least two availability zones**.
- Physical HSMs (if applicable) are stored in **biometric-access controlled data centers**, monitored 24/7.
- **Tamper-evident seals** must be used; any sign of tampering is immediately escalated to the CSCO.

16. Key Backup, Rotation & Compromise Procedure



16.1 Key Backup

Key Type	Backup Location	Encryption
Master Encryption Keys (MEK)	Encrypted HSM cluster	AES-256 with KMS wrapping
Data Encryption Keys (DEK)	Never exported; re-generated if lost	N/A
Key Metadata	SmartComply GRC	Encrypted database

16.2 Rotation Policy

Key Type	Rotation Frequency
DEKs (used to encrypt CHD)	Every 12 months or upon suspected compromise
KEKs (wrap DEKs)	Every 24 months
TLS/SSL Certificates	90 days (Let's Encrypt) or 12 months (enterprise CA)
SSH Host Keys	Annually or after personnel turnover

All key rotation events must be logged and verified in the **Key Management Register**.

16.3 Key Compromise Response

If a cryptographic key is suspected to be compromised:



1. Immediate Actions

- Revoke affected key in KMS / HSM.
- Notify CSCO and Incident Response Team within **15 minutes**.

2. Containment

- Disable related access, rotate impacted keys.
- Force re-establishment of secure sessions.

3. Recovery

- Re-encrypt affected data using new DEK.
- Verify data integrity.

4. Audit Trail

- Log incident in SmartComply → "Crypto-Incident Register".
- File RCA within **5 business days**.

17. Secure Disposal of Cryptographic Keys

To prevent unauthorized recovery, all expired or decommissioned cryptographic material must be destroyed securely.

Key Disposal Method	Description
Cryptographic Erasure	Deleting or revoking key material in HSM/KMS so encrypted data becomes unreadable
Zeroization (Hardware)	Physically erasing HSM memory (as per NIST SP 800-88 & FIPS 140-2)
Multi-Person Approval	Requires two authorized individuals to sign disposal request
Documentation	Disposal logged with Key ID, timestamp, approvers, and verification outcome

All disposal events must be retained for **7 years** for audit purposes.



18. Logging, Monitoring & Auditing of Cryptographic Operations

18.1 Mandatory Logging

The following cryptographic events **must be logged** with timestamp, user identity, and outcome:

- Key creation, access, encryption, decryption, export, deletion
- TLS certificate generation and renewal
- Failed HSM authentication attempts
- Token vault access events

Logs are forwarded in real-time to the **SIEM (Splunk)** and stored for **minimum 12 months**.

18.2 Monitoring & Alerting

Event Type	Response SLA
5 failed HSM login attempts	Alert within 5 minutes
Unauthorized KMS API call	Incident response triggered immediately
Expiring certificates <15 days	Automatic alerts to DevOps & CSCO
Key tampering attempt	Full escalation to CISO & CEO

18.3 Audit & Review

- Quarterly crypto audits by Compliance & IT.
- Annual independent audit (e.g., PCI DSS Attestation of Compliance).
- Any deviation triggers corrective action within **30 days**.



19. Policy Review & Maintenance

Activity	Frequency	Owner
Full policy review	Annually or after major breach	CSCO
Update based on regulatory changes	Within 30 days	Compliance Team
Test cryptographic recovery	Twice per year	DevOps & Security
Staff re-training on this policy	Annually	HR & Compliance