



NETWORK SECURITY POLICY

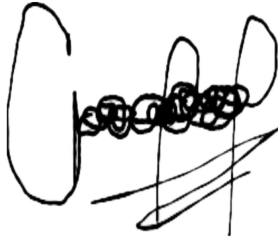
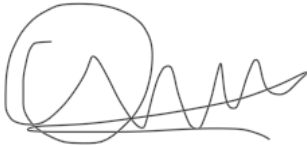
Revision History

Version	Date	Change Description	Author
1.0	17 September 2025	Initial Policy Documentation	Chief Security & Compliance Officer

Document Review & Approval

Next Scheduled Review: 17 September 2026

Distribution: All Employees, Contractors, and Authorized Third Parties

Name	Title	Signature	Date
Preston Obadan	Chief Executive Officer (CEO)		17 September 2025
Oleksii Bondarenko	Chief Security & Compliance Officer (CSCO)		14 September 2025



Kevin Kegera

Chief Commercial Officer
(CCO)

17 September 2025

1. INTRODUCTION

1.1 Purpose

This Network Security Policy establishes mandatory security requirements, roles, and technical controls governing the design, implementation, management, monitoring, and protection of Orchestrate Global's network infrastructure.

It aims to safeguard information assets—particularly cardholder data—across all Company-operated environments, whether on-premises, hybrid, or cloud-based (AWS, Azure, GCP).

This policy aligns with the following standards and frameworks:

- **PCI DSS v4.0**
- **ISO/IEC 27001:2022**
- **NIST Cybersecurity Framework (CSF)**
- **NIST SP 800-53, SP 800-123, SP 800-115**
- **CIS Critical Security Controls v8**

1.2 Scope

This policy applies to all:

Network Components

- Routers, switches, firewalls, load balancers, WAFs



- Cloud VPCs/VNets, transit gateways, peering connections
- Security groups, network ACLs, SD-WAN, API gateways
- VPN infrastructure, remote access servers

Endpoints & Systems

- Corporate devices: laptops, desktops, physical & virtual servers
- Mobile devices under MDM or corporate use (contractors included)
- IoT/OT devices connected to corporate infrastructure

Data Types

- **Cardholder Data (CHD):** PAN, cardholder names, CVV, track data (temporary if PCI exception applies)
- **Sensitive Authentication Data (SAD)**
- **Personally Identifiable Information (PII)**
- Internal business data, intellectual property, operational records

Personnel

- Full-time employees, contractors, consultants
- Managed Service Providers (MSPs) and third-party vendors with network or system access

Environments Covered

- **Production systems**
- **Staging & development networks**
- **Backup & disaster recovery environments**
- **Cardholder Data Environment (CDE)**

Exclusion: Public marketing websites are excluded if properly segmented and validated through penetration testing.



1.3 Objectives

The core objectives of this network security policy are:

Objective	Description
Confidentiality	Prevent unauthorized data access through encryption, segmentation, and IAM.
Integrity	Protect against unauthorized modification of data or network configurations via hashing, FIM, and change control.
Availability	Ensure continuous, reliable operation of systems via redundancy, DDoS mitigation, and DR plans.
Accountability	Ensure all user actions are traceable through logging, authentication, and non-repudiation.
Compliance	Maintain adherence to legal, regulatory, and contractual obligations (e.g., PCI DSS, GDPR).

2. ROLES AND RESPONSIBILITIES

Clear accountability is essential to ensure effective governance, secure network operations, and compliance with PCI DSS, ISO 27001, and NIST CSF.



Role

Key Responsibilities

Chief Executive Officer (CEO)

- Holds ultimate accountability for the organization's risk posture.
- Approves major security investments and policies.

Chief Security & Compliance Officer (CSCO)

- Owns this Network Security Policy.
- Oversees risk management, policy enforcement, data protection, and third-party security.
- Acts as Data Protection Officer (DPO) where legally required.

Chief Technology Officer (CTO)

- Ensures network architecture aligns with business and security objectives.
- Approves major infrastructure changes.

Director of Technology / Engineering Manager

- Manages day-to-day network operations and system performance.
- Ensures secure implementation of solutions and coordination with CSCO on risks.

Infrastructure Engineer

- Configures and maintains firewalls, VPNs, routing tables, DNS, DHCP, VPCs, subnets.
- Conducts log monitoring, vulnerability remediation, and network patching.

IT Compliance Officer

- Ensures adherence to PCI DSS, ISO 27001, GDPR, and internal security standards.



- Coordinates audits and manages Approved Scanning Vendor (ASV) reports.

Security Operations Center (SOC) Analysts

- Monitor SIEM, IDS/IPS, and network alerts 24/7.
- Respond to security incidents based on IR playbooks.

System Administrators

- Apply OS and network device hardening.
- Manage patching, user provisioning, and endpoint firewalls.

Software Engineers / DevOps

- Ensure secure configuration of CI/CD pipelines, IaC templates, and SDLC adherence.

All Employees / Contractors

- Must complete mandatory security awareness training.
- Protect passwords, prevent unauthorized access, report security incidents.

Note: Role-Based Access Control (RBAC) is maintained within the IAM system and reviewed quarterly.

3. NETWORK DESIGN & ARCHITECTURE PRINCIPLES

3.1 Zero Trust Architecture (ZTA)

Orchestrate Global adopts a **Zero Trust (“Never trust, always verify”)** security model:

- No implicit trust based on network location or user group.
- All access requests are authenticated, authorized, and encrypted.
- Micro-segmentation isolates sensitive workloads (e.g., CDE, Finance HR).
- Continuous monitoring and device posture checks (e.g., antivirus, OS patch level).



- Privileged access is granted using Just-in-Time (JIT) and Just-Enough Access (JEA).

3.2 Network Segmentation

To reduce risk and PCI DSS scope:

Environment

Segmentation Requirement

CDE (Cardholder Data Environment)

Must be isolated from all other networks using firewalls, VLANs, and security groups.

DMZ (Demilitarized Zone)

Only necessary inbound/outbound traffic allowed via reverse proxies, WAFs, or load balancers.

Corporate Network

Access to CDE granted only via MFA-enabled jump hosts or VPN gateways.

Development & Testing

Must remain separate from production unless explicit approval is given.

3.3 Cloud Network Security

All cloud-hosted systems (AWS, Azure, GCP) must comply with the following:

- No public IP addresses assigned to CDE systems.
- VPCs/VNets must use private subnets and secure peering (e.g., AWS PrivateLink, Transit Gateway).
- Security Groups and Network ACLs must implement **default deny (deny-all)** rules unless explicitly allowed.
- Use of cloud-native firewalls (AWS Network Firewall, Azure Firewall, GCP Firewall Rules).



- Management interfaces must be accessible only through VPN or bastion hosts.
- Logging must be enabled (VPC Flow Logs, AWS CloudTrail, Azure NSG Flow Logs).

3.4 Network Documentation & Diagrams

Type	Description	Review Frequency
High-Level Network Diagram (HLD)	Shows trust boundaries, CDE scope, data flows, VPNs, internet gateways	Annually or after major change
Low-Level Diagram (LLD)	Includes subnets, IP address ranges, VLANs, firewalls, routes, device inventory	Updated in real-time via CMDB
Storage Location	Maintained in SharePoint / Confluence with version control	Access restricted to authorized roles

3.5 Hardening & Secure Configuration Standards

All network and system devices must follow CIS, NIST, and SANS hardening standards:

Requirements include:

- Disable unused ports, protocols, and services (e.g., Telnet, SMBv1, FTP, SNMPv1).
- Enforce SSHv2 or TLS 1.2+ for management access.
- Default admin passwords must be changed before deployment.
- Apply critical patches within 14 days; all other patches within 30 days.
- Enable logging and synchronize time via NTP.



4. ACCESS CONTROL

Access to Orchestrate Global's network resources must be controlled based on the principles of **least privilege**, **role-based access control (RBAC)**, and **need-to-know** as required by PCI DSS and ISO 27001.

4.1 Authentication & Authorization

Mandatory Requirements:

- **Multi-Factor Authentication (MFA)** is required for:
 - Remote access (VPN, SSH, RDP, cloud consoles)
 - Administrative and privileged accounts
 - Access to CDE systems or databases containing PII
- **Password Policy:**
 - Minimum 12 characters (Privileged Accounts: 15+)
 - Must include uppercase, lowercase, number, and special character
 - Expire every 90 days (60 days for privileged users)
 - Minimum 5 previous passwords remembered (no reuse)
- **Service Accounts:**
 - Must not be shared
 - Managed via Privileged Access Management (PAM) solutions
 - Password/keys rotated every 90 days or after employee offboarding



4.2 Remote Access Security

Requirement

Control

Remote Access Method	Must use company-managed VPN (OpenVPN, Cisco AnyConnect, Zscaler Private Access)
Encryption Standard	All remote sessions must use TLS 1.2+ or SSHv2
Split Tunneling	Disabled for VPN connections
Device Compliance	Only company-approved or MDM-managed devices may connect
Session Timeout	Sessions auto-disconnect after 15 minutes of inactivity
Logging	VPN logs must include username, source IP, timestamps, MFA result

4.3 User Provisioning & Deprovisioning

- All access must be requested via HR or department manager and approved by CSCO or CTO.
- Accounts must be:
 - **Created** only after identity verification and role validation.
 - **Disabled within 1 hour** of employee termination.
 - **Reviewed quarterly** to remove dormant accounts or excessive privileges.



- Access control lists (ACLs), IAM roles, and firewall policies must be updated immediately when users change departments or roles.

4.4 Cardholder Data Environment (CDE)

Access

- Only authorized personnel may access CDE under **strict RBAC and MFA**.
- All administrative access must occur through secured jump servers/bastion hosts.
- Direct database access to PAN or CVV data is prohibited unless explicitly approved by CSCO.
- All access must be logged and retained for **a minimum of 1 year**.

5. SECURITY MONITORING & LOGGING

5.1 Logging Requirements

All network devices, servers, cloud services, and security systems must forward logs to a centralized **Security Information and Event Management (SIEM)** system.

Log Source	Minimum Retention	Content Required
Firewall, IDS/IPS	1 year (3 years for CDE)	Source/Dest IP, port, action, timestamp
VPN/Auth Logs	1 year	Username, IP, session duration, MFA success/failure
Server OS Logs	90 days (1 year for production)	User logins, privilege escalations, service starts



File Integrity Monitoring (FIM)	1 year	File path, hash change, user/process responsible
Cloud Logs (AWS CloudTrail/Azure Activity Logs)	1 year	API actions, IAM changes, network config changes

Time synchronization: All systems must use centralized **NTP servers** to maintain accurate timestamps.

5.2 Intrusion Detection & Prevention (IDS/IPS)

- Network-based IDS/IPS must monitor traffic at all entry/exit points of the CDE.
- IDS/IPS rules updated weekly from vendor and threat intelligence feeds.
- All **critical alerts must be reviewed within 5 minutes** by SOC Analysts.
- Alerts requiring incident response trigger activation of the Incident Response Plan.

5.3 File Integrity Monitoring (FIM)

FIM must be configured on all systems that store, process, or transmit cardholder data.

It must:

- Monitor OS system files, registry keys, configuration files, web server directories.
- Compare files to known-good cryptographic hashes daily or in real-time.
- Send alerts to SIEM for SOC review.
- Retain records of FIM alerts for **minimum 12 months**.

6. CHANGE & CONFIGURATION MANAGEMENT



6.1 Change Control Process

All network changes must follow this process:

1. **Request Submission** (via Jira/ServiceNow)
2. **Impact & Risk Analysis** (Security, CDE impact considered)
3. **Approval** (CTO or delegated Change Advisory Board)
4. **Testing in non-production environment**
5. **Scheduled implementation window**
6. **Post-implementation validation**
7. **Documentation updated (CMDB, diagrams, firewall rules)**
8. **Emergency changes** → must be reviewed within 72 hours post-implementation

6.2 Configuration Management & Drift Prevention

- All cloud infrastructure must be deployed using **Infrastructure-as-Code (IaC)** tools (Terraform, AWS CloudFormation).
- IaC templates must be scanned using **tfsec/Checkov** before deployment.
- Manual changes to production network devices or cloud configurations are prohibited unless approved through emergency change protocol.
- Backups of firewall configs, router settings, and switch configurations must be taken daily and stored securely.

7. VULNERABILITY MANAGEMENT & PENETRATION TESTING

7.1 Vulnerability Scanning

Type	Frequency	Conducted By	Scope
------	-----------	--------------	-------



External Scans	Quarterly + after significant change	PCI SSC Approved Scanning Vendor (ASV)	All public-facing IPs and CDE perimeter
Internal Scans	Quarterly + after significant change	Internal Security Team or Qualified Third Party	All internal systems incl. CDE, cloud, corporate network
Cloud Posture Scanning	Continuous (daily/weekly)	Automated CSPM tools (e.g., Prisma, Wiz, AWS Security Hub)	AWS, Azure, GCP configurations

Policy Requirements:

- All scans must produce “passing” results (no CVSS score ≥ 4.0).
- Vulnerabilities with:
 - **CVSS ≥ 9.0 (Critical):** Remediated within 14 days
 - **CVSS 7.0–8.9 (High):** Remediated within 30 days
 - **CVSS < 7.0 (Medium/Low):** Addressed per risk priority
- Rescans must validate remediation.
- All results retained for **minimum 24 months**.

7.2 Penetration Testing

Mandatory Requirements:

- Conducted **at least annually** or after significant infrastructure/application changes.
- Must cover:
 - **Network-layer testing** (internal + external)
 - **Application-layer testing** (aligned to OWASP Top 10)



- **Segmentation testing** to confirm isolation of CDE from non-CDE networks
- Testing methodologies must follow:
 - NIST SP 800-115
 - PCI DSS Requirement 11.4
 - PTES / OSSTMM framework

Qualified Testers:

External firms must have **OSCP, CREST, GIAC** or equivalent certifications. Internal testing allowed only if independence is maintained.

7.3 Wireless Security

- Quarterly scans for rogue access points using tools like **AirMagnet, Ekahau, or Cisco Prime**.
- Unauthorized devices must be immediately disconnected, investigated, and reported to CSCO.
- Wireless networks handling CHD must use:
 - WPA3 Enterprise **or** WPA2 Enterprise with RADIUS + certificate-based authentication
 - Unique credentials per user (no shared Wi-Fi passwords)

8. INCIDENT RESPONSE & SECURITY EVENT MANAGEMENT

8.1 Incident Response Process

All network or security incidents must follow the **Incident Response Plan (IRP)** which includes:

1. **Identification** → Detection via SIEM, IDS/IPS, FIM alerts.
2. **Containment** (within 15 minutes for critical incidents)
3. **Eradication** → Remove malicious code, disable compromised credentials



4. **Recovery** → Restore operations using backups or redeployment
5. **Lessons Learned** → Root cause analysis & documentation within 5 business days

Forensic Evidence: Must be preserved for at least **6 months** for potential legal/audit investigation.

8.2 Incident Reporting Obligations

Incident Type

Notification Requirement

PCI Cardholder Data Breach

PCI SSC, acquiring bank, and affected clients within 72 hours

GDPR Personal Data Breach

Supervisory Authority & affected individuals within 72 hours

System Outage > 1 hour affecting CDE

CTO and CSCO must be notified immediately

Third-party/vendor breach

Vendor must notify Orchestrate Global within 24 hours per contract

9. AUDIT & COMPLIANCE MANAGEMENT

9.1 Internal Audits

- Conducted **biannually** by the IT Compliance Officer or Internal Audit function.
- Must evaluate compliance with PCI DSS Requirement 1 (Network Security), 7 (Access Control), 10 (Logging), and 11 (Testing).



- Findings tracked in the GRC platform until remediation.

9.2 External Audits

- **Annual PCI DSS Report on Compliance (ROC) or SAQ D** (if applicable)
- **ISO/IEC 27001** surveillance audit (if certified)
- **Penetration test and ASV scan reports** must be available for QSA review

10. POLICY COMPLIANCE & ENFORCEMENT

10.1 Enforcement

Non-compliance with this policy may result in:

- Revocation of user privileges
- Mandatory retraining
- Disciplinary action up to termination
- Legal or financial penalties if negligence leads to a data breach

10.2 Exceptions

- Any deviation requires **written approval from CSCO and CTO**
- Must include risk justification, compensating controls, and expiration date
- Maximum exception period: **90 days**

11. POLICY REVIEW & MAINTENANCE

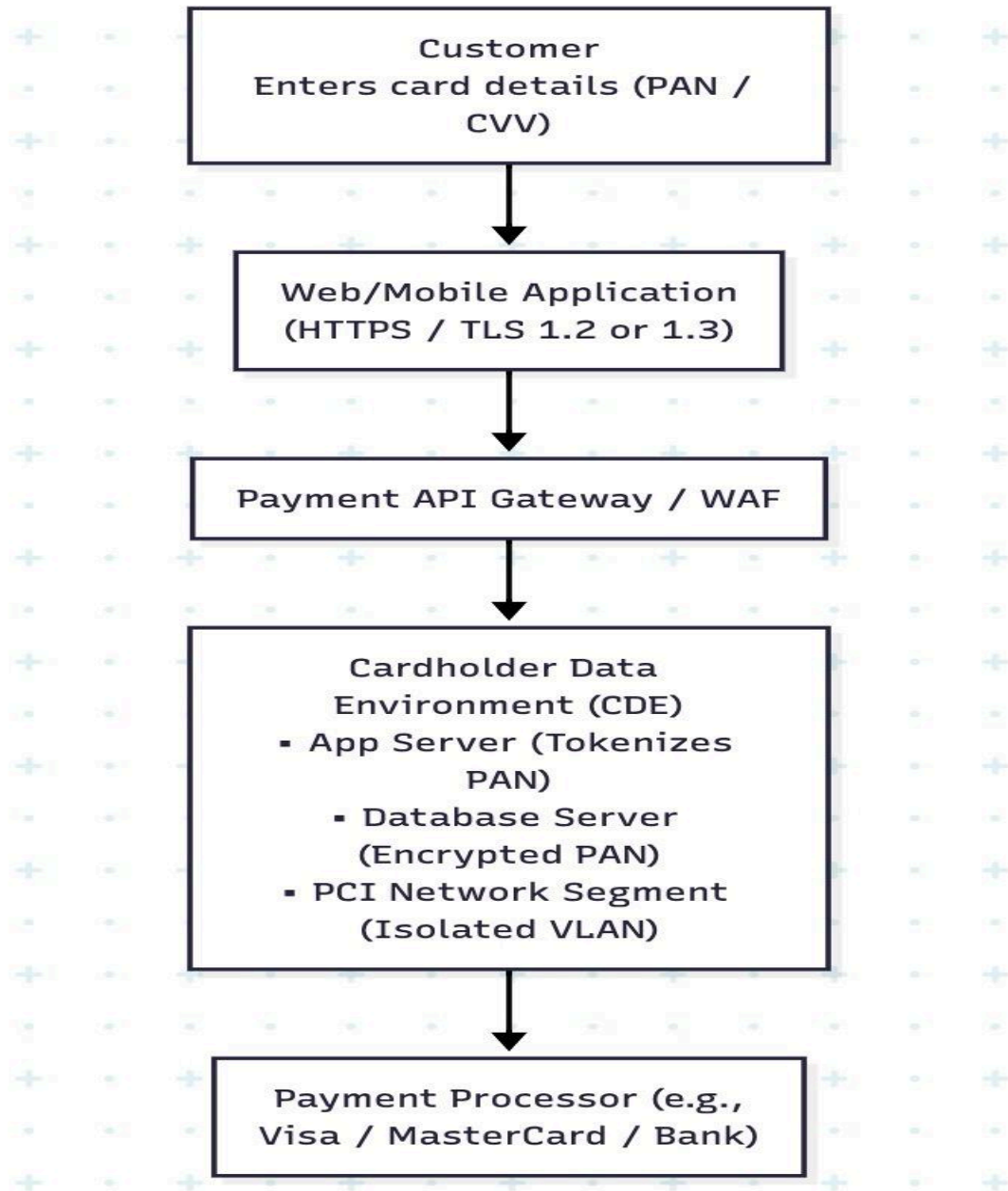
This policy shall be reviewed under the following conditions:



Trigger	Example
Scheduled review	Annually (next on 17 September 2026)
Significant security incident	Network breach, ransomware attack
Regulatory changes	PCI DSS updates, GDPR amendments
Major architecture change	Cloud migration, data center move



12. CARDHOLDER DATA FLOW DIAGRAM





13. HIGH-LEVEL NETWORK DIAGRAM

