Contents

Chapter 1

PCI-DSS Compliance Handbook

Document Metadata

- **Created on:** 2026-02-10
- **Author:** Andreas Huemmer [andreas.huemmer@adminsend.de]
- **Version:** 0.0.5
- **Type:** PCI-DSS Handbook

---

ewpage

Chapter 2

Scope and CDE Definition

Document ID: PCI-0010
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

2.1 1. Purpose

This document defines the scope of PCI-DSS compliance for AdminSend GmbH and describes the Cardholder Data Environment (CDE).

2.1.1 1.1 Objectives

- **Scope Definition:** Clear delineation of the CDE from the rest of the network
- **Compliance Focus:** Identification of all PCI-DSS-relevant systems and processes
- **Risk Minimization:** Reduction of compliance scope through segmentation
- **Audit Preparation:** Documentation for QSA assessments

2.1.2 1.2 References

- **PCI-DSS v4.0:** Requirements 1, 2, 11, 12
- **PCI-DSS Information Supplement:** Guidance for PCI DSS Scoping and Network Segmentation
- **PA-DSS:** Payment Application Data Security Standard (if applicable)

2.2 2. Merchant/Service Provider Information

2.2.1 2.1 Organization Information

Organization: AdminSend GmbH
Address: Musterstraße 123, 80331 München
Country: Deutschland
Website: https://www.adminsend.de

2.2.2 2.2 PCI-DSS Classification

Merchant Level: [TODO: Level 1/2/3/4]
Service Provider Level: [TODO: Level 1/2 or N/A]
Merchant ID: {{ meta.pci.merchant_id }}
Service Provider ID: {{ meta.pci.service_provider_id }}

Transaction Volume (annual): - Visa: [TODO: Number of transactions] - Mastercard: [TODO: Number of transactions] - American Express: [TODO: Number of transactions] - Discover: [TODO: Number of transactions] - Total: [TODO: Number of transactions]

2.2.3 2.3 Acquiring Banks

Bank Name	Contact	Merchant ID	Card Brands
[TODO: Bank 1]	[TODO: Contact]	[TODO: ID]	Visa, Mastercard
[TODO: Bank 2]	[TODO: Contact]	[TODO: ID]	American Express

2.3 3. Cardholder Data Environment (CDE)

2.3.1 3.1 CDE Definition

The Cardholder Data Environment (CDE) includes:

1. **Systems:** All systems that store, process, or transmit cardholder data (CHD)
2. **Networks:** All network segments connected to CDE systems
3. **People:** All employees and service providers with access to CHD
4. **Processes:** All business processes involving CHD

2.3.2 3.2 Cardholder Data (CHD)

Primary Account Number (PAN): - 13-19 digit card number - **Storage:** [TODO: Yes/No, where?] - **Encryption:** [TODO: Algorithm, e.g., AES-256]

Cardholder Name: - Name of cardholder - **Storage:** [TODO: Yes/No, where?]

Service Code: - 3-digit code on magnetic stripe - **Storage:** [TODO: Yes/No, where?]

Expiration Date: - Card validity date - **Storage:** [TODO: Yes/No, where?]

2.3.3 3.3 Sensitive Authentication Data (SAD)

MUST NOT be stored after authorization:

- **Full Track Data:** Magnetic stripe data (Track 1, Track 2)
- **CAV2/CVC2/CVV2/CID:** Card verification value (3-4 digits)
- **PIN/PIN Block:** PIN data

Confirmation: AdminSend GmbH does NOT store Sensitive Authentication Data after authorization. [TODO: Confirm]

2.4 4. CDE Systems and Components

2.4.1 4.1 Systems in CDE

System ID	System Name	Type	Function	CHD Type	Location
[TODO: SYS-001]	[TODO: Payment Gateway]	Server	Payment processing	PAN, Name	[TODO: DC1]
[TODO: SYS-002]	[TODO: POS Terminal]	Endpoint	Card input	PAN	[TODO: Branch 1]
[TODO: SYS-003]	[TODO: Database]	Database	CHD storage	PAN (encrypted)	[TODO: DC1]
[TODO: SYS-004]	[TODO: Web Server]	Server	E-Commerce	PAN (transit)	[TODO: DC1]

2.4.2 4.2 Network Components in CDE

Component	Type	Function	Location
[TODO: FW-CDE-01]	Firewall	CDE segmentation	[TODO: DC1]
[TODO: SW-CDE-01]	Switch	CDE network	[TODO: DC1]
[TODO: RTR-CDE-01]	Router	CDE routing	[TODO: DC1]
[TODO: IDS-CDE-01]	IDS/IPS	Intrusion detection	[TODO: DC1]

2.4.3 4.3 Applications in CDE

Application	Version	Vendor	PA-DSS Certified	Function
[TODO: Payment App]	[TODO: v2.1]	[TODO: Vendor]	[TODO: Yes/No]	Payment processing
[TODO: POS Software]	[TODO: v3.0]	[TODO: Vendor]	[TODO: Yes/No]	Point of sale
[TODO: E-Commerce]	[TODO: v1.5]	[TODO: Vendor]	[TODO: Yes/No]	Online shop

2.5 5. Locations

2.5.1 5.1 Physical Locations with CDE

Location ID	Location Name	Address	CDE Systems	Staff with CHD Access
[TODO: LOC-01]	Headquarters	[TODO: Address]	[TODO: List]	[TODO: Number]
[TODO: LOC-02]	Data Center	[TODO: Address]	[TODO: List]	[TODO: Number]
[TODO: LOC-03]	Branch 1	[TODO: Address]	[TODO: POS]	[TODO: Number]

2.5.2 5.2 Remote Access to CDE

Remote Access Allowed: [TODO: Yes/No]

If yes: - **Access Method:** [TODO: VPN, Jump Server, etc.] - **Multi-Factor Authentication:** [TODO: Yes/No, Method] - **Authorized Users:** [TODO: Roles/Persons]

2.6 6. Data Flows

2.6.1 6.1 Cardholder Data Flows

[TODO: Insert data flow diagram - see PCI-0040]

Main Data Flows:

1. **Card Input → Authorization:**
   - Source: [TODO: POS Terminal/Web Form]
   - Destination: [TODO: Payment Gateway]
   - Protocol: [TODO: TLS 1.2+]
   - Encryption: [TODO: Yes/No]
2. **Authorization → Storage:**
   - Source: [TODO: Payment Gateway]
   - Destination: [TODO: Database]
   - Encryption: [TODO: AES-256]
   - Tokenization: [TODO: Yes/No]
3. **Reporting/Query:**
   - Source: [TODO: Database]
   - Destination: [TODO: Reporting System]
   - Masking: [TODO: Yes, last 4 digits only]

2.6.2 6.2 External Connections

Connection	Source	Destination	Purpose	Encryption
[TODO: Acquiring Bank]	CDE	Bank	Authorization	TLS 1.2+
[TODO: Payment Processor]	CDE	Processor	Processing	TLS 1.2+
[TODO: ASV Scans]	Internet	CDE	Vulnerability scans	N/A

2.7 7. Scope Exclusions

2.7.1 7.1 Systems Outside CDE

The following systems are NOT part of the CDE:

System	Justification	Segmentation
[TODO: Intranet]	No CHD processing	Firewall separation
[TODO: Email Server]	No CHD storage	Separate VLAN
[TODO: Development]	No production data	Physically separated

2.7.2 7.2 Excluded Locations

[TODO: List locations that do not process CHD]

2.8 8. Network Segmentation

2.8.1 8.1 Segmentation Strategy

Segmentation Method: [TODO: VLAN, Firewall, physical separation]

CDE Segments: - **CDE-Core:** Systems with CHD storage - **CDE-DMZ:** Systems with CHD transit (no storage) - **Management:** Administrative systems for CDE

Non-CDE Segments: - **Corporate:** Office network - **Guest:** Guest WiFi - **Development:** Development environment

2.8.2 8.2 Segmentation Validation

Last Validation: [TODO: Date]
Performed by: [TODO: Name/Company]
Method: [TODO: Penetration test, Network scan]
Result: [TODO: Successful/Failed]
Next Validation: [TODO: Date]

2.9 9. Personnel with CDE Access

2.9.1 9.1 Roles with CHD Access

Role	Number of People	Access Level	Justification
[TODO: Payment Admin]	[TODO: 2]	Full	Administration
[TODO: Cashier]	[TODO: 10]	Limited	POS operation
[TODO: Support]	[TODO: 3]	Query only	Customer service

2.9.2 9.2 Service Providers with CDE Access

Service Provider	Purpose	Access Method	PCI-DSS Status
[TODO: Payment Processor]	Payment processing	API	AOC available
[TODO: Hosting Provider]	Server hosting	Remote admin	AOC available
[TODO: QSA]	Audit	On-site	N/A

2.10 10. Scope Changes

2.10.1 10.1 Change Management

Process for Scope Changes:

1. **Identification:** New systems/processes with CHD
2. **Assessment:** Check PCI-DSS relevance
3. **Documentation:** Update scope document
4. **Approval:** CISO approval required
5. **Implementation:** Apply PCI-DSS controls

2.10.2 10.2 Change History

Date	Change	Justification	Approved by
[TODO: 2026-01-15]	New POS system	Branch expansion	[TODO: CISO]
[TODO: 2026-02-01]	Tokenization	Scope reduction	[TODO: CISO]

2.11 11. Compliance Responsibilities

2.11.1 11.1 Responsible Persons

PCI-DSS Program Manager: [TODO: Name] ([TODO: Email])
CISO: {{ meta.roles.ciso.name }} ({{ meta.roles.ciso.email }})
IT Manager: [TODO: Name] ([TODO: Email])
QSA (Qualified Security Assessor): [TODO: Company/Name]
ASV (Approved Scanning Vendor): [TODO: Company]

2.11.2 11.2 RACI Matrix

Activity	PCI Manager	CISO	IT Manager	QSA
Scope definition	A	C	R	I
Network segmentation	C	A	R	I
Compliance monitoring	R	A	C	I
Annual assessment	C	A	I	R

Legend: R = Responsible, A = Accountable, C = Consulted, I = Informed

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initial creation

ewpage

Chapter 3

Network Segmentation

Document ID: PCI-0020
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

3.1 1. Purpose

This document describes the network segmentation used to isolate the Cardholder Data Environment (CDE) from the rest of the corporate network.

3.1.1 1.1 Objectives

- **Scope Reduction:** Minimize PCI-DSS-relevant systems
- **Risk Minimization:** Limit potential attack surfaces
- **Compliance:** Meet PCI-DSS Requirement 1
- **Security:** Protect cardholder data through network isolation

3.2 2. Network Architecture

3.2.1 2.1 Network Segments

CDE Segments:

Segment ID	Segment Name	VLAN ID	IP Range	Purpose
[TODO: CDE-CORE]	CDE Core	[TODO: 100]	[TODO: 10.1.100.0/24]	CHD Storage

Segment ID	Segment Name	VLAN ID	IP Range	Purpose
[TODO: CDE-DMZ]	CDE DMZ	[TODO: 101]	[TODO: 10.1.101.0/24]	CHD Transit
[TODO: CDE-MGMT]	CDE Management	[TODO: 102]	[TODO: 10.1.102.0/24]	CDE Administration

Non-CDE Segments:

Segment ID	Segment Name	VLAN ID	IP Range	Purpose
[TODO: CORP]	Corporate	[TODO: 10]	[TODO: 10.1.10.0/24]	Office Network
[TODO: GUEST]	Guest	[TODO: 20]	[TODO: 10.1.20.0/24]	Guest WiFi
[TODO: DEV]	Development	[TODO: 30]	[TODO: 10.1.30.0/24]	Development

3.2.2 2.2 Network Diagram

[TODO: Insert network diagram - see diagrams/network_segmentation.png]

```
Internet
    |
[Perimeter Firewall]
    |
    +--- [CDE-DMZ] --- [CDE Firewall] --- [CDE-CORE]
    |                                          |
    |                                     [CDE-MGMT]
    |
    +--- [Corporate Network]
    |
    +--- [Guest Network]
    |
    +--- [Development Network]
```

3.3 3. Firewall Configuration

3.3.1 3.1 Firewall Overview

Firewall ID	Type	Location	Function	Vendor/Model
[TODO: FW-PERIMETER]	Perimeter	[TODO: DC1]	Internet Border	[TODO: Vendor/Model]
[TODO: FW-CDE]	Internal	[TODO: DC1]	CDE Segmentation	[TODO: Vendor/Model]
[TODO: FW-MGMT]	Internal	[TODO: DC1]	Management Access	[TODO: Vendor/Model]

3.3.2 3.2 Firewall Rules (CDE Segmentation)

Basic Principle: Default Deny (all connections blocked by default)

3.3.2.1 3.2.1 Inbound Connections to CDE

Rule ID	Source	Destination	Port/Protocol	Purpose	Approved By
[TODO: FW-001]	Internet	CDE-DMZ	443/TCP	HTTPS E-Commerce	[TODO: CISO]
[TODO: FW-002]	Corporate	CDE-MGMT	22/TCP	SSH Admin	[TODO: CISO]
[TODO: FW-003]	Acquiring Bank	CDE-CORE	443/TCP	Payment API	[TODO: CISO]

3.3.2.2 3.2.2 Outbound Connections from CDE

Rule ID	Source	Destination	Port/Protocol	Purpose	Approved By
[TODO: FW-101]	CDE-CORE	Acquiring Bank	443/TCP	Authorization	[TODO: CISO]
[TODO: FW-102]	CDE-CORE	Update Server	443/TCP	Security Updates	[TODO: CISO]
[TODO: FW-103]	CDE-MGMT	SIEM	514/TCP	Log Forwarding	[TODO: CISO]

3.3.2.3 3.2.3 Blocked Connections

Explicitly blocked: - CDE → Corporate Network (except Management) - Corporate → CDE (except authorized admin access) - CDE → Internet (except explicitly allowed services) - Guest → CDE (all connections)

3.3.3 3.3 Firewall Rule Review

Review Interval: Quarterly
Responsible: [TODO: Network Security Team]
Last Review: [TODO: Date]
Next Review: [TODO: Date]

Review Process: 1. Review all firewall rules 2. Identify unused rules 3. Validate business justification 4. Document changes 5. CISO approval

3.4 4. Router Configuration

3.4.1 4.1 Router Overview

Router ID	Location	Function	Vendor/Model
[TODO: RTR-CORE]	[TODO: DC1]	Core Routing	[TODO: Vendor/Model]

Router ID	Location	Function	Vendor/Model
[TODO: RTR-CDE]	[TODO: DC1]	CDE Routing	[TODO: Vendor/Model]

3.4.2 4.2 Access Control Lists (ACLs)

[TODO: Document router ACLs similar to firewall rules]

3.5 5. Segmentation Validation

3.5.1 5.1 Validation Methods

Annual validation required (PCI-DSS Req 11.4.6):

1. **Penetration Testing:**
   - Attempt to bypass CDE segmentation
   - Test firewall rules
   - Validate network isolation
2. **Network Scans:**
   - Port scans from different segments
   - Reachability tests
   - Routing validation
3. **Configuration Review:**
   - Review firewall configurations
   - Check router ACLs
   - VLAN configuration validation

3.5.2 5.2 Validation History

Date	Method	Performed By	Result	Actions
[TODO: 2025-12-01]	Penetration Test	[TODO: Company]	Successful	None
[TODO: 2025-06-15]	Network Scan	[TODO: Team]	1 Vulnerability	Rule FW-042 removed

3.5.3 5.3 Next Validation

Planned Date: [TODO: Date]
Method: [TODO: Penetration Test/Scan]
Performing Company: [TODO: Name]

3.6 6. Wireless Networks

3.6.1 6.1 Wireless Segmentation

Wireless Networks:

SSID	Segment	Encryption	CDE Access	Purpose
[TODO: Corp-WiFi]	Corporate	WPA3-Enterprise	No	Employees
[TODO: Guest-WiFi]	Guest	WPA3-Personal	No	Guests
[TODO: CDE-WiFi]	CDE-MGMT	WPA3-Enterprise + MFA	Yes	CDE Admin

Important: Wireless networks with CDE access require: - WPA3 or higher - Multi-Factor Authentication - Separate VLAN segmentation - Encrypted transmission

3.6.2 6.2 Wireless Access Points

AP ID	Location	SSID	Segment	Firmware Version
[TODO: AP-001]	[TODO: Office]	Corp-WiFi	Corporate	[TODO: v2.1]
[TODO: AP-002]	[TODO: DC]	CDE-WiFi	CDE-MGMT	[TODO: v2.1]

3.7 7. Remote Access

3.7.1 7.1 VPN Configuration

VPN Access to CDE:

VPN Type	Target Group	Authentication	Target Segment	Encryption
[TODO: SSL-VPN]	Administrators	MFA (Token)	CDE-MGMT	TLS 1.3
[TODO: IPSec-VPN]	Service Providers	MFA (Certificate)	CDE-MGMT	AES-256

VPN Requirements: - Multi-Factor Authentication (MFA) required - Encryption: TLS 1.2+ or IPSec with AES-256 - Session timeout: [TODO: 15 minutes inactivity] - Logging of all VPN connections

3.7.2 7.2 Jump Server / Bastion Hosts

Jump Server for CDE Access:

Server ID	Location	Function	Access Method
[TODO: JUMP-01]	CDE-MGMT	Admin Access	SSH/RDP via VPN

Jump Server Requirements: - No direct Internet connection - Access only via VPN with MFA - Complete logging of all sessions - No local data storage

3.8 8. Monitoring and Alerting

3.8.1 8.1 Network Monitoring

Monitored Metrics: - Firewall rule violations - Unexpected connection attempts to CDE - Changes to firewall configurations - Network traffic anomalies

Monitoring Tools: - [TODO: SIEM System] - [TODO: Network Monitoring Tool] - [TODO: IDS/IPS]

3.8.2 8.2 Alerting Rules

Alert ID	Condition	Severity	Notification
[TODO: ALT-001]	Connection from Corporate to CDE-CORE	Critical	SOC + CISO
[TODO: ALT-002]	Firewall rule change	High	Network Team
[TODO: ALT-003]	Failed VPN login (3x)	Medium	Security Team

3.9 9. Change Management

3.9.1 9.1 Change Process

Process for Network Changes:

1. **Change Request:** Formal request with justification
2. **Security Review:** Assessment of PCI-DSS impact
3. **Testing:** Test in non-production environment
4. **Approval:** CISO approval for CDE changes
5. **Implementation:** Execute with rollback plan
6. **Documentation:** Update this document
7. **Validation:** Verify segmentation

3.9.2 9.2 Change History

Date	Change	Justification	Approved By	Validated
[TODO: 2026-01-15]	New firewall rule FW-105	Payment API	[TODO: CISO]	Yes

---

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 4

Roles and Responsibilities

Document ID: PCI-0030
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

4.1 1. Purpose

This document defines the roles, responsibilities, and accountabilities for PCI-DSS compliance at AdminSend GmbH.

4.1.1 1.1 Objectives

- **Clear Responsibilities:** Unambiguous assignment of PCI-DSS tasks
- **Accountability:** Establishment of decision-making authority
- **Compliance:** Meet PCI-DSS Requirement 12.4
- **Communication:** Transparent communication channels

4.2 2. Organizational Structure

4.2.1 2.1 Executive Management

Chief Executive Officer (CEO): - **Name:** {{ meta.roles.ceo.name }} - **Email:** {{ meta.roles.ceo.email }} - **Phone:** {{ meta.roles.ceo.phone }}

Responsibilities: - Overall responsibility for PCI-DSS compliance - Approval of PCI-DSS budget - Approval of information security policy - Escalation point for critical compliance issues

Chief Information Security Officer (CISO): - **Name:** {{ meta.roles.ciso.name }} - **Email:** {{ meta.roles.ciso.email }} - **Phone:** {{ meta.roles.ciso.phone }}

Responsibilities: - Leadership of PCI-DSS compliance program - Approval of security policies and standards - Oversight of compliance activities - Reporting to executive management - Approval of exceptions (risk acceptance)

4.2.2 2.2 PCI-DSS Program Management

PCI-DSS Program Manager: - **Name:** [TODO: Name] - **Email:** [TODO: Email] - **Phone:** [TODO: Phone]

Responsibilities: - Day-to-day management of PCI-DSS program - Coordination of all compliance activities - Preparation for audits and assessments - Maintenance of PCI-DSS documentation - Training coordination - Liaison to QSA and acquiring banks

PCI-DSS Compliance Team: - **Members:** [TODO: List of team members]

Responsibilities: - Support of program manager - Execution of compliance checks - Documentation of evidence - Coordination with business units

4.2.3 2.3 IT and Operations

Chief Information Officer (CIO): - **Name:** {{ meta.roles.cio.name }} - **Email:** {{ meta.roles.cio.email }} - **Phone:** {{ meta.roles.cio.phone }}

Responsibilities: - Responsibility for IT infrastructure and systems - Approval of IT changes in CDE - Provision of resources for PCI-DSS compliance - Escalation point for IT-related compliance issues

IT Security Manager: - **Name:** [TODO: Name] - **Email:** [TODO: Email] - **Phone:** [TODO: Phone]

Responsibilities: - Implementation of security controls - Management of firewalls and network segmentation - Patch management and vulnerability management - Incident response - Log monitoring and analysis

System Administrators: - **Count:** [TODO: Count] - **Contact:** [TODO: Team email]

Responsibilities: - Administration of CDE systems - Execution of security updates - Backup and recovery - Compliance with hardening standards

Network Administrators: - **Count:** [TODO: Count] - **Contact:** [TODO: Team email]

Responsibilities: - Management of network components - Firewall configuration and maintenance - Network segmentation - VPN management

4.2.4 2.4 Application Development

Development Manager: - **Name:** [TODO: Name] - **Email:** [TODO: Email] - **Phone:** [TODO: Phone]

Responsibilities: - Secure software development (Secure SDLC) - Code reviews and security testing - Compliance with secure coding standards - Vulnerability management in applications

Developers: - **Count:** [TODO: Count] - **Contact:** [TODO: Team email]

Responsibilities: - Development of secure applications - Participation in security training - Remediation of security vulnerabilities - Documentation of applications

4.2.5 2.5 Business Operations

Operations Manager: - **Name:** [TODO: Name] - **Email:** [TODO: Email] - **Phone:** [TODO: Phone]

Responsibilities: - Business processes involving cardholder data - Training of employees - Compliance with operational procedures - Incident reporting

Store/Branch Managers: - **Count:** [TODO: Count] - **Contact:** [TODO: Contact list]

Responsibilities: - Physical security at locations - Training of cashiers/POS operators - Compliance with PCI-DSS procedures - Reporting of security incidents

4.2.6 2.6 Human Resources

HR Manager: - **Name:** [TODO: Name] - **Email:** [TODO: Email] - **Phone:** [TODO: Phone]

Responsibilities: - Background checks for employees with CDE access - Onboarding and offboarding - Training coordination - Non-disclosure agreements (NDAs)

4.2.7 2.7 Legal and Compliance

Legal Counsel: - **Name:** [TODO: Name] - **Email:** [TODO: Email] - **Phone:** [TODO: Phone]

Responsibilities: - Legal advice on PCI-DSS - Contract review (service providers) - Data protection and compliance - Breach notification (legal aspects)

Data Protection Officer (DPO): - **Name:** [TODO: Name] - **Email:** [TODO: Email] - **Phone:** [TODO: Phone]

Responsibilities: - Data protection compliance (GDPR) - Interface between PCI-DSS and data protection - Data protection impact assessments - Reporting of data breaches

4.3 3. External Roles

4.3.1 3.1 Qualified Security Assessor (QSA)

Company: [TODO: QSA Company]
Contact: [TODO: Name]
Email: [TODO: Email]
Phone: [TODO: Phone]
QSA ID: [TODO: QSA ID]

Responsibilities: - Conduct annual PCI-DSS assessment - Creation of Report on Compliance (ROC) - Advice on compliance questions - Validation of security controls

4.3.2 3.2 Approved Scanning Vendor (ASV)

Company: [TODO: ASV Company]
Contact: [TODO: Name]

Email: [TODO: Email]
Phone: [TODO: Phone]
ASV ID: [TODO: ASV ID]

Responsibilities: - Quarterly vulnerability scans - Creation of scan reports - Validation of remediation - Passing scan attestation

4.3.3 3.3 Penetration Testing Firm

Company: [TODO: Pentest Company]
Contact: [TODO: Name]
Email: [TODO: Email]
Phone: [TODO: Phone]

Responsibilities: - Annual penetration tests - Segmentation validation - Creation of pentest reports - Retest after remediation

4.3.4 3.4 Service Providers

Service Provider	Contact	Role	PCI-DSS Status
[TODO: Payment Processor]	[TODO: Contact]	Payment Processing	AOC available
[TODO: Hosting Provider]	[TODO: Contact]	Server Hosting	AOC available
[TODO: Managed Security]	[TODO: Contact]	SIEM/SOC	AOC available

4.4 4. RACI Matrices

4.4.1 4.1 PCI-DSS Requirement 1: Firewall Configuration

Activity	CISO	PCI Mgr	IT Sec	Network	QSA
Create firewall policy	A	R	C	C	I
Configure firewall rules	C	I	A	R	I
Quarterly rule review	A	R	C	C	I
Approve changes	A	C	R	I	I

4.4.2 4.2 PCI-DSS Requirement 3: Protect Stored Data

Activity	CISO	PCI Mgr	IT Sec	Dev Mgr	QSA
Encryption policy	A	R	C	C	I
Key management	C	I	A	R	I
Data deletion	C	R	A	C	I
Tokenization	C	R	C	A	I

4.4.3 4.3 PCI-DSS Requirement 6: Secure Development

Activity	CISO	PCI Mgr	IT Sec	Dev Mgr	Developers
Secure coding standards	A	C	C	R	I
Code reviews	C	I	C	A	R
Vulnerability scanning	C	R	A	C	I
Patch deployment	C	R	A	R	C

4.4.4 4.4 PCI-DSS Requirement 8: Authentication

Activity	CISO	PCI Mgr	IT Sec	HR	QSA
Authentication policy	A	R	C	C	I
User management	C	I	A	R	I
MFA implementation	C	R	A	I	I
Access removal (offboarding)	C	R	A	R	I

4.4.5 4.5 PCI-DSS Requirement 10: Logging

Activity	CISO	PCI Mgr	IT Sec	Ops Mgr	QSA
Logging policy	A	R	C	C	I
Log configuration	C	I	A	R	I
Daily log review	C	R	A	C	I
Log retention	A	R	C	I	I

4.4.6 4.6 PCI-DSS Requirement 12: Security Policy

Activity	CEO	CISO	PCI Mgr	Legal	QSA
Approve security policy	A	R	C	C	I
Annual risk assessment	C	A	R	I	I
Training program	C	A	R	C	I
Incident response plan	C	A	R	C	I

Legend: - **R** (Responsible): Execution responsibility - **A** (Accountable): Overall responsibility, decision authority (only one person per activity) - **C** (Consulted): Consulted, subject matter expertise - **I** (Informed): Informed

4.5 5. Escalation Paths

4.5.1 5.1 Compliance Escalation

Level 1: PCI-DSS Program Manager
Level 2: CISO
Level 3: CEO

Escalation Criteria: - Critical compliance gaps - Failed audits - Data breaches - Unremediable vulnerabilities

4.5.2 5.2 Security Incident Escalation

Level 1: IT Security Manager (24/7 on-call)
Level 2: CISO
Level 3: CEO + Legal Counsel

Escalation Criteria: - Suspected data breach - Compromise of CDE systems - Malware infection in CDE - Unauthorized access to cardholder data

4.5.3 5.3 Emergency Contact Information

24/7 Security Hotline: [TODO: Phone number]
Security Email: [TODO: security@organization.com]
Incident Response Team: [TODO: Contact list]

4.6 6. Training and Awareness

4.6.1 6.1 Training Requirements

Role	Training Topics	Frequency	Responsible
All Employees	Security Awareness	Annual	HR + PCI Mgr
CDE Administrators	PCI-DSS Deep Dive	Annual	PCI Mgr
Developers	Secure Coding	Annual	Dev Mgr
Cashiers/POS	PCI-DSS Basics	Upon hire + annual	Ops Mgr

4.6.2 6.2 Training Documentation

Training evidence required: - Attendance list - Training materials - Participant confirmations - Test results (if applicable)

Retention Period: [TODO: 3 years]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initial creation

ewpage

Chapter 5

Data Flow Diagrams

Document ID: PCI-0040
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

5.1 1. Purpose

This document visualizes all cardholder data (CHD) flows within AdminSend GmbH.

5.1.1 1.1 Objectives

- **Transparency:** Complete visibility of all CHD flows
- **Scope Definition:** Identification of all PCI-DSS-relevant systems
- **Risk Assessment:** Detection of potential vulnerabilities
- **Compliance:** Meet PCI-DSS Requirement 12.5.2

5.2 2. Data Flow Overview

5.2.1 2.1 Main Data Flows

[TODO: Insert high-level data flow diagram - see diagrams/data_flow_overview.png]

Data Flow Phases: 1. **Capture:** Card input at POS/web form 2. **Transmission:** Transport for authorization 3. **Processing:** Authorization by acquiring bank 4. **Storage:** Persistence for reporting (if required) 5. **Deletion:** Secure disposal after retention period

5.2.2 2.2 Data Flow Categories

Category	Description	Systems	Encryption
Point of Sale	Card input in stores	POS Terminals	P2PE
E-Commerce	Online payments	Web Server, Payment Gateway	TLS 1.3
Call Center	Phone orders	CRM, IVR	Tokenization
Recurring Billing	Recurring payments	Billing System	Tokenization

5.3 3. Detailed Data Flows

5.3.1 3.1 Point-of-Sale Data Flow

[TODO: Insert POS data flow diagram]

Steps: 1. Customer presents card at POS terminal 2. Terminal reads card data (encrypted) 3. Encrypted data to payment gateway 4. Gateway sends to acquiring bank 5. Authorization response back to terminal 6. Receipt for customer

Involved Systems: - POS Terminal: [TODO: Model/Vendor] - Payment Gateway: [TODO: System ID] - Acquiring Bank: [TODO: Bank Name]

Data Protection: - P2PE (Point-to-Point Encryption) - No storage of full track data - Only last 4 digits on receipt

5.3.2 3.2 E-Commerce Data Flow

[TODO: Insert e-commerce data flow diagram]

Steps: 1. Customer enters card data in web form 2. HTTPS transmission to web server 3. Forward to payment gateway 4. Gateway tokenizes PAN 5. Token back to web server for storage 6. Authorization with token

Involved Systems: - Web Server: [TODO: System ID] - Payment Gateway: [TODO: System ID] - Database: [TODO: System ID] (tokens only)

Data Protection: - TLS 1.3 for transmission - Tokenization before storage - No storage of CVV2

5.3.3 3.3 Call Center Data Flow

[TODO: Insert call center data flow diagram]

Steps: 1. Customer provides card data by phone 2. Agent enters data in CRM (masked) 3. IVR system captures sensitive data 4. Direct transmission to payment gateway 5. Token back to CRM

Involved Systems: - CRM System: [TODO: System ID] - IVR System: [TODO: System ID] - Payment Gateway: [TODO: System ID]

Data Protection: - IVR for sensitive data entry - No storage of PAN in CRM - Only token stored

5.4 4. System Overview

5.4.1 4.1 Systems with CHD Access

System ID	System Name	CHD Type	Function	Encryption
[TODO: SYS-001]	POS Terminal	PAN (Transit)	Card Input	P2PE
[TODO: SYS-002]	Payment Gateway	PAN	Authorization	TLS 1.3
[TODO: SYS-003]	Database	Token	Storage	AES-256
[TODO: SYS-004]	Web Server	PAN (Transit)	E-Commerce	TLS 1.3

5.4.2 4.2 Data Transmission Protocols

Connection	Protocol	Encryption	Port
POS → Gateway	HTTPS	TLS 1.3	443
Web → Gateway	HTTPS	TLS 1.3	443
Gateway → Bank	HTTPS	TLS 1.3	443
Gateway → DB	SQL/TLS	TLS 1.2+	3306

5.5 5. Data Storage

5.5.1 5.1 Stored Cardholder Data

Data Type	Storage Location	Encryption	Retention Period	Justification
PAN (Token)	Database	AES-256	[TODO: 13 months]	Refunds
Cardholder Name	Database	AES-256	[TODO: 13 months]	Refunds
Transaction Data	Database	AES-256	[TODO: 7 years]	Accounting

Not Stored: - Full Track Data - CVV2/CVC2/CID - PIN/PIN Block

5.5.2 5.2 Data Deletion

Deletion Process: 1. Automatic identification of expired data 2. Secure deletion (overwrite/crypto-shredding) 3. Logging of deletion operations 4. Quarterly verification

Responsible: [TODO: Data Retention Manager]

5.6 6. External Data Flows

5.6.1 6.1 Acquiring Bank

Bank: [TODO: Bank Name]
Connection: HTTPS/TLS 1.3
Data Type: PAN, transaction data
Purpose: Authorization and settlement

5.6.2 6.2 Payment Processor

Processor: [TODO: Processor Name]
Connection: HTTPS/TLS 1.3
Data Type: PAN (encrypted)
Purpose: Payment processing

5.6.3 6.3 Tokenization Service

Service: [TODO: Service Name]
Connection: HTTPS/TLS 1.3
Data Type: PAN → Token
Purpose: Scope reduction

5.7 7. Data Flow Change Management

5.7.1 7.1 Change Process

For changes to data flows: 1. Update diagrams 2. PCI-DSS impact assessment 3. CISO approval 4. Document the change 5. Train affected employees

5.7.2 7.2 Change History

Date	Change	Justification	Approved By
[TODO: 2026-01-15]	Tokenization implemented	Scope reduction	[TODO: CISO]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 6

Compliance Program

Document ID: PCI-0050
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

6.1 1. Purpose

This document describes the PCI-DSS compliance program of AdminSend GmbH.

6.1.1 1.1 Objectives

- **Continuous Compliance:** Maintain PCI-DSS compliance
- **Governance:** Structured oversight and control
- **Risk Management:** Proactive identification and treatment of risks
- **Audit Readiness:** Preparation for assessments and audits

6.2 2. Compliance Governance

6.2.1 2.1 Governance Structure

PCI-DSS Steering Committee: - **Chair:** {{ meta.roles.ciso.name }} - **Members:** CEO, CIO, PCI Program Manager, Legal, Operations Manager - **Frequency:** Quarterly - **Purpose:** Strategic decisions, budget, risk assessment

PCI-DSS Working Group: - **Lead:** PCI Program Manager - **Members:** IT Security, Network, Development, Operations - **Frequency:** Monthly - **Purpose:** Operational implementation, problem solving, coordination

6.2.2 2.2 Management Commitment

Information Security Policy: - Approved by: {{ meta.roles.ceo.name }} - Date: [TODO: Date] - Annual review: [TODO: Month]

PCI-DSS Commitment: AdminSend GmbH commits to compliance with all PCI-DSS requirements to protect cardholder data.

6.3 3. Compliance Activities

6.3.1 3.1 Annual Activities

Activity	Responsible	Timeframe	Status
PCI-DSS Assessment (QSA)	PCI Program Manager	[TODO: Q1]	[TODO]
Penetration Test	IT Security	[TODO: Q2]	[TODO]
Risk Assessment	CISO	[TODO: Q3]	[TODO]
Policy Review	CISO	[TODO: Q4]	[TODO]
Security Awareness Training	HR + PCI Mgr	[TODO: Ongoing]	[TODO]

6.3.2 3.2 Quarterly Activities

Activity	Responsible	Frequency	Last Performed
ASV Vulnerability Scans	ASV	Quarterly	[TODO: Date]
Firewall Rule Review	Network Team	Quarterly	[TODO: Date]
Steering Committee Meeting	CISO	Quarterly	[TODO: Date]
Compliance Reporting	PCI Program Manager	Quarterly	[TODO: Date]

6.3.3 3.3 Monthly Activities

Activity	Responsible	Frequency	Last Performed
Working Group Meeting	PCI Program Manager	Monthly	[TODO: Date]
Compliance Dashboard Review	CISO	Monthly	[TODO: Date]
Patch Status Review	IT Security	Monthly	[TODO: Date]

6.3.4 3.4 Daily Activities

Activity	Responsible	Frequency
Log Review	IT Security	Daily
Incident Monitoring	SOC	24/7
Backup Verification	System Admin	Daily

6.4 4. Compliance Metrics and KPIs

6.4.1 4.1 Key Performance Indicators

KPI	Target Value	Measurement	Responsible
Vulnerability Remediation Time	< 30 days (High/Critical)	Monthly	IT Security
Patch Compliance Rate	> 95%	Monthly	System Admin
Security Training Completion	100%	Annual	HR
Failed Login Attempts	< 100/day	Daily	IT Security
Firewall Rule Changes	All approved	Monthly	Network Team

6.4.2 4.2 Compliance Dashboard

Monitored Metrics: - Number of open vulnerabilities (by severity) - Patch status of all CDE systems - Number of security incidents - Employee training status - Status of quarterly ASV scans - Firewall rule compliance

Dashboard Access: [TODO: URL/System]
Update: Daily automatic

6.5 5. Audit and Assessment

6.5.1 5.1 Annual PCI-DSS Assessment

Assessment Type: [TODO: SAQ or ROC]
QSA: [TODO: Company/Name]
Last Assessment: [TODO: Date]
Next Assessment: [TODO: Date]
Result: [TODO: Compliant/Non-Compliant]

Assessment Preparation: 1. Document collection (3 months before assessment) 2. Pre-assessment audit (2 months before assessment) 3. Remediation of open items (1 month before assessment) 4. QSA assessment (scheduled date) 5. Follow-up and AOC receipt

6.5.2 5.2 Attestation of Compliance (AOC)

Last AOC: [TODO: Date]
Valid Until: [TODO: Date]
Submitted To: [TODO: Acquiring Banks]

AOC Distribution: - Acquiring banks - Payment brands (if required) - Business partners (upon request)

6.5.3 5.3 Internal Audits

Frequency: Semi-annual
Responsible: Internal Audit Team
Scope: Sampling of all 12 PCI-DSS requirements

Last Audit: [TODO: Date]
Next Audit: [TODO: Date]

6.6 6. Risk Management

6.6.1 6.1 Annual Risk Assessment

Methodology: [TODO: e.g., ISO 27005, NIST 800-30]
Last Assessment: [TODO: Date]
Next Assessment: [TODO: Date]

Identified Risks:

Risk ID	Description	Likelihood	Impact	Measures
[TODO: R-001]	Data breach	Medium	High	Encryption, monitoring
[TODO: R-002]	Insider threat	Low	High	Access control, logging

6.6.2 6.2 Risk Mitigation

Risk Mitigation Strategies: - Technical controls (encryption, firewalls, IDS/IPS) - Organizational controls (policies, training) - Physical controls (access control, video surveillance) - Insurance (cyber insurance)

6.7 7. Incident Response

6.7.1 7.1 Incident Response Plan

Documented in: PCI-0630 Incident Response

Incident Categories: - Data breach - Malware infection - Unauthorized access - Denial of service - Physical security incident

6.7.2 7.2 Breach Notification

Notification Requirements: - Acquiring banks: Immediately - Payment brands: Per brand requirements - Affected cardholders: Per local legislation - Supervisory authorities: Per GDPR (72 hours)

Responsible: Legal Counsel + CISO

6.8 8. Training and Awareness

6.8.1 8.1 Training Program

Target Groups:

Target Group	Training Content	Frequency	Duration
All Employees	Security Awareness	Annual	1 hour
CDE Administrators	PCI-DSS Deep Dive	Annual	4 hours
Developers	Secure Coding	Annual	8 hours
Cashiers/POS	PCI-DSS Basics	Upon hire	2 hours

6.8.2 8.2 Training Materials

Available Materials: - E-learning modules - Presentations - Checklists - Posters and infographics - Phishing simulations

Storage Location: [TODO: Intranet/LMS URL]

6.9 9. Document Management

6.9.1 9.1 PCI-DSS Documentation

Document Register:

Document ID	Title	Version	Last Updated	Owner
PCI-0010	Scope and CDE	1.0	[TODO]	PCI Mgr
PCI-0020	Network Segmentation	1.0	[TODO]	Network
PCI-0030	Roles	1.0	[TODO]	PCI Mgr

Document Retention: Minimum 3 years
Access Control: Authorized personnel only

6.9.2 9.2 Evidence Collection

Required Evidence: - Firewall configurations - Scan reports (ASV) - Penetration test reports - Training records - Log reviews - Change logs

Storage Location: [TODO: Document management system]

6.10 10. Continuous Improvement

6.10.1 10.1 Improvement Process

Sources for Improvements: - Audit findings - Incident lessons learned - Vulnerability scan results - Employee feedback - Industry trends

6.10.2 10.2 Improvement Measures

Measure	Priority	Responsible	Target Date	Status
[TODO: Tokenization]	High	IT Security	[TODO]	In Progress
[TODO: SIEM Upgrade]	Medium	IT Security	[TODO]	Planned

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default }}	{{ meta.document.author | default }}	Initial creation

ewpage

Chapter 7

Firewall Configuration

Document ID: PCI-0100
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

7.1 1. Purpose

This document defines firewall configuration standards for AdminSend GmbH per PCI-DSS Requirement 1.

7.1.1 1.1 Objectives

- **Network Security:** Protect CDE through firewall controls
- **Access Control:** Restrict unauthorized network access
- **Compliance:** Meet PCI-DSS Requirement 1
- **Documentation:** Traceable firewall configuration

7.1.2 1.2 Scope

Affected Systems: - Perimeter firewalls (Internet border) - Internal firewalls (CDE segmentation) - Host-based firewalls (servers, workstations) - Cloud firewalls (if applicable)

7.2 2. Firewall Standards

7.2.1 2.1 Basic Principles

Default Deny: - All connections blocked by default - Only explicitly approved connections allowed - Documentation of all exceptions required

Least Privilege: - Minimum required access rights - Specific source and destination IP addresses - Specific ports and protocols

Defense in Depth: - Multiple firewall layers - Perimeter + internal segmentation - Host-based firewalls as additional layer

7.2.2 2.2 Firewall Architecture

Firewall Layers:

1. **Perimeter Firewall:**
   - Protection from Internet threats
   - Inbound and outbound traffic
   - DMZ for public services
2. **Internal Firewall:**
   - CDE segmentation
   - Separation of corporate and CDE
   - Access control between segments
3. **Host-based Firewall:**
   - Protection of individual systems
   - Additional defense layer
   - Protection during network compromise

7.3 3. Firewall Rule Management

7.3.1 3.1 Rule Requirements

Each firewall rule must contain: - Unique rule ID - Source (IP address/network) - Destination (IP address/network) - Port/protocol - Action (Allow/Deny) - Business justification - Approver - Creation date - Review date

7.3.2 3.2 Rule Approval Process

Process for new rules:

1. **Request:** Change request with justification
2. **Security Review:** Assessment by IT Security
3. **Approval:** CISO approval for CDE rules
4. **Implementation:** Configuration by network team
5. **Documentation:** Update of ruleset
6. **Validation:** Test of rule

Approval Matrix:

Rule Type	Approver	Documentation
CDE-related	CISO	Complete
Corporate	IT Manager	Standard
Temporary	IT Security	With expiration date

7.3.3 3.3 Quarterly Rule Review

Review Process:

1. **Review all rules:** Complete review
2. **Validation:** Business justification still valid?
3. **Cleanup:** Removal of unused rules
4. **Documentation:** Update documentation
5. **Approval:** CISO confirmation

Last Review: [TODO: Date]
Next Review: [TODO: Date]
Responsible: [TODO: Network Security Team]

7.4 4. Firewall Configuration Standards

7.4.1 4.1 Perimeter Firewall

Inbound Traffic:

Service	Port	Protocol	Source	Destination	Allowed
HTTPS	443	TCP	Any	Web Server (DMZ)	Yes
SSH	22	TCP	Admin IPs	Jump Server	Yes (with MFA)
All others	*	*	Any	CDE	No

Outbound Traffic:

Service	Port	Protocol	Source	Destination	Allowed
HTTPS	443	TCP	CDE	Acquiring Bank	Yes
DNS	53	UDP	CDE	DNS Server	Yes
NTP	123	UDP	CDE	NTP Server	Yes
All others	*	*	CDE	Internet	No (Default Deny)

7.4.2 4.2 Internal Firewall (CDE Segmentation)

CDE → Corporate: - Blocked by default - Exceptions only with CISO approval - Logging of all connection attempts

Corporate → CDE: - Only authorized admin access - MFA required - Via jump server/VPN - Complete logging

7.4.3 4.3 Host-based Firewalls

Requirements: - Enabled on all CDE systems - Configuration per hardening standards - Central management (if possible) - Logging enabled

Example Configuration (Linux iptables):

```
# Default Deny
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

# Allow established connections
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow specific services
iptables -A INPUT -p tcp --dport 443 -j ACCEPT  # HTTPS
iptables -A INPUT -p tcp --dport 22 -s 10.1.102.0/24 -j ACCEPT  # SSH from Management

# Log dropped packets
iptables -A INPUT -j LOG --log-prefix "FW-DROP: "
```

7.5 5. Prohibited Configurations

The following configurations are NOT allowed:

- **Any-Any Rules:** No rules with Source=Any and Destination=Any
- **Direct Internet Connections:** CDE systems must not communicate directly with Internet
- **Unencrypted Protocols:** Telnet, FTP, HTTP (except redirect to HTTPS)
- **Deprecated Protocols:** SSLv2, SSLv3, TLS 1.0, TLS 1.1
- **Undocumented Rules:** All rules must be documented

7.6 6. Change Management

7.6.1 6.1 Emergency Changes

Emergency changes allowed for: - Active security incidents - Critical system failures - Immediate threats

Process: 1. Verbal approval by CISO 2. Immediate implementation 3. Retrospective documentation (within 24h) 4. Formal approval (within 48h)

7.6.2 6.2 Change History

Date	Rule ID	Change	Justification	Approved By
[TODO: 2026-01-15]	FW-105	New rule	Payment API	[TODO: CISO]
[TODO: 2026-02-01]	FW-042	Removed	No longer needed	[TODO: CISO]

7.7 7. Monitoring and Alerting

7.7.1 7.1 Firewall Logging

Logging Requirements: - All blocked connections - All allowed connections to/from CDE - Firewall configuration changes - Firewall system events (start, stop, errors)

Log Retention: [TODO: 90 days online, 1 year archive]
Log Forwarding: [TODO: SIEM system]

7.7.2 7.2 Alerting Rules

Alert	Condition	Severity	Notification
Unauthorized CDE access	Blocked connection to CDE	High	SOC + IT Security
Firewall rule change	Configuration change	Medium	Network Team
Firewall failure	Firewall unreachable	Critical	SOC + CISO

7.8 8. Compliance Validation

7.8.1 8.1 Validation Activities

Quarterly: - Firewall rule review - Documentation validation - Unused rule cleanup

Annual: - Penetration test of firewall configuration - Segmentation validation - Compliance audit

7.8.2 8.2 Validation Documentation

Required Evidence: - Firewall configuration files - Rule review logs - Change logs - Approval records

---

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 8

Access Control

Document ID: PCI-0400
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

8.1 1. Purpose

This document defines the access control policies for AdminSend GmbH in accordance with PCI-DSS Requirement 7.

8.1.1 1.1 Objectives

- **Need-to-Know Principle:** Access only for authorized personnel
- **Least Privilege:** Minimum required access rights
- **Role-Based Access Control:** RBAC implementation
- **Compliance:** Fulfillment of PCI-DSS Requirement 7

8.1.2 1.2 Scope

Affected Systems: - All CDE systems - Systems with cardholder data - Administrative systems - Databases with CHD

8.2 2. Access Control Principles

8.2.1 2.1 Need-to-Know

Principle: - Access only for persons with business necessity - Documented justification required - Regular review of access rights

8.2.2 2.2 Least Privilege

Principle: - Minimum required permissions - No unnecessary administrator rights - Time-limited privileged access

8.2.3 2.3 Separation of Duties

Principle: - Separation of critical functions - No single person with complete control - Four-eyes principle for critical operations

8.3 3. Role-Based Access Control (RBAC)

8.3.1 3.1 Defined Roles

Role	Description	CDE Access	CHD Access
Payment Administrator	Full payment system administration	Yes	Yes (full)
System Administrator	Server and network administration	Yes	No
Database Administrator	Database management	Yes	Yes (encrypted)
Application Administrator	Application management	Yes	No
Security Administrator	Security system administration	Yes	No
Cashier	POS operation	Limited	Yes (input only)
Support Staff	Customer service	Limited	Yes (query only, masked)
Developer	Software development	No	No
Auditor	Compliance review	Read-only	Yes (logs only)

8.3.2 3.2 Permission Matrix

System/Resource	Payment Admin	Sys Admin	DB Admin	App Admin	Cashier	Support
Payment Gateway	RWX	RW	R	RW	-	R
CDE Database	RWX	R	RWX	R	-	R (masked)
POS Terminal	RW	RW	-	RW	RW	R
Firewall	RW	RWX	-	-	-	-
SIEM	RW	RW	-	-	-	R
Backup System	RW	RWX	RW	-	-	-

Legend: R = Read, W = Write, X = Execute, - = No Access

8.4 4. Access Management Process

8.4.1 4.1 Access Request

Process:

1. **Request:** Form with justification
2. **Manager Approval:** Supervisor approves
3. **Security Review:** IT Security reviews
4. **CISO Approval:** Required for CDE access
5. **Provisioning:** IT implements access
6. **Documentation:** Access is documented
7. **Notification:** User is informed

Approval Matrix:

Access Type	Approver	Documentation
CDE Access	CISO	Complete
CHD Access	CISO + Manager	Complete
Corporate Access	Manager	Standard
Temporary Access	IT Security	With expiration date

8.4.2 4.2 Access Modification

Process for Role Change:

1. **Identification:** Role change detected
2. **Assessment:** New access requirements
3. **Approval:** Same as new request
4. **Revocation:** Remove old permissions
5. **Provisioning:** Grant new permissions
6. **Validation:** Test access

8.4.3 4.3 Access Revocation

Process for Termination:

1. **Notification:** HR informs IT
2. **Immediate Revocation:** Deactivate all access
3. **Return:** Hardware and access credentials
4. **Documentation:** Document revocation
5. **Validation:** Test access (should be blocked)

Timeframe: - Upon termination: Immediately on last working day - Upon transfer: Within 24 hours - Upon suspicion: Immediately

8.5 5. Privileged Access

8.5.1 5.1 Administrative Accounts

Requirements: - Separate admin accounts (not for daily work) - Strong authentication (MFA required) - Complete logging of all actions - Regular review

Naming Convention: - Standard user: `firstname.lastname` - Admin user: `firstname.lastname-admin` - Service account: `svc-servicename`

8.5.2 5.2 Privileged Access Management (PAM)

PAM System: [TODO: Name of PAM system]

Functions: - Just-in-Time (JIT) access - Session recording - Password vaulting - Automatic password rotation

Process: 1. Admin requests privileged access 2. Approval by CISO (automatic or manual) 3. Time-limited access granted 4. Session is recorded 5. Automatic revocation after expiration

8.5.3 5.3 Emergency Access

Break-Glass Accounts: - Only for emergencies - Password in sealed envelope - Usage must be documented - Change password after use

Process: 1. Emergency identified 2. Open envelope (with witness) 3. Use access 4. Document incident 5. Change password immediately 6. Inform CISO

8.6 6. Access Control for Cardholder Data

8.6.1 6.1 CHD Access Restrictions

Full PAN Access: - Only for authorized roles - Documented business justification - CISO approval required - Complete logging

Masked PAN Access: - Only last 4 digits visible - For support and reporting - Standard approval sufficient

No PAN Access: - All other users - Developers (test data only) - External service providers (without necessity)

8.6.2 6.2 Data Masking

Masking Rules: - PAN: Only first 6 and last 4 digits (e.g., 123456******1234) - Expiration date: Fully masked - CVV: Never display (must not be stored) - Cardholder name: Partially masked (e.g., John D******)

Exceptions: - Payment administrators (full access) - Only with CISO approval - Complete logging

8.7 7. Application Access Control

8.7.1 7.1 Application Permissions

Permission Model: - Role-based permissions - Granular function rights - No shared accounts - Unique user IDs

Example (Payment Application):

Function	Payment Admin	Cashier	Support
Perform transaction	Yes	Yes	No
Cancel transaction	Yes	Limited	No
View reports	Yes	No	Yes (masked)
Change configuration	Yes	No	No
Manage users	Yes	No	No

8.7.2 7.2 API Access Control

API Authentication: - API keys with expiration - OAuth 2.0 for external APIs - Mutual TLS for critical APIs - Rate limiting

API Authorization: - Scope-based permissions - Minimum required scopes - Logging of all API calls

8.8 8. Database Access Control

8.8.1 8.1 Database Permissions

Permission Model: - Separate DB accounts per application - No shared accounts - Least privilege for applications - DBA access only for administration

Example:

Account	Type	Permissions	Purpose
app_payment	Application	SELECT, INSERT, UPDATE	Payment application
app_reporting	Application	SELECT	Reporting
dba_admin	DBA	ALL	Administration
backup_user	Service	SELECT	Backup

8.8.2 8.2 Encrypted Columns

CHD Columns: - PAN: Encrypted (AES-256) - Access only via decryption function - Logging of all decryptions - Only authorized accounts

8.9 9. Network Access Control

8.9.1 9.1 Network Access

Access Methods: - VPN for remote access - Jump server for admin access - No direct internet connection to CDE

Authentication: - Multi-Factor Authentication (MFA) - Certificate-based authentication - Strong passwords

8.9.2 9.2 Network Segmentation

Access Control Between Segments: - Firewall rules - ACLs on switches - Micro-segmentation

8.10 10. Physical Access Control

8.10.1 10.1 Data Center

Access Control: - Badge system - Biometric authentication - Escort requirement for visitors - Logging of all access

Authorized Persons: - Data center personnel - Authorized administrators - Maintenance personnel (with escort)

8.10.2 10.2 Offices with CDE Access

Access Control: - Locked rooms - Badge access - Visitor log

8.11 11. Service Provider Access Control

8.11.1 11.1 Service Provider Access

Requirements: - Separate accounts for each service provider - Time-limited access - Complete logging - PCI-DSS AOC required

Approval Process: 1. Service provider contract with PCI clauses 2. AOC validation 3. CISO approval 4. Time-limited access 5. Monitoring during access

8.11.2 11.2 Remote Support

Process: - Only after approval - Session recording - Accompanied by internal admin - Immediate revocation after completion

8.12 12. Access Control Monitoring

8.12.1 12.1 Logging

Logged Events: - Successful logins - Failed logins - Privileged actions - Access to CHD - Permission changes

Log Retention: [TODO: 90 days online, 1 year archive]

8.12.2 12.2 Alerting

Alert	Condition	Severity	Notification
Multiple failed logins	>5 in 15 min	Medium	SOC

Alert	Condition	Severity	Notification
Admin login outside business hours	After 10 PM	Medium	SOC + Manager
CHD access	Any access	Low	SIEM
Permission change	Any change	Medium	IT Security

8.13 13. Access Control Reviews

8.13.1 13.1 Quarterly Review

Review Process:

1. **User Review:** All users with CDE access
2. **Permission Review:** Validate all permissions
3. **Inactive Accounts:** Identify and deactivate
4. **Documentation:** Document results
5. **Approval:** CISO confirmation

Last Review: [TODO: Date]
Next Review: [TODO: Date]
Responsible: [TODO: IT Security Team]

8.13.2 13.2 Recertification

Annual Recertification: - All users with CDE access - Manager confirms business necessity - IT Security validates permissions - CISO approves

8.14 14. Compliance Validation

8.14.1 14.1 Validation Activities

Quarterly: - Access control review - Inactive account cleanup - Permission documentation

Annually: - Complete recertification - Penetration testing - Compliance audit

8.14.2 14.2 Validation Documentation

Required Evidence: - Access control policies - Permission matrix - Approval evidence - Review protocols - Recertification evidence

---

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 9

User Authentication

Document ID: PCI-0410
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

9.1 1. Purpose

This document defines the authentication policies for AdminSend GmbH in accordance with PCI-DSS Requirement 8.

9.1.1 1.1 Objectives

- **Unique Identification:** Each user uniquely identifiable
- **Strong Authentication:** Multi-Factor Authentication (MFA)
- **Secure Passwords:** Enforce password policies
- **Compliance:** Fulfillment of PCI-DSS Requirement 8

9.1.2 1.2 Scope

Affected Systems: - All CDE systems - Administrative systems - Applications with CHD access - Remote access systems

9.2 2. User Identification

9.2.1 2.1 Unique User IDs

Requirements: - Each user has unique ID - No shared accounts - No generic accounts (except documented exceptions) - User ID must not be reused

Naming Convention: - Format: `firstname.lastname` - For duplicates: `firstname.lastname2` - Service accounts: `svc-servicename` - Admin accounts: `firstname.lastname-admin`

9.2.2 2.2 Prohibited Account Types

Not Allowed: - Shared accounts (multiple people, one account) - Generic accounts (e.g., "admin", "user", "test") - Group accounts - Vendor default accounts (must be disabled)

Exceptions: - Emergency accounts (Break-Glass) - documented - Service accounts - documented and monitored - Console access (only with logging)

9.3 3. Authentication Methods

9.3.1 3.1 Multi-Factor Authentication (MFA)

MFA Required for: - All CDE access - Administrative access - Remote access (VPN, Jump Server) - Privileged accounts - Access to CHD

MFA Factors:

1. **Something You Know:**
   - Password
   - PIN
2. **Something You Have:**
   - Hardware token
   - Software token (Authenticator App)
   - Smart card
   - SMS (backup only)
3. **Something You Are:**
   - Biometrics (fingerprint, facial recognition)

MFA Implementation: - At least 2 different factors - Factors must be independent - MFA System: [TODO: Name of MFA system]

9.3.2 3.2 Password Authentication

Password Requirements:

- **Minimum Length:** 12 characters (15 for admin accounts)
- **Complexity:**
  - Uppercase letters (A-Z)
  - Lowercase letters (a-z)
  - Digits (0-9)
  - Special characters (!@#$%^&*)
- **No Dictionary Words**
- **No Personal Information** (name, birthdate, etc.)
- **No Reuse** of last 4 passwords

Password Change: - Every 90 days for standard users - Every 90 days for admin accounts - Immediately upon suspicion of compromise - Upon first login

Password Storage: - Only as hash (bcrypt, PBKDF2, Argon2) - Never in cleartext - Salt for each hash - No reversible encryption

9.3.3 3.3 Certificate-Based Authentication

Usage: - Server-to-server communication - API authentication - VPN access (in addition to MFA)

Requirements: - Certificates from trusted CA - Regular renewal - Revocation checking (CRL/OCSP) - Secure key storage

9.4 4. Account Management

9.4.1 4.1 Account Creation

Process: 1. Approved access request 2. Create unique user ID 3. Generate temporary password 4. MFA registration 5. Notify user 6. Force password change on first login

9.4.2 4.2 Account Deactivation

Automatic Deactivation: - After 90 days of inactivity - Upon employee termination - Upon role change (old account)

Manual Deactivation: - During security incidents - Upon suspicion of compromise - At manager's request

Process: 1. Deactivate account (do not delete) 2. Terminate all sessions 3. Validate access (should be blocked) 4. Document

9.4.3 4.3 Account Deletion

Timeframe: - 90 days after deactivation - After completion of audits/investigations - After retention requirements

Process: 1. Confirm account no longer needed 2. Backup account data (if required) 3. Delete account 4. Document

9.5 5. Password Management

9.5.1 5.1 Password Reset

Self-Service Reset: - Via Identity Management System - After successful identity verification - Security questions or email verification - MFA verification

Helpdesk Reset: - Identity verification required - Temporary password - Force password change on next login - Document reset

9.5.2 5.2 Password Lockout

Account Lockout After: - 6 failed login attempts - Lockout for 30 minutes - Or manual unlock by admin

Unlock: - Automatically after 30 minutes - Or by helpdesk after identity verification - Document unlock

9.5.3 5.3 Password Vault

For Privileged Passwords: - Central password vault solution - Automatic password rotation - Check-out/check-in process - Session recording - Complete logging

Vault System: [TODO: Name of vault system]

9.6 6. Session Management

9.6.1 6.1 Session Timeouts

Inactivity Timeout: - 15 minutes for CDE systems - 30 minutes for corporate systems - 5 minutes for privileged sessions

Maximum Session Duration: - 8 hours for standard users - 4 hours for admin sessions - Re-authentication required

9.6.2 6.2 Session Security

Requirements: - Unique session IDs - Session ID rotation after login - Secure session cookies (HttpOnly, Secure, SameSite) - Session invalidation on logout - No session IDs in URLs

9.6.3 6.3 Concurrent Sessions

Restrictions: - Maximum 2 concurrent sessions per user - Only 1 privileged session at a time - Warning on new session - Option to terminate old sessions

9.7 7. Remote Authentication

9.7.1 7.1 VPN Access

Authentication: - Username + Password - Plus MFA (Hardware token or Authenticator App) - Certificate-based authentication (optional)

Authorization: - Only authorized users - Access to specific network segments - Complete logging

9.7.2 7.2 Jump Server

Authentication: - MFA required - Privileged accounts - Session recording - Time-limited access

Access Control: - Only from authorized source IPs - Only to authorized target systems - Complete logging

9.8 8. Application Authentication

9.8.1 8.1 Web Applications

Authentication: - Username + Password - MFA for CDE applications - Session management - HTTPS required

Security Measures: - Brute-force protection (Rate Limiting) - CAPTCHA after multiple failures - Account lockout - Secure password storage

9.8.2 8.2 API Authentication

Methods: - API Keys (with expiration) - OAuth 2.0 - JWT (JSON Web Tokens) - Mutual TLS

Requirements: - No API keys in code - API key rotation - Scope-based authorization - Rate limiting

9.9 9. Service Account Management

9.9.1 9.1 Service Accounts

Requirements: - Unique service account IDs - Documented usage - Strong passwords (32+ characters) - Regular password rotation (90 days) - No interactive logins

Naming Convention: - Format: `svc-servicename` - Example: `svc-payment-gateway`

9.9.2 9.2 Service Account Monitoring

Monitoring: - Log all service account activities - Alerts on unusual activities - Regular review of usage - Deactivation of unused accounts

9.10 10. Authentication Logging

9.10.1 10.1 Logged Events

Successful Authentication: - User ID - Timestamp - Source IP address - Target system - Authentication method

Failed Authentication: - User ID (or attempt) - Timestamp - Source IP address - Target system - Failure reason

Other Events: - Password changes - Account lockouts - Account unlocks - MFA registration - Privileged actions

9.10.2 10.2 Log Retention

Retention: - 90 days online - 1 year archive - Immutable (WORM)

Log Forwarding: - To SIEM system - Real-time transmission - Encrypted transmission

9.11 11. Authentication Monitoring

9.11.1 11.1 Alerting

Alert	Condition	Severity	Notification
Multiple failed logins	>5 in 15 min	Medium	SOC
Admin login outside business hours	After 10 PM	Medium	SOC + Manager
MFA failure	>3 failures	Low	SOC

Alert	Condition	Severity	Notification
Account lockout	Any lockout	Low	Helpdesk
Privileged access	Any access	Low	SIEM
Password change	Outside business hours	Low	SIEM

9.11.2 11.2 Anomaly Detection

Monitoring: - Unusual login times - Unusual source IPs - Geographic anomalies - Multiple concurrent logins - Privileged access

9.12 12. Vendor Default Accounts

9.12.1 12.1 Default Account Management

Requirements: - Identify all default accounts - Disable or delete default accounts - If required: Change password - Document all default accounts

Examples: - admin/admin - root/root - Administrator/password - sa (SQL Server)

9.12.2 12.2 Default Account Inventory

System	Default Account	Status	Action
[TODO: System 1]	admin	Disabled	Deleted
[TODO: System 2]	root	Active	Password changed
[TODO: System 3]	Administrator	Disabled	Renamed

9.13 13. Authentication Testing

9.13.1 13.1 Penetration Tests

Annually: - Test authentication mechanisms - Simulate brute-force attacks - MFA bypass attempts - Session management tests

9.13.2 13.2 Vulnerability Scans

Quarterly: - Identify weak passwords - Identify default accounts - Authentication vulnerabilities

9.14 14. Compliance Validation

9.14.1 14.1 Validation Activities

Quarterly: - Password policy compliance - Validate MFA implementation - Identify inactive accounts - Review default accounts

Annually: - Complete authentication audit - Penetration testing - Compliance assessment

9.14.2 14.2 Validation Documentation

Required Evidence: - Authentication policies - MFA configuration - Password policy configuration - Account management protocols - Penetration test reports

---

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated | default('') }}	{{ meta.document.author | default('') }}	Initial creation

ewpage

Chapter 10

Physical Security

Document ID: PCI-0420
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

10.1 1. Purpose

This document defines the physical security controls for AdminSend GmbH in accordance with PCI-DSS Requirement 9.

10.1.1 1.1 Objectives

- **Physical Protection:** Protect CDE systems from unauthorized access
- **Access Control:** Restrict physical access
- **Media Security:** Secure handling of media
- **Compliance:** Fulfillment of PCI-DSS Requirement 9

10.1.2 1.2 Scope

Affected Locations: - Data centers with CDE systems - Server rooms - Offices with POS terminals - Media storage rooms

10.2 2. Physical Access Control

10.2.1 2.1 Access Control Systems

Implemented Systems: - Badge system: [TODO: Name of system] - Biometric authentication: [TODO: Type] - Video surveillance: [TODO: Number of cameras] - Alarm system: [TODO: Name

of system]

Requirements: - Unique identification of each person - Logging of all access - Automatic lockout after business hours - Alerting on unauthorized access

10.2.2 2.2 Access Authorization

Authorization Levels:

Level	Authorization	Areas	Personnel
Level 1	Full access	All areas	Facility Manager, CISO
Level 2	CDE access	Data center, server rooms	IT Administrators
Level 3	Limited	Offices with POS	Cashiers, Support
Level 4	Escorted	All areas	Visitors, Service providers

Approval Process: 1. Request by manager 2. Security review 3. CISO approval (for CDE areas) 4. Badge issuance 5. Documentation

10.2.3 2.3 Data Center Access Control

Requirements: - Two-factor authentication (Badge + Biometrics) - Mantrap/Airlock - Video surveillance (24/7) - Alerting on unauthorized access - Logging of all access

Authorized Personnel: - Data center personnel - Authorized IT administrators - Maintenance personnel (with escort only)

Visitor Policy: - Pre-registration required - Escort requirement - Visitor badge - Logging

10.3 3. Visitor Management

10.3.1 3.1 Visitor Registration

Process: 1. Pre-registration by host 2. Identity verification upon arrival 3. Issue visitor badge 4. Security briefing 5. Escort by authorized employee 6. Return badge upon departure

Visitor Badge: - Clearly visible - Time-limited - Unique number - Photo (optional)

10.3.2 3.2 Visitor Escort

Requirements: - Constant escort in CDE areas - Escort must be authorized - No unattended visitors - Document escort

Exceptions: - Public areas (reception, cafeteria) - Only after security briefing

10.3.3 3.3 Visitor Log

Logged Information: - Visitor name - Company - Purpose of visit - Host - Arrival time - Departure time - Areas visited - Escort

Retention: 90 days

10.4 4. Employee Identification

10.4.1 4.1 Employee Badges

Requirements: - Photo ID - Name - Employee number - Department - Expiration date - Visibly worn

Issuance: - Upon hiring - After identity verification - Documentation

Return: - Upon termination - Upon loss (deactivation + reissuance)

10.4.2 4.2 Employee/Visitor Distinction

Measures: - Different badge colors - Clear "VISITOR" marking - Time-limited visitor badges

10.5 5. Video Surveillance

10.5.1 5.1 Camera Locations

Monitored Areas: - All data center entrances - Server rooms - Areas with POS terminals - Media storage rooms - Parking lots (optional)

Camera Specifications: - Minimum resolution: 1080p - Night vision capable - Motion detection - Tamper protection

10.5.2 5.2 Recording and Storage

Requirements: - Continuous recording (24/7) - Retention: 90 days - Secure storage (encrypted) - Access control to recordings - Backup of recordings

Access to Recordings: - Only authorized personnel - Logging of all access - Approval by Security Manager

10.5.3 5.3 Privacy

Measures: - Signs indicating video surveillance - Privacy policy - No surveillance of private areas (restrooms, changing rooms) - GDPR compliance

10.6 6. Media Handling

10.6.1 6.1 Media Classification

Classification Levels:

Level	Description	Examples	Handling
Critical	CHD in cleartext	Backup tapes with unencrypted CHD	Encrypted, secured
Confidential	CHD encrypted	Encrypted backups	Secured
Internal	No CHD	System logs	Standard
Public	No sensitive data	Marketing material	No restriction

10.6.2 6.2 Media Storage

Requirements: - Secured storage room - Access control - Climate control - Fire protection - Inventory management

Storage Room Specifications: - Fire-resistant cabinets for critical media - Locked cabinets - Access control (badge system) - Video surveillance - Logging of all access

10.6.3 6.3 Media Transport

Internal Transport: - Sealed containers - Escort person - Documentation (handover protocol)

External Transport: - Encrypted media - Sealed containers - Trusted courier - Tracking - Insurance - Documentation

Courier Requirements: - Background check - Confidentiality agreement - Insurance - Tracking system

10.7 7. Media Destruction

10.7.1 7.1 Destruction Methods

Paper: - Cross-cut shredder (DIN 66399 P-4 or higher) - For CHD: P-5 or higher - Secure disposal of shreds

Electronic Media:

Media Type	Method	Standard
Hard drives	Degaussing + physical destruction	NIST 800-88
SSDs	Cryptographic erasure + destruction	NIST 800-88
USB drives	Physical destruction	NIST 800-88
CDs/DVDs	Shredding	DIN 66399 O-4
Backup tapes	Degaussing + shredding	NIST 800-88

Certification: - Destruction certificate required - Document all destroyed media - Record serial numbers

10.7.2 7.2 Destruction Service Provider

Requirements: - Certified service provider (e.g., DIN 66399) - Confidentiality agreement - On-site destruction or secure pickup - Destruction certificate - Insurance

Service Provider: [TODO: Name of service provider]

10.7.3 7.3 Destruction Log

Logged Information: - Date of destruction - Media type - Serial number (if available) - Destruction method - Performed by - Certificate number

Retention: 3 years

10.8 8. Point-of-Sale (POS) Security

10.8.1 8.1 POS Terminal Protection

Physical Security: - Tamper protection (Tamper-evident Seals) - Regular inspection - Secure mounting - Video surveillance of area

Inspection: - Daily before business opening - After maintenance - Upon suspicion of tampering

Checklist: - [ ] Tamper seal intact - [ ] No unusual devices connected - [ ] No damage - [ ] Firmware version correct

10.8.2 8.2 POS Terminal Inventory

Inventory Management: - List of all POS terminals - Serial numbers - Locations - Responsible persons - Maintenance history

Quarterly Review: - Validate inventory - Check locations - Verify tamper seals - Documentation

10.8.3 8.3 POS Terminal Maintenance

Maintenance Process: 1. Announce maintenance 2. Escort by authorized employee 3. Document all activities 4. Apply new tamper seals 5. Functional test 6. Documentation

10.9 9. Backup Media

10.9.1 9.1 Backup Media Security

Requirements: - Encrypted backups - Secure storage - Offsite storage - Access control - Inventory management

Storage: - Onsite: Fire-resistant safe - Offsite: Secure data center or vault

10.9.2 9.2 Backup Media Transport

Process: - Encrypted media - Sealed containers - Trusted courier - Handover protocol - Documentation

10.10 10. Workplace Security

10.10.1 10.1 Clean Desk Policy

Requirements: - No sensitive documents on desks - Lock screens when absent - Documents in locked cabinets - No passwords on sticky notes

Controls: - Regular inspections - Employee awareness

10.10.2 10.2 Screen Privacy

Requirements: - Privacy filters for screens with CHD - Screens not visible from outside - Automatic screen lock (15 minutes)

10.11 11. Emergency Access

10.11.1 11.1 Break-Glass Procedure

Process: - Sealed envelope with emergency access credentials - Storage in safe - Access only with witness - Document each use - Immediate password change after use

Documentation: - Date and time - Reason for emergency access - Performed by - Witness - Actions performed

10.11.2 11.2 Emergency Evacuation

Process: - Evacuation plan - Assembly points - Responsible persons - Regular drills

Security Measures: - Automatic lockdown of all systems - Activate alarm system - Notify security

10.12 12. Compliance Validation

10.12.1 12.1 Validation Activities

Quarterly: - POS terminal inspection - Media inventory - Visitor log review - Video surveillance test

Annually: - Physical security audit - Penetration test (physical) - Employee awareness

10.12.2 12.2 Validation Documentation

Required Evidence: - Access control logs - Visitor logs - POS inspection logs - Media destruction certificates - Video recordings (90 days)

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 11

Logging and Monitoring

Document ID: PCI-0500
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

11.1 1. Purpose

This document defines the logging and monitoring requirements for AdminSend GmbH in accordance with PCI-DSS Requirement 10.

11.1.1 1.1 Objectives

- **Traceability:** Log all access to CDE and CHD
- **Anomaly Detection:** Identify suspicious activities
- **Incident Response:** Enable forensic investigations
- **Compliance:** Fulfillment of PCI-DSS Requirement 10

11.1.2 1.2 Scope

Affected Systems: - All CDE systems - Systems with CHD access - Network components - Security systems

11.2 2. Logging Requirements

11.2.1 2.1 Events to Log

User Access: - All logins (successful and failed) - All logouts - Privileged actions - Access to CHD - Permission changes

System Events: - System starts and stops - Configuration changes - Software installations - Patch installations - Service starts and stops

Network Events: - Firewall rule changes - Blocked connections - VPN connections - IDS/IPS alerts

Security Events: - Antivirus detections - Security policy violations - Account lockouts - Password changes

Database Events: - All access to CHD tables - Schema changes - Privileged database operations - Failed access attempts

11.2.2 2.2 Log Entry Format

Required Fields: - **User ID:** Who performed the action? - **Event Type:** What happened? - **Timestamp:** When did it happen? (synchronized time) - **Success/Failure:** Was the action successful? - **Source:** Where did the action come from? (IP address, hostname) - **Target:** Which system/resource was affected? - **Additional Details:** Relevant context information

Example:

```
2026-02-06 14:32:15 UTC | USER=john.doe | EVENT=LOGIN_SUCCESS | SOURCE=10.1.100.50 | TARGET=pay
```

11.3 3. SIEM System

11.3.1 3.1 SIEM Implementation

SIEM System: [TODO: Name of SIEM system]

Functions: - Central log collection - Real-time analysis - Event correlation - Alerting - Reporting - Forensic search

Architecture: - Log sources → Log forwarder → SIEM - Encrypted transmission (TLS 1.2+) - Redundant SIEM servers - Secure log storage

11.3.2 3.2 Log Forwarding

Configuration: - All CDE systems send logs to SIEM - Real-time transmission (< 5 minutes delay) - Encrypted transmission - Authentication of log sources

Log Forwarders: - Syslog (RFC 5424) - Windows Event Forwarding - Agent-based (e.g., Splunk Forwarder, Elastic Beats)

11.3.3 3.3 Log Parsing and Normalization

Requirements: - Uniform log format - Parsing of all relevant fields - Normalization of timestamps - Enrichment with context (e.g., Geo-IP)

11.4 4. Log Retention

11.4.1 4.1 Retention Periods

Online Storage: - 90 days in SIEM (fast access) - Full-text search possible - Real-time analysis

Archive Storage: - 1 year in archive - Compressed - Encrypted - WORM storage (Write Once Read Many)

Long-term Archiving: - According to legal requirements - Secure storage - Documentation

11.4.2 4.2 Log Backup

Requirements: - Daily log backups - Offsite storage - Encrypted backups - Regular restore tests

11.5 5. Log Integrity

11.5.1 5.1 Protection Against Tampering

Measures: - WORM storage for logs - Digital signatures - Hash values for log files - Access control to logs - Logging of log access

Validation: - Regular integrity checks - Automatic alerts on tampering - Forensic investigation on suspicion

11.5.2 5.2 Log Access Control

Permissions: - Only authorized personnel - Read-only access for most users - Full access only for log administrators - Logging of all log access

Roles: - Log Administrator: Full access - Security Analyst: Read access, search, alerting - Auditor: Read access - Standard User: No access

11.6 6. Time Synchronization

11.6.1 6.1 NTP Configuration

Requirements: - All systems synchronized with NTP - Internal NTP servers - External NTP sources (Stratum 1 or 2) - Redundant NTP servers

NTP Servers: - Primary: [TODO: IP address] - Secondary: [TODO: IP address] - External source: [TODO: e.g., time.nist.gov]

Time Zone: - UTC for all logs - Local time zone for display (with UTC offset)

11.6.2 6.2 Time Drift Monitoring

Monitoring: - Maximum drift: 1 second - Alerts on drift $>$ 1 second - Automatic correction - Logging of time changes

11.7 7. Monitoring and Alerting

11.7.1 7.1 Security Monitoring

24/7 Monitoring: - Security Operations Center (SOC) - Real-time monitoring of all alerts - Incident response on critical alerts - Escalation by severity

SOC Team: - SOC Analyst (Tier 1) - Senior SOC Analyst (Tier 2) - Security Engineer (Tier 3) - CISO (Escalation)

11.7.2 7.2 Alerting Rules

Critical Alerts:

Alert	Condition	Action	Escalation
Multiple failed logins	>10 in 5 min	Immediate investigation	SOC → CISO
Unauthorized CDE access	Blocked connection to CDE	Immediate investigation	SOC → IT Security
Malware detection	Antivirus alert	System isolation	SOC → IT Security
Data exfiltration	Large data transfer	Block connection	SOC → CISO
Privileged action	Root/Admin action	Logging, review	SOC
Firewall rule change	Configuration change	Validation	SOC → Network Team

High Alerts: - Admin login outside business hours - Access to CHD - Configuration changes - New software installation

Medium Alerts: - Failed authentication - Password change - Account lockout

Low Alerts: - Informational events - Routine activities

11.7.3 7.3 Alert Response

Process: 1. Receive alert 2. Assess severity 3. Initial investigation 4. Escalation (if required) 5. Incident response (if required) 6. Documentation 7. Follow-up

Response Times: - Critical: Immediate (< 15 minutes) - High: < 1 hour - Medium: < 4 hours - Low: < 24 hours

11.8 8. Log Review

11.8.1 8.1 Daily Log Review

Process: - Automated analysis by SIEM - Review critical alerts - Identify anomalies - Document findings

Responsible: SOC Team

11.8.2 8.2 Weekly Log Review

Process: - Review all alerts of the week - Trend analysis - Identify patterns - Optimize alerting rules

Responsible: Senior SOC Analyst

11.8.3 8.3 Monthly Log Review

Process: - Comprehensive analysis of all logs - Compliance validation - Reporting to management - Identify improvements

Responsible: IT Security Manager

11.9 9. Use Cases and Correlation Rules

11.9.1 9.1 Defined Use Cases

Authentication: - Brute-force attacks - Credential stuffing - Unusual login times - Geographic anomalies

Access Control: - Unauthorized access - Privilege escalation - Lateral movement

Data Exfiltration: - Large data transfers - Unusual data access - Access to many records

Malware: - Antivirus detections - Suspicious processes - Command & Control communication

Insider Threats: - Unusual user activities - Access outside working hours - Mass downloads

11.9.2 9.2 Correlation Rules

Example Rule: Brute-Force Attack

```
IF (failed_logins > 10 IN 5 minutes)
AND (same_source_ip)
THEN
  ALERT "Brute-force attack detected"
  SEVERITY = CRITICAL
  ACTION = Block_IP
```

Example Rule: Privilege Escalation

```
IF (user_receives_admin_rights)
AND (user_performs_privileged_action IN 10 minutes)
THEN
  ALERT "Possible privilege escalation"
  SEVERITY = HIGH
  ACTION = Investigate
```

11.10 10. Audit Trails

11.10.1 10.1 Audit Trail Requirements

For All CHD Access: - Complete audit trails - Immutable - Traceable - Chronologically ordered

Information: - Who accessed? - When was access? - Which data was accessed? - Which action was performed? - Was the action successful?

11.10.2 10.2 Audit Trail Review

Process: - Regular review (daily for critical systems) - Identify anomalies - Document findings - Follow-up on anomalies

11.11 11. Forensic Investigations

11.11.1 11.1 Log Analysis for Forensics

Process: 1. Incident identified 2. Collect relevant logs 3. Create timeline 4. Root cause analysis 5. Documentation 6. Lessons learned

Tools: - SIEM forensic functions - Log analysis tools - Timeline analysis tools

11.11.2 11.2 Chain of Custody

Requirements: - Document all log access - Immutability of logs - Traceable chain of evidence - Legally sound documentation

11.12 12. Compliance Validation

11.12.1 12.1 Validation Activities

Daily: - Log review - Alert response - Anomaly detection

Weekly: - Trend analysis - Use case validation

Monthly: - Comprehensive log review - Compliance reporting

Quarterly: - Log retention validation - SIEM configuration review

Annually: - Complete logging audit - Penetration testing - Compliance assessment

11.12.2 12.2 Validation Documentation

Required Evidence: - Logging configuration - SIEM configuration - Log review protocols - Alert response protocols - Forensic investigation reports

---

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 12

Network Security Testing

Document ID: PCI-0510
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

12.1 1. Purpose

This document defines the network security testing requirements for AdminSend GmbH in accordance with PCI-DSS Requirement 11.

12.1.1 1.1 Objectives

- **Vulnerability Identification:** Regular vulnerability scans
- **Penetration Testing:** Annual security tests
- **Intrusion Detection:** IDS/IPS implementation
- **Compliance:** Fulfillment of PCI-DSS Requirement 11

12.1.2 1.2 Scope

Affected Systems: - All CDE systems - Perimeter systems - Internal networks - Web applications

12.2 2. Vulnerability Scanning

12.2.1 2.1 Quarterly Scans

Requirements: - Quarterly external scans by ASV - Quarterly internal scans - After significant changes - All systems in CDE

ASV (Approved Scanning Vendor): - Name: [TODO: ASV name] - Contact: [TODO: Contact] - Last scan: [TODO: Date] - Next scan: [TODO: Date]

12.2.2 2.2 External Vulnerability Scans

Process: 1. Commission ASV scan 2. Perform scan 3. Analyze results 4. Remediate vulnerabilities 5. Perform re-scan 6. Achieve passing scan 7. Archive ASV report

Passing Scan Criteria: - No vulnerabilities with CVSS 4.0 - All critical vulnerabilities remediated - ASV confirmation

12.2.3 2.3 Internal Vulnerability Scans

Process: - Quarterly scans of all internal systems - Authenticated scans (with credentials) - Complete network scans - Vulnerability prioritization - Remediation plan

Scan Tool: [TODO: Name of scan tool]

Scan Scope: - All CDE systems - All systems with CHD access - Network components - Databases - Web applications

12.2.4 2.4 Vulnerability Management

Prioritization:

CVSS Score	Severity	Remediation Deadline
9.0 - 10.0	Critical	7 days
7.0 - 8.9	High	30 days
4.0 - 6.9	Medium	90 days
0.1 - 3.9	Low	180 days

Remediation Process: 1. Vulnerability identified 2. Risk assessment 3. Create remediation plan 4. Implement patch/fix 5. Validation 6. Documentation

12.3 3. Penetration Testing

12.3.1 3.1 Annual Penetration Tests

Requirements: - Annually by qualified testers - After significant changes - External and internal tests - Network and application tests

Penetration Testing Firm: - Name: [TODO: Company] - Contact: [TODO: Contact] - Last test: [TODO: Date] - Next test: [TODO: Date]

12.3.2 3.2 External Penetration Tests

Scope: - Perimeter systems - Publicly accessible web applications - VPN access - Email systems

Methodology: - Black-box testing - Exploitation of vulnerabilities - Social engineering (optional) - Documentation of all findings

12.3.3 3.3 Internal Penetration Tests

Scope: - CDE network - Internal applications - Lateral movement tests - Privilege escalation

Methodology: - Gray-box testing - Authenticated tests - Exploitation - Post-exploitation

12.3.4 3.4 Segmentation Testing

Requirements: - Validation of network segmentation - Attempts to cross CDE boundaries - Firewall rule validation - Documentation of results

Process: 1. Document segmentation 2. Define test scenarios 3. Perform penetration test 4. Analyze results 5. Remediate vulnerabilities 6. Re-test 7. Documentation

12.4 4. Intrusion Detection/Prevention

12.4.1 4.1 IDS/IPS Implementation

Requirements: - IDS/IPS at all CDE boundaries - Real-time monitoring - Automatic alerts - Regular signature updates

IDS/IPS Systems:

System	Type	Location	Function
[TODO: IDS-01]	Network IDS	Perimeter	Detection
[TODO: IPS-01]	Network IPS	CDE boundary	Prevention
[TODO: HIDS-01]	Host IDS	CDE servers	Detection

12.4.2 4.2 IDS/IPS Signatures

Requirements: - Current signatures - Daily updates - Custom signatures for known threats - Regular review

Update Process: 1. Download signature updates 2. Test in test environment 3. Deploy to production 4. Validation 5. Documentation

12.4.3 4.3 IDS/IPS Alerting

Alert Categories: - Critical: Immediate action required - High: Investigation within 1 hour - Medium: Investigation within 4 hours - Low: Review within 24 hours

Alert Response: - Automatic notification to SOC - Initial investigation - Escalation if needed - Incident response - Documentation

12.5 5. File Integrity Monitoring (FIM)

12.5.1 5.1 FIM Implementation

Requirements: - FIM on all CDE systems - Monitoring of critical files - Real-time monitoring - Automatic alerts

FIM Tool: [TODO: Name of FIM tool]

12.5.2 5.2 Monitored Files

Critical Files: - System files - Configuration files - Application files - Log files - Database files

Examples: - `/etc/passwd`, `/etc/shadow` (Linux) - `C:\Windows\System32\config\SAM` (Windows) - Firewall configurations - Web server configurations - Database configurations

12.5.3 5.3 FIM Alerting

Alerts on: - File changes - File deletions - New files - Permission changes - Owner changes

Alert Response: 1. Receive alert 2. Validate change 3. Authorized change? (Change Request) 4. If unauthorized: Incident response 5. Documentation

12.6 6. Change Detection

12.6.1 6.1 Change Detection Mechanisms

Requirements: - Automatic detection of changes - Comparison with baseline - Alerting on unauthorized changes - Documentation of all changes

Monitored Changes: - Configuration changes - Software installations - Patch installations - User changes - Permission changes

12.6.2 6.2 Baseline Management

Process: 1. Create initial baseline 2. Document baseline 3. Regular validation 4. Update after approved changes 5. Documentation

Baseline Components: - System configuration - Installed software - Network configuration - Users and permissions - Services and processes

12.7 7. Wireless Security Testing

12.7.1 7.1 Wireless Access Point Detection

Requirements: - Quarterly scans for wireless APs - Detection of rogue APs - Validation of authorized APs - Documentation

Scan Methods: - Wireless scanners - Physical inspections - Network scans

12.7.2 7.2 Wireless Security Standards

Requirements for Authorized WLANs: - WPA3 or WPA2 with AES - Strong authentication (802.1X) - Separate VLAN for WLAN - No connection to CDE without additional controls

12.8 8. Web Application Security Testing

12.8.1 8.1 Application Security Tests

Requirements: - Annual security tests - After significant changes - OWASP Top 10 coverage - Authenticated and unauthenticated tests

Test Methods: - Automated scans (DAST) - Manual penetration tests - Code reviews (SAST) - Fuzzing

12.8.2 8.2 OWASP Top 10

Vulnerabilities to Test: 1. Broken Access Control 2. Cryptographic Failures 3. Injection 4. Insecure Design 5. Security Misconfiguration 6. Vulnerable and Outdated Components 7. Identification and Authentication Failures 8. Software and Data Integrity Failures 9. Security Logging and Monitoring Failures 10. Server-Side Request Forgery (SSRF)

12.9 9. Social Engineering Testing

12.9.1 9.1 Phishing Simulations

Requirements: - Regular phishing tests - Various scenarios - Employee awareness - Documentation of results

Process: 1. Plan phishing campaign 2. Send emails 3. Measure click rates 4. Train employees 5. Documentation

12.9.2 9.2 Physical Social Engineering

Tests: - Tailgating attempts - Badge cloning - Dumpster diving - Pretexting

Documentation: - Successful attacks - Identify vulnerabilities - Improvement measures - Employee awareness

12.10 10. Compliance Validation

12.10.1 10.1 Validation Activities

Quarterly: - Vulnerability scans (external and internal) - Wireless AP scans - FIM validation

Annually: - Penetration tests (external and internal) - Segmentation tests - Web application security tests - Social engineering tests

12.10.2 10.2 Validation Documentation

Required Evidence: - ASV scan reports (4 per year) - Internal scan reports (4 per year) - Penetration test reports (1 per year) - Segmentation test reports - FIM configuration and logs - IDS/IPS configuration and logs

---

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 13

Information Security Policy

Document ID: PCI-0600
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

13.1 1. Purpose

This document defines the information security policy for AdminSend GmbH in accordance with PCI-DSS Requirement 12.

13.1.1 1.1 Objectives

- **Security Governance:** Establish a security framework
- **Risk Management:** Systematic risk identification and treatment
- **Compliance:** Fulfillment of PCI-DSS Requirement 12
- **Awareness:** Sensitization of all employees

13.1.2 1.2 Scope

Affected Persons: - All employees - All service providers - All persons with access to CDE or CHD

13.2 2. Information Security Policy

13.2.1 2.1 Security Objectives

Confidentiality: - Protection of cardholder data from unauthorized access - Access control according to need-to-know principle - Encryption of sensitive data

Integrity: - Protection against unauthorized modification - Validation of data changes - Audit trails for all changes

Availability: - Ensuring system availability - Business continuity planning - Disaster recovery

13.2.2 2.2 Security Principles

Defense in Depth: - Multi-layered security controls - No single point of failure - Redundancy of critical systems

Least Privilege: - Minimum required permissions - Regular review - Time-limited privileged access

Separation of Duties: - Separation of critical functions - Four-eyes principle - No single person with complete control

Secure by Default: - Secure default configurations - Deactivation of unnecessary services - Hardening of all systems

13.3 3. Roles and Responsibilities

13.3.1 3.1 Governance Structure

Executive Management: - Overall responsibility for information security - Approval of security policies - Provision of resources

CISO (Chief Information Security Officer): - Responsible for security program - Compliance monitoring - Incident response coordination - Reporting to executive management

PCI-DSS Program Manager: - Responsible for PCI-DSS compliance - Coordination of assessments - Documentation and evidence - Liaison to QSA and acquiring banks

IT Security Team: - Implementation of security controls - Security monitoring - Vulnerability management - Incident response

IT Operations: - System administration - Patch management - Backup and recovery - Change management

All Employees: - Compliance with security policies - Reporting of security incidents - Participation in security awareness training

13.3.2 3.2 RACI Matrix

Activity	Executive	CISO	PCI Manager	IT Security	IT Ops	Employees
Policy approval	A	R	C	C	I	I
Security controls	C	A	C	R	R	I
Compliance monitoring	I	A	R	C	I	I
Incident response	I	A	C	R	C	R

Activity	Executive	CISO	PCI Manager	IT Security	IT Ops	Employees
Security awareness	C	A	C	R	I	R

Legend: R = Responsible, A = Accountable, C = Consulted, I = Informed

13.4 4. Risk Management

13.4.1 4.1 Risk Analysis Process

Annual Risk Analysis: 1. Asset identification 2. Threat identification 3. Vulnerability analysis 4. Risk assessment 5. Risk treatment 6. Documentation

Risk Assessment: - Likelihood (1-5) - Impact (1-5) - Risk Score = Likelihood × Impact

Risk Matrix:

Risk Score	Category	Treatment
20-25	Critical	Immediate measures
15-19	High	Measures within 30 days
10-14	Medium	Measures within 90 days
5-9	Low	Monitoring
1-4	Very low	Accept

13.4.2 4.2 Risk Treatment

Options: - **Avoid:** Discontinue activity - **Reduce:** Implement controls - **Transfer:** Insurance, outsourcing - **Accept:** Consciously accept risk (with approval)

Risk Acceptance: - Only by CISO or executive management - Documented justification - Regular review - Time-limited

13.5 5. Security Awareness Program

13.5.1 5.1 Training Program

Mandatory Training: - Onboarding training (upon hiring) - Annual refresher training - Role-specific training - Ad-hoc training as needed

Training Content: - PCI-DSS basics - Handling cardholder data - Password security - Phishing recognition - Social engineering - Incident reporting - Clean desk policy - Acceptable use policy

13.5.2 5.2 Training Documentation

Required Evidence: - Training attendance lists - Training materials - Training certificates - Knowledge tests - Refresher training

Tracking: - Training database - Automatic reminders - Compliance reporting

13.5.3 5.3 Awareness Campaigns

Regular Campaigns: - Monthly security newsletters - Phishing simulations - Security posters - Intranet articles - Team meetings

13.6 6. Incident Response

13.6.1 6.1 Incident Response Plan

Phases: 1. **Preparation:** Preparation and training 2. **Detection:** Detection of incidents 3. **Analysis:** Analysis and assessment 4. **Containment:** Containment 5. **Eradication:** Eradication 6. **Recovery:** Recovery 7. **Post-Incident:** Lessons learned

Incident Response Team: - Incident Response Manager - IT Security Analysts - IT Operations - Legal/Compliance - PR/Communications - Executive Management (for major incidents)

13.6.2 6.2 Incident Classification

Severity Levels:

Severity	Description	Examples	Response Time
Critical	Massive impact	Data exfiltration, ransomware	Immediate
High	Significant impact	Malware infection, unauthorized access	$<$ 1 hour
Medium	Moderate impact	Phishing success, policy violation	$<$ 4 hours
Low	Minor impact	Suspicious activity	$<$ 24 hours

13.6.3 6.3 Incident Reporting

Reporting Obligation: - All employees must report incidents - Report to IT Security or Helpdesk - No fear of consequences for reporting - Quick reporting is important

Reporting Channels: - Email: [TODO: security@organization.com] - Phone: [TODO: +1 XXX XXX XXXX] - Incident portal: [TODO: URL] - Helpdesk: [TODO: Phone]

13.6.4 6.4 Breach Notification

For Data Breaches: - Notification of acquiring banks - Notification of card brands - Notification of data protection authority (GDPR) - Notification of affected cardholders - Forensic investigation

Timeframe: - Acquiring banks: Immediately - Card brands: According to requirements - Data protection authority: 72 hours (GDPR) - Cardholders: Without undue delay

13.7 7. Service Provider Management

13.7.1 7.1 Service Provider Selection

Due Diligence: - Check PCI-DSS compliance status - Request AOC (Attestation of Compliance) - Assess security controls - Contractual security requirements

Requirements: - PCI-DSS compliant (if CHD access) - Current AOC - Incident response process - Insurance

13.7.2 7.2 Service Provider Monitoring

Annual Review: - AOC validation - Security controls review - Incident review - Contract compliance

Documentation: - List of all service providers - AOCs - Contracts with PCI clauses - Review protocols

13.7.3 7.3 Service Provider Contracts

Required Clauses: - PCI-DSS compliance obligation - Incident notification - Audit rights - Data protection (GDPR) - Liability - Termination for non-compliance

13.8 8. Document Management

13.8.1 8.1 Document Control

Requirements: - Version control - Approval process - Regular reviews - Archiving of old versions

Document Lifecycle: 1. Creation 2. Review 3. Approval 4. Publication 5. Annual review 6. Update or archiving

13.8.2 8.2 Document Retention

Retention Periods: - Policies: Current + 3 years - Audit reports: 3 years - Logs: 1 year - Incident reports: 3 years - Training records: 3 years

13.9 9. Compliance Monitoring

13.9.1 9.1 Continuous Monitoring

Monitoring Activities: - Daily security monitoring - Weekly compliance checks - Monthly compliance reports - Quarterly reviews - Annual assessments

13.9.2 9.2 Compliance Reporting

Reports: - Monthly compliance status to CISO - Quarterly report to executive management - Annual compliance report - Ad-hoc reports for incidents

13.9.3 9.3 Internal Audits

Annual Audits: - All PCI-DSS requirements - Sample-based - Documentation of findings - Corrective actions - Follow-up

13.10 10. Policy Review

13.10.1 10.1 Annual Review

Process: 1. Review all policies 2. Identify changes 3. Make updates 4. Obtain approval 5. Communicate to employees 6. Update training

Responsible: CISO

13.10.2 10.2 Ad-hoc Reviews

Triggers: - Significant changes in CDE - New threats - Regulatory changes - After major incidents - Audit findings

13.11 11. Compliance Validation

13.11.1 11.1 Validation Activities

Quarterly: - Policy compliance checks - Training status review - Service provider AOC validation

Annually: - Complete risk analysis - Internal audits - QSA assessment - Policy review

13.11.2 11.2 Validation Documentation

Required Evidence: - Information security policy - Risk analysis reports - Training records - Incident response protocols - Service provider AOCs - Audit reports

---

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage

Chapter 14

Appendix: Evidence Register

Document ID: PCI-0700
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

14.1 1. Purpose

This document serves as a central register of all evidence for PCI-DSS compliance of AdminSend GmbH.

14.1.1 1.1 Usage

- **Audit Preparation:** Quick access to all evidence
- **Compliance Tracking:** Overview of document status
- **Gap Analysis:** Identification of missing evidence

14.2 2. Evidence Register by Requirements

14.2.1 2.1 Requirement 1: Firewall and Network Security

Evidence	Document	Location	Last Updated	Status
Firewall configuration	PCI-0100	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Firewall ruleset	Firewall-Rules.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Network diagram	Network-Diagram.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]

Evidence	Document	Location	Last Updated	Status
Quarterly rule reviews	FW-Review-Q1-2026.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Change logs	Change-Log-2026.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]

14.2.2 2.2 Requirement 2: Secure Configurations

Evidence	Document	Location	Last Updated	Status
Hardening standards	Hardening-Guide.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Configuration baselines	Config-Baselines.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Vendor default accounts	Default-Accounts.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
System inventory	Asset-Inventory.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]

14.2.3 2.3 Requirement 3: Protection of Stored Cardholder Data

Evidence	Document	Location	Last Updated	Status
Data retention policy	Data-Retention-Policy.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Encryption standards	Encryption-Standards.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Key management procedures	Key-Management.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
CHD inventory	CHD-Inventory.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Data flow diagrams	Data-Flow-Diagrams.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]

14.2.4 2.4 Requirement 4: Encryption of Transmission

Evidence	Document	Location	Last Updated	Status
Encryption policy	Transmission-Encryption.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
TLS configurations	TLS-Config.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Certificate management	Certificate-Management.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]

Evidence	Document	Location	Last Updated	Status
Scan reports (TLS)	TLS-Scan-Report.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]

14.2.5 2.5 Requirement 5: Malware Protection

Evidence	Document	Location	Last Updated	Status
Antivirus policy	Antivirus-Policy.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
AV configuration	AV-Configuration.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
AV update logs	AV-Update-Logs.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Malware detections	Malware-Incidents.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]

14.2.6 2.6 Requirement 6: Secure Systems and Applications

Evidence	Document	Location	Last Updated	Status
Patch management policy	Patch-Management.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Patch logs	Patch-Logs-2026.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Vulnerability scan reports	Vuln-Scan-Q1-2026.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Secure SDLC policy	Secure-SDLC.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Code review reports	Code-Review-2026.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Change management logs	Change-Management-2026.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]

14.2.7 2.7 Requirement 7: Access Control

Evidence	Document	Location	Last Updated	Status
Access control policy	PCI-0400	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Permission matrix	Access-Matrix.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Access requests	Access-Requests-2026.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]

Evidence	Document	Location	Last Updated	Status
Quarterly access reviews	Access-Review-Q1-2026.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Recertification evidence	Recertification-2026.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]

14.2.8 2.8 Requirement 8: Identification and Authentication

Evidence	Document	Location	Last Updated	Status
Authentication policy	PCI-0410	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Password policy	Password-Policy.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
MFA configuration	MFA-Configuration.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
User inventory	User-Inventory.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Account management logs	Account-Management-2026.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]

14.2.9 2.9 Requirement 9: Physical Security

Evidence	Document	Location	Last Updated	Status
Physical security policy	PCI-0420	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Access control logs	Access-Control-Logs-2026.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Visitor logs	Visitor-Logs-2026.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
POS inspection logs	POS-Inspection-Q1-2026.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Media destruction certificates	Media-Destruction-2026.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Video surveillance logs	CCTV-Logs-2026.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]

14.2.10 2.10 Requirement 10: Logging and Monitoring

Evidence	Document	Location	Last Updated	Status
Logging policy	PCI-0500	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]

Evidence	Document	Location	Last Updated	Status
SIEM configuration	SIEM-Configuration.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Log review protocols	Log-Review-2026.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Alerting rules	Alerting-Rules.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Incident response logs	Incident-Response-2026.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
NTP configuration	NTP-Configuration.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]

14.2.11 2.11 Requirement 11: Security Testing

Evidence	Document	Location	Last Updated	Status
Security testing policy	PCI-0510	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
ASV scan reports	ASV-Scan-Q1-2026.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Internal scan reports	Internal-Scan-Q1-2026.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Penetration test reports	Pentest-2026.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Segmentation test reports	Segmentation-Test-2026.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
FIM configuration	FIM-Configuration.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
IDS/IPS configuration	IDS-IPS-Configuration.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Wireless scan reports	Wireless-Scan-Q1-2026.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]

14.2.12 2.12 Requirement 12: Information Security Policy

Evidence	Document	Location	Last Updated	Status
Information security policy	PCI-0600	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Risk assessment reports	Risk-Assessment-2026.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Training records	Training-Records-2026.xlsx	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]

Evidence	Document	Location	Last Updated	Status
Incident response plan	Incident-Response-Plan.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Service provider AOCs	Vendor-AOCs-2026.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Service provider contracts	Vendor-Contracts.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
Internal audit reports	Internal-Audit-2026.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]
QSA assessment reports	QSA-Report-2026.pdf	[TODO: Path]	[TODO: Date]	[TODO: Current/Outdated]

14.3 3. Document Status Tracking

14.3.1 3.1 Document Lifecycle

Status	Description	Next Action
Current	Document is current and valid	Annual review
Review due	Annual review is due	Perform review
Outdated	Document is no longer current	Update required
In progress	Document is being updated	Complete
Missing	Document does not exist	Creation required

14.3.2 3.2 Review Schedule

Document Type	Review Frequency	Responsible
Policies	Annually	CISO
Procedures	Annually	IT Security Manager
Configurations	Quarterly	IT Operations
Scan reports	Quarterly	IT Security
Audit reports	After each audit	PCI Manager

14.4 4. Audit Preparation

14.4.1 4.1 Checklist for QSA Assessment

- ☐ All evidence current
- ☐ All documents accessible
- ☐ All reviews performed
- ☐ All scans current (< 90 days)
- ☐ All training documented
- ☐ All incidents documented
- ☐ All service provider AOCs current
- ☐ All change logs complete

14.4.2 4.2 Missing Evidence

Requirement	Missing Evidence	Priority	Due Date	Responsible
[TODO]	[TODO]	[TODO: High/Medium/Low]	[TODO: Date]	[TODO: Name]

14.5 5. Document Archiving

14.5.1 5.1 Archiving Policy

Retention Periods: - Policies: Current + 3 years - Audit reports: 3 years - Scan reports: 1 year - Logs: 1 year - Training records: 3 years - Incident reports: 3 years

Archive Location: [TODO: Location for archived documents]

14.5.2 5.2 Archived Documents

Document	Archive Date	Retention Until	Location
[TODO]	[TODO: Date]	[TODO: Date]	[TODO: Path]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ vuln_defaults.author }}	Initial creation

ewpage

Chapter 15

Appendix: Glossary and Abbreviations

Document ID: PCI-0710
Organization: AdminSend GmbH
Owner: IT Operations Manager
Approved by: CIO
Version: 1.0.0
Status: Draft / In Review / Approved
Classification: internal
Last Updated: {{ meta.document.last_updated }}

15.1 1. Purpose

This document defines all terms and abbreviations used in the PCI-DSS documentation of AdminSend GmbH.

15.2 2. PCI-DSS Terms

15.2.1 A

Acquiring Bank (Acquirer) - Bank that processes payment card transactions for merchants - Responsible for merchant's PCI-DSS compliance

AOC (Attestation of Compliance) - Confirmation of PCI-DSS compliance - Issued by QSA or through self-assessment

ASV (Approved Scanning Vendor) - Vendor approved by PCI SSC for vulnerability scans - Performs quarterly external scans

Authentication - Process of identity verification - Typically through password, token, or biometrics

Authorization - Process of permission verification - Determines which actions a user may perform

15.2.2 C

Cardholder Data (CHD) - Cardholder data - Includes PAN, cardholder name, expiration date, service code

Cardholder Data Environment (CDE) - Environment that stores, processes, or transmits cardholder data - Includes systems, networks, people, and processes

CDE Segmentation - Network segmentation to isolate CDE - Reduces compliance scope

CVV/CVC/CVV2/CVC2 - Card Verification Value/Code - 3-4 digit security code - Must NOT be stored after authorization

15.2.3 D

Data Retention - Data retention policy - Defines how long data may be stored

Default Account - Vendor pre-configured account - Must be disabled or password changed

DMZ (Demilitarized Zone) - Network segment between internet and internal network - For publicly accessible services

15.2.4 E

Encryption - Encryption of data - Required for stored and transmitted CHD

Encryption Key - Key for encryption and decryption - Must be securely stored and managed

15.2.5 F

FIM (File Integrity Monitoring) - File integrity monitoring - Detects unauthorized changes to critical files

Firewall - Network security device - Controls traffic between network segments

15.2.6 H

Hashing - One-way encryption - For password storage

Hardening - System hardening - Removal of unnecessary services and functions

15.2.7 I

IDS/IPS (Intrusion Detection/Prevention System) - System for detecting and preventing attacks - Required at all CDE boundaries

Incident Response - Response to security incidents - Structured process for handling incidents

15.2.8 K

Key Management - Management of cryptographic keys - Includes generation, storage, rotation, destruction

15.2.9 L

Least Privilege - Principle of minimum permissions - Users receive only required access rights

Logging - Recording of events - Required for all access to CDE and CHD

15.2.10 M

Malware - Malicious software - Viruses, trojans, ransomware, etc.

Merchant - Merchant that accepts payment cards - Subject to PCI-DSS compliance

MFA (Multi-Factor Authentication) - Multi-factor authentication - Required for CDE access

15.2.11 N

Need-to-Know - Principle of authorized knowledge - Access only with business necessity

Network Segmentation - Network segmentation - Separation of CDE and corporate network

NTP (Network Time Protocol) - Protocol for time synchronization - Required for correct timestamps in logs

15.2.12 P

PA-DSS (Payment Application Data Security Standard) - Security standard for payment applications - Complements PCI-DSS

PAN (Primary Account Number) - Primary account number - 13-19 digit card number - Core of cardholder data

Penetration Test - Security test through simulated attacks - Required annually

PCI DSS (Payment Card Industry Data Security Standard) - Security standard for payment card industry - Defines requirements for protecting cardholder data

PCI SSC (Payment Card Industry Security Standards Council) - Organization that develops and manages PCI-DSS

POS (Point of Sale) - Point of sale - Terminal for card input

15.2.13 Q

QSA (Qualified Security Assessor) - Qualified security assessor - Performs PCI-DSS assessments

15.2.14 R

RBAC (Role-Based Access Control) - Role-based access control - Permissions based on roles

Risk Assessment - Risk analysis - Required annually

ROC (Report on Compliance) - Compliance report - Created by QSA after assessment

15.2.15 S

SAD (Sensitive Authentication Data) - Sensitive authentication data - Full track data, CVV, PIN - Must NOT be stored after authorization

SAQ (Self-Assessment Questionnaire) - Self-assessment questionnaire - For smaller merchants without QSA assessment

Scope - Scope of PCI-DSS compliance - All systems that store, process, or transmit CHD

Segmentation - See Network Segmentation

Service Provider - Service provider that processes CHD on behalf - Subject to PCI-DSS compliance

SIEM (Security Information and Event Management) - System for central log management and analysis

Strong Cryptography - Strong encryption - At least AES-128, RSA-2048

15.2.16 T

Tokenization - Replacement of PAN with token - Reduces compliance scope

TLS (Transport Layer Security) - Encryption protocol for data transmission - At least TLS 1.2 required

Track Data - Magnetic stripe data - Track 1 and Track 2 - Must NOT be stored after authorization

15.2.17 V

Vulnerability - Vulnerability in system or application - Must be identified and remediated

Vulnerability Scan - Vulnerability scan - Required quarterly (external and internal)

15.2.18 W

WAF (Web Application Firewall) - Firewall for web applications - Protection against OWASP Top 10

WORM (Write Once Read Many) - Storage that can only be written once - For log storage to ensure integrity

15.3 3. Abbreviations

Abbreviation	Meaning
ACL	Access Control List
AES	Advanced Encryption Standard
AOC	Attestation of Compliance
API	Application Programming Interface
ASV	Approved Scanning Vendor
AV	Antivirus
BAA	Business Associate Agreement

Abbreviation	Meaning
CA	Certificate Authority
CDE	Cardholder Data Environment
CHD	Cardholder Data
CISO	Chief Information Security Officer
CRL	Certificate Revocation List
CVV	Card Verification Value
CVSS	Common Vulnerability Scoring System
DAST	Dynamic Application Security Testing
DBA	Database Administrator
DMZ	Demilitarized Zone
DPA	Data Processing Agreement
EAL	Evaluation Assurance Level
EDR	Endpoint Detection and Response
FIM	File Integrity Monitoring
GDPR	General Data Protection Regulation
HIDS	Host-based Intrusion Detection System
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
JIT	Just-in-Time
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
NIDS	Network-based Intrusion Detection System
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OS	Operating System
OWASP	Open Web Application Security Project
PA-DSS	Payment Application Data Security Standard
PAM	Privileged Access Management
PAN	Primary Account Number
PCI DSS	Payment Card Industry Data Security Standard
PCI SSC	Payment Card Industry Security Standards Council
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
POS	Point of Sale
QSA	Qualified Security Assessor
RACI	Responsible, Accountable, Consulted, Informed
RBAC	Role-Based Access Control
RFC	Request for Comments

Abbreviation	Meaning
ROC	Report on Compliance
RPO	Recovery Point Objective
RSA	Rivest-Shamir-Adleman (encryption algorithm)
RTO	Recovery Time Objective
SAD	Sensitive Authentication Data
SAQ	Self-Assessment Questionnaire
SAST	Static Application Security Testing
SDLC	Software Development Lifecycle
SIEM	Security Information and Event Management
SOC	Security Operations Center
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer (deprecated, replaced by TLS)
SSO	Single Sign-On
TLS	Transport Layer Security
TOE	Target of Evaluation
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAF	Web Application Firewall
WORM	Write Once Read Many

15.4 4. Organization-Specific Terms

[TODO: Add organization-specific terms and abbreviations here]

Term/Abbreviation	Meaning
[TODO]	[TODO]

Document History:

Version	Date	Author	Changes
0.1	{{ meta.document.last_updated }}	{{ defaults.author }}	Initial creation

ewpage