Contents

1 PCI-DSS Compliance Handbuch **5**

2 Geltungsbereich und CDE-Definition **6**
2.1 1. Zweck . . . 6
2.2 2. Merchant/Service Provider Information . . . 7
2.3 3. Cardholder Data Environment (CDE) . . . 7
2.4 4. CDE-Systeme und -Komponenten . . . 8
2.5 5. Standorte und Lokationen . . . 8
2.6 6. Datenflüsse . . . 9
2.7 7. Scope-Ausschlüsse . . . 10
2.8 8. Netzwerksegmentierung . . . 10
2.9 9. Personal mit CDE-Zugriff . . . 10
2.10 10. Scope-Änderungen . . . 11
2.11 11. Compliance-Verantwortlichkeiten . . . 11

3 Netzwerksegmentierung **13**
3.1 1. Zweck . . . 13
3.2 2. Netzwerkarchitektur . . . 13
3.3 3. Firewall-Konfiguration . . . 14
3.4 4. Router-Konfiguration . . . 15
3.5 5. Segmentierungsvalidierung . . . 16
3.6 6. Wireless Networks . . . 16
3.7 7. Remote Access . . . 17
3.8 8. Monitoring und Alerting . . . 18
3.9 9. Änderungsmanagement . . . 18

4 Rollen und Verantwortlichkeiten **20**
4.1 1. Zweck . . . 20
4.2 2. Organisationsstruktur . . . 20
4.3 3. Externe Rollen . . . 22
4.4 4. RACI-Matrizen . . . 23
4.5 5. Eskalationspfade . . . 25
4.6 6. Schulung und Awareness . . . 25

5 Datenfluss-Diagramme **27**
5.1 1. Zweck . . . 27
5.2 2. Datenfluss-Übersicht . . . 27

5.3 3. Detaillierte Datenflüsse 28
5.4 4. Systemübersicht 29
5.5 5. Datenspeicherung 29
5.6 6. Externe Datenflüsse 30
5.7 7. Datenfluss-Änderungsmanagement 30

6 Compliance-Programm **32**
6.1 1. Zweck 32
6.2 2. Compliance-Governance 32
6.3 3. Compliance-Aktivitäten 33
6.4 4. Compliance-Metriken und KPIs 34
6.5 5. Audit und Assessment 34
6.6 6. Risikomanagement 35
6.7 7. Incident Response 35
6.8 8. Schulung und Awareness 36
6.9 9. Dokumentenmanagement 36
6.10 10. Kontinuierliche Verbesserung 37

7 Firewall-Konfiguration **38**
7.1 1. Zweck 38
7.2 2. Firewall-Standards 38
7.3 3. Firewall-Regelmanagement 39
7.4 4. Firewall-Konfigurationsstandards 40
7.5 5. Verbotene Konfigurationen 41
7.6 6. Änderungsmanagement 41
7.7 7. Monitoring und Alerting 42
7.8 8. Compliance-Validierung 42

8 Zugriffskontrolle **43**
8.1 1. Zweck 43
8.2 2. Zugriffskontrollprinzipien 43
8.3 3. Rollenbasierte Zugriffskontrolle (RBAC) 44
8.4 4. Zugriffsverwaltungsprozess 45
8.5 5. Privilegierte Zugriffe 46
8.6 6. Zugriffskontrolle für Karteninhaberdaten 46
8.7 7. Zugriffskontrolle für Anwendungen 47
8.8 8. Zugriffskontrolle für Datenbanken 47
8.9 9. Zugriffskontrolle für Netzwerk 48
8.10 10. Zugriffskontrolle für physischen Zugang 48
8.11 11. Zugriffskontrolle für Dienstleister 48
8.12 12. Zugriffskontrolle-Überwachung 48
8.13 13. Zugriffskontrolle-Reviews 49
8.14 14. Compliance-Validierung 49

9 Benutzerauthentifizierung **51**
9.1 1. Zweck 51
9.2 2. Benutzeridentifikation 51
9.3 3. Authentifizierungsmethoden 52

9.4 4. Account-Management . . . 53
9.5 5. Passwort-Management . . . 53
9.6 6. Session-Management . . . 54
9.7 7. Remote-Authentifizierung . . . 54
9.8 8. Anwendungs-Authentifizierung . . . 55
9.9 9. Service-Account-Management . . . 55
9.10 10. Authentifizierungs-Logging . . . 55
9.11 11. Authentifizierungs-Monitoring . . . 56
9.12 12. Vendor Default Accounts . . . 56
9.13 13. Authentifizierungs-Testing . . . 56
9.14 14. Compliance-Validierung . . . 57

10 Physische Sicherheit **58**
10.1 1. Zweck . . . 58
10.2 2. Physische Zutrittskontrolle . . . 58
10.3 3. Besuchermanagement . . . 59
10.4 4. Mitarbeiter-Identifikation . . . 60
10.5 5. Videoüberwachung . . . 60
10.6 6. Medien-Handling . . . 60
10.7 7. Medien-Vernichtung . . . 61
10.8 8. Point-of-Sale (POS) Sicherheit . . . 62
10.9 9. Medien-Backup . . . 62
10.1010. Arbeitsplatz-Sicherheit . . . 63
10.1111. Notfallzugang . . . 63
10.1212. Compliance-Validierung . . . 63

11 Logging und Monitoring **65**
11.1 1. Zweck . . . 65
11.2 2. Logging-Anforderungen . . . 65
11.3 3. SIEM-System . . . 66
11.4 4. Log-Retention . . . 67
11.5 5. Log-Integrität . . . 67
11.6 6. Zeitsynchronisation . . . 67
11.7 7. Monitoring und Alerting . . . 68
11.8 8. Log-Review . . . 68
11.9 9. Use Cases und Korrelationsregeln . . . 69
11.1010. Audit Trails . . . 70
11.1111. Forensische Untersuchungen . . . 70
11.1212. Compliance-Validierung . . . 70

12 Netzwerksicherheitstests **72**
12.1 1. Zweck . . . 72
12.2 2. Vulnerability Scanning . . . 72
12.3 3. Penetrationstests . . . 73
12.4 4. Intrusion Detection/Prevention . . . 74
12.5 5. File Integrity Monitoring (FIM) . . . 75
12.6 6. Change Detection . . . 75
12.7 7. Wireless Security Testing . . . 75

12.8 8. Web Application Security Testing . . . 76
12.9 9. Social Engineering Testing . . . 76
12.1010. Compliance-Validierung . . . 76

13 Informationssicherheitsrichtlinie 78
13.1 1. Zweck . . . 78
13.2 2. Informationssicherheitsrichtlinie . . . 78
13.3 3. Rollen und Verantwortlichkeiten . . . 79
13.4 4. Risikomanagement . . . 80
13.5 5. Security Awareness Program . . . 80
13.6 6. Incident Response . . . 81
13.7 7. Dienstleister-Management . . . 82
13.8 8. Dokumentenmanagement . . . 82
13.9 9. Compliance-Monitoring . . . 82
13.1010. Richtlinien-Review . . . 83
13.1111. Compliance-Validierung . . . 83

14 Anhang: Nachweisregister 84
14.1 1. Zweck . . . 84
14.2 2. Nachweisregister nach Requirements . . . 84
14.3 3. Dokumentenstatus-Tracking . . . 90
14.4 4. Audit-Vorbereitung . . . 91
14.5 5. Dokumenten-Archivierung . . . 91

15 Anhang: Glossar und Abkürzungen 93
15.1 1. Zweck . . . 93
15.2 2. PCI-DSS-Begriffe . . . 93
15.3 3. Abkürzungen . . . 97
15.4 4. Organisationsspezifische Begriffe . . . 98

Chapter 1

PCI-DSS Compliance Handbuch

Dokument-Metadaten

- **Erstellt am:** 2026-02-10
- **Autor:** Andreas Huemmer [andreas.huemmer@adminsend.de]
- **Version:** 0.0.5
- **Typ:** PCI-DSS-Handbuch

---

ewpage

Chapter 2

Geltungsbereich und CDE-Definition

Dokument-ID: PCI-0010
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

2.1 1. Zweck

Dieses Dokument definiert den Geltungsbereich der PCI-DSS-Compliance für AdminSend GmbH und beschreibt das Cardholder Data Environment (CDE).

2.1.1 1.1 Ziele

- **Scope-Definition:** Klare Abgrenzung des CDE vom restlichen Netzwerk
- **Compliance-Fokus:** Identifikation aller PCI-DSS-relevanten Systeme und Prozesse
- **Risikominimierung:** Reduktion des Compliance-Scope durch Segmentierung
- **Audit-Vorbereitung:** Dokumentation für QSA-Assessments

2.1.2 1.2 Referenzen

- **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 (falls zutreffend)

2.2 2. Merchant/Service Provider Information

2.2.1 2.1 Organisationsinformationen

Organisation: AdminSend GmbH
Adresse: Musterstraße 123, 80331 München
Land: Deutschland
Website: https://www.adminsend.de

2.2.2 2.2 PCI-DSS-Klassifizierung

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

Transaktionsvolumen (jährlich): - Visa: [TODO: Anzahl Transaktionen] - Mastercard: [TODO: Anzahl Transaktionen] - American Express: [TODO: Anzahl Transaktionen] - Discover: [TODO: Anzahl Transaktionen] - Gesamt: [TODO: Anzahl Transaktionen]

2.2.3 2.3 Acquiring Banks

Bank Name	Kontakt	Merchant ID	Kartenmarken
[TODO: Bank 1]	[TODO: Kontakt]	[TODO: ID]	Visa, Mastercard
[TODO: Bank 2]	[TODO: Kontakt]	[TODO: ID]	American Express

2.3 3. Cardholder Data Environment (CDE)

2.3.1 3.1 CDE-Definition

Das Cardholder Data Environment (CDE) umfasst:

1. **Systeme:** Alle Systeme, die Karteninhaberdaten (CHD) speichern, verarbeiten oder übertragen
2. **Netzwerke:** Alle Netzwerksegmente, die mit CDE-Systemen verbunden sind
3. **Personen:** Alle Mitarbeiter und Dienstleister mit Zugriff auf CHD
4. **Prozesse:** Alle Geschäftsprozesse, die CHD involvieren

2.3.2 3.2 Karteninhaberdaten (CHD)

Primäre Kontonummer (PAN): - 13-19-stellige Kartennummer - **Speicherung:** [TODO: Ja/Nein, wo?] - **Verschlüsselung:** [TODO: Algorithmus, z.B. AES-256]

Karteninhabername: - Name des Karteninhabers - **Speicherung:** [TODO: Ja/Nein, wo?]

Service Code: - 3-stelliger Code auf Magnetstreifen - **Speicherung:** [TODO: Ja/Nein, wo?]

Ablaufdatum: - Gültigkeitsdatum der Karte - **Speicherung:** [TODO: Ja/Nein, wo?]

2.3.3 3.3 Sensitive Authentication Data (SAD)

DARF NICHT nach Autorisierung gespeichert werden:

- **Full Track Data:** Magnetstreifendaten (Track 1, Track 2)
- **CAV2/CVC2/CVV2/CID:** Kartenprüfnummer (3-4 Stellen)
- **PIN/PIN Block:** PIN-Daten

Bestätigung: AdminSend GmbH speichert KEINE Sensitive Authentication Data nach Autorisierung. [TODO: Bestätigen]

2.4 4. CDE-Systeme und -Komponenten

2.4.1 4.1 Systeme im CDE

System-ID	Systemname	Typ	Funktion	CHD-Typ	Standort
[TODO: SYS-001]	[TODO: Payment Gateway]	Server	Zahlungsabwicklung	PAN, Name	[TODO: RZ1]
[TODO: SYS-002]	[TODO: POS-Terminal]	Endpoint	Karteneingabe	PAN	[TODO: Filiale 1]
[TODO: SYS-003]	[TODO: Datenbank]	Database	CHD-Speicherung	PAN (verschlüsselt)	[TODO: RZ1]
[TODO: SYS-004]	[TODO: Webserver]	Server	E-Commerce	PAN (Transit)	[TODO: RZ1]

2.4.2 4.2 Netzwerkkomponenten im CDE

Komponente	Typ	Funktion	Standort
[TODO: FW-CDE-01]	Firewall	CDE-Segmentierung	[TODO: RZ1]
[TODO: SW-CDE-01]	Switch	CDE-Netzwerk	[TODO: RZ1]
[TODO: RTR-CDE-01]	Router	CDE-Routing	[TODO: RZ1]
[TODO: IDS-CDE-01]	IDS/IPS	Intrusion Detection	[TODO: RZ1]

2.4.3 4.3 Anwendungen im CDE

Anwendung	Version	Hersteller	PA-DSS-zertifiziert	Funktion
[TODO: Payment App]	[TODO: v2.1]	[TODO: Vendor]	[TODO: Ja/Nein]	Zahlungsabwicklung
[TODO: POS-Software]	[TODO: v3.0]	[TODO: Vendor]	[TODO: Ja/Nein]	Point of Sale
[TODO: E-Commerce]	[TODO: v1.5]	[TODO: Vendor]	[TODO: Ja/Nein]	Online-Shop

2.5 5. Standorte und Lokationen

2.5.1 5.1 Physische Standorte mit CDE

Standort-ID	Standortname	Adresse	CDE-Systeme	Mitarbeiter mit CHD-Zugriff
[TODO: LOC-01]	Hauptsitz	[TODO: Adresse]	[TODO: Liste]	[TODO: Anzahl]
[TODO: LOC-02]	Rechenzentrum	[TODO: Adresse]	[TODO: Liste]	[TODO: Anzahl]
[TODO: LOC-03]	Filiale 1	[TODO: Adresse]	[TODO: POS]	[TODO: Anzahl]

2.5.2 5.2 Remote-Zugriff auf CDE

Remote-Zugriff erlaubt: [TODO: Ja/Nein]

Falls ja: - **Zugriffsmethode:** [TODO: VPN, Jump Server, etc.] - **Multi-Faktor-Authentifizierung:** [TODO: Ja/Nein, Methode] - **Berechtigte Benutzer:** [TODO: Rollen/Personen]

2.6 6. Datenflüsse

2.6.1 6.1 Karteninhaberdaten-Flüsse

[TODO: Fügen Sie Datenflussdiagramm ein - siehe PCI-0040]

Hauptdatenflüsse:

1. **Karteneingabe → Autorisierung:**
   - Quelle: [TODO: POS-Terminal/Webformular]
   - Ziel: [TODO: Payment Gateway]
   - Protokoll: [TODO: TLS 1.2+]
   - Verschlüsselung: [TODO: Ja/Nein]
2. **Autorisierung → Speicherung:**
   - Quelle: [TODO: Payment Gateway]
   - Ziel: [TODO: Datenbank]
   - Verschlüsselung: [TODO: AES-256]
   - Tokenisierung: [TODO: Ja/Nein]
3. **Reporting/Abfrage:**
   - Quelle: [TODO: Datenbank]
   - Ziel: [TODO: Reporting-System]
   - Maskierung: [TODO: Ja, nur letzte 4 Ziffern]

2.6.2 6.2 Externe Verbindungen

Verbindung	Quelle	Ziel	Zweck	Verschlüsselung
[TODO: Acquiring Bank]	CDE	Bank	Autorisierung	TLS 1.2+
[TODO: Payment Processor]	CDE	Processor	Abwicklung	TLS 1.2+
[TODO: ASV Scans]	Internet	CDE	Vulnerability Scans	N/A

2.7 7. Scope-Ausschlüsse

2.7.1 7.1 Systeme außerhalb des CDE

Folgende Systeme sind NICHT Teil des CDE:

System	Begründung	Segmentierung
[TODO: Intranet]	Keine CHD-Verarbeitung	Firewall-Trennung
[TODO: E-Mail-Server]	Keine CHD-Speicherung	Separate VLAN
[TODO: Entwicklungsumgebung]	Keine Produktionsdaten	Physisch getrennt

2.7.2 7.2 Ausgeschlossene Standorte

[TODO: Listen Sie Standorte auf, die keine CHD verarbeiten]

2.8 8. Netzwerksegmentierung

2.8.1 8.1 Segmentierungsstrategie

Segmentierungsmethode: [TODO: VLAN, Firewall, physische Trennung]

CDE-Segmente: - **CDE-Core:** Systeme mit CHD-Speicherung - **CDE-DMZ:** Systeme mit CHD-Transit (keine Speicherung) - **Management:** Administrative Systeme für CDE

Nicht-CDE-Segmente: - **Corporate:** Büronetzwerk - **Guest:** Gast-WLAN - **Development:** Entwicklungsumgebung

2.8.2 8.2 Segmentierungsvalidierung

Letzte Validierung: [TODO: Datum]
Durchgeführt von: [TODO: Name/Firma]
Methode: [TODO: Penetrationstest, Netzwerk-Scan]
Ergebnis: [TODO: Erfolgreich/Fehlgeschlagen]
Nächste Validierung: [TODO: Datum]

2.9 9. Personal mit CDE-Zugriff

2.9.1 9.1 Rollen mit CHD-Zugriff

Rolle	Anzahl Personen	Zugriffslevel	Begründung
[TODO: Payment Admin]	[TODO: 2]	Voll	Administration
[TODO: Kassierer]	[TODO: 10]	Eingeschränkt	POS-Bedienung
[TODO: Support]	[TODO: 3]	Nur Abfrage	Kundenservice

2.9.2 9.2 Dienstleister mit CDE-Zugriff

Dienstleister	Zweck	Zugriffsmethode	PCI-DSS-Status
[TODO: Payment Processor]	Zahlungsabwicklung	API	AOC vorhanden
[TODO: Hosting Provider]	Server-Hosting	Remote-Admin	AOC vorhanden
[TODO: QSA]	Audit	Vor-Ort	N/A

2.10 10. Scope-Änderungen

2.10.1 10.1 Änderungsmanagement

Prozess für Scope-Änderungen:

1. **Identifikation:** Neue Systeme/Prozesse mit CHD
2. **Bewertung:** PCI-DSS-Relevanz prüfen
3. **Dokumentation:** Scope-Dokument aktualisieren
4. **Genehmigung:** CISO-Freigabe erforderlich
5. **Implementation:** PCI-DSS-Kontrollen anwenden

2.10.2 10.2 Änderungshistorie

Datum	Änderung	Begründung	Genehmigt durch
[TODO: 2026-01-15]	Neues POS-System	Filialerweiterung	[TODO: CISO]
[TODO: 2026-02-01]	Tokenisierung	Scope-Reduktion	[TODO: CISO]

2.11 11. Compliance-Verantwortlichkeiten

2.11.1 11.1 Verantwortliche Personen

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

2.11.2 11.2 RACI-Matrix

Aktivität	PCI Manager	CISO	IT-Leiter	QSA
Scope-Definition	A	C	R	I
Netzwerksegmentierung	C	A	R	I
Compliance-Monitoring	R	A	C	I

Aktivität	PCI Manager	CISO	IT-Leiter	QSA
Jährliches Assessment	C	A	I	R

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

---

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 3

Netzwerksegmentierung

Dokument-ID: PCI-0020
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

3.1 1. Zweck

Dieses Dokument beschreibt die Netzwerksegmentierung zur Isolation des Cardholder Data Environment (CDE) vom restlichen Unternehmensnetzwerk.

3.1.1 1.1 Ziele

- **Scope-Reduktion:** Minimierung der PCI-DSS-relevanten Systeme
- **Risikominimierung:** Begrenzung potenzieller Angriffsflächen
- **Compliance:** Erfüllung von PCI-DSS Requirement 1
- **Sicherheit:** Schutz von Karteninhaberdaten durch Netzwerkisolation

3.2 2. Netzwerkarchitektur

3.2.1 2.1 Netzwerksegmente

CDE-Segmente:

Segment-ID	Segmentname	VLAN-ID	IP-Bereich	Zweck
[TODO: CDE-CORE]	CDE Core	[TODO: 100]	[TODO: 10.1.100.0/24]	CHD-Speicherung

Segment-ID	Segmentname	VLAN-ID	IP-Bereich	Zweck
[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

Nicht-CDE-Segmente:

Segment-ID	Segmentname	VLAN-ID	IP-Bereich	Zweck
[TODO: CORP]	Corporate	[TODO: 10]	[TODO: 10.1.10.0/24]	Büronetzwerk
[TODO: GUEST]	Guest	[TODO: 20]	[TODO: 10.1.20.0/24]	Gast-WLAN
[TODO: DEV]	Development	[TODO: 30]	[TODO: 10.1.30.0/24]	Entwicklung

3.2.2 2.2 Netzwerkdiagramm

[TODO: Fügen Sie Netzwerkdiagramm ein - siehe 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-Konfiguration

3.3.1 3.1 Firewall-Übersicht

Firewall-ID	Typ	Standort	Funktion	Hersteller/Modell
[TODO: FW-PERIMETER]	Perimeter	[TODO: RZ1]	Internet-Grenze	[TODO: Vendor/Model]
[TODO: FW-CDE]	Internal	[TODO: RZ1]	CDE-Segmentierung	[TODO: Vendor/Model]
[TODO: FW-MGMT]	Internal	[TODO: RZ1]	Management-Zugriff	[TODO: Vendor/Model]

3.3.2 3.2 Firewall-Regeln (CDE-Segmentierung)

Grundprinzip: Default Deny (alle Verbindungen standardmäßig blockiert)

3.3.2.1 3.2.1 Eingehende Verbindungen zum CDE

Regel-ID	Quelle	Ziel	Port/Protokoll	Zweck	Genehmigt durch
[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 Ausgehende Verbindungen vom CDE

Regel-ID	Quelle	Ziel	Port/Protokoll	Zweck	Genehmigt durch
[TODO: FW-101]	CDE-CORE	Acquiring Bank	443/TCP	Autorisierung	[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 Blockierte Verbindungen

Explizit blockiert: - CDE → Corporate Network (außer Management) - Corporate → CDE (außer autorisierte Admin-Zugriffe) - CDE → Internet (außer explizit erlaubte Dienste) - Guest → CDE (alle Verbindungen)

3.3.3 3.3 Firewall-Regelüberprüfung

Überprüfungsintervall: Quartalsweise
Verantwortlich: [TODO: Network Security Team]
Letzte Überprüfung: [TODO: Datum]
Nächste Überprüfung: [TODO: Datum]

Überprüfungsprozess: 1. Review aller Firewall-Regeln 2. Identifikation ungenutzter Regeln 3. Validierung der Business-Begründung 4. Dokumentation von Änderungen 5. Genehmigung durch CISO

3.4 4. Router-Konfiguration

3.4.1 4.1 Router-Übersicht

Router-ID	Standort	Funktion	Hersteller/Modell
[TODO: RTR-CORE]	[TODO: RZ1]	Core Routing	[TODO: Vendor/Model]
[TODO: RTR-CDE]	[TODO: RZ1]	CDE Routing	[TODO: Vendor/Model]

3.4.2 4.2 Access Control Lists (ACLs)

[TODO: Dokumentieren Sie Router-ACLs analog zu Firewall-Regeln]

3.5 5. Segmentierungsvalidierung

3.5.1 5.1 Validierungsmethoden

Jährliche Validierung erforderlich (PCI-DSS Req 11.4.6):

1. **Penetrationstests:**
   - Versuch, CDE-Segmentierung zu umgehen
   - Test von Firewall-Regeln
   - Validierung der Netzwerkisolation
2. **Netzwerk-Scans:**
   - Port-Scans von verschiedenen Segmenten
   - Erreichbarkeitstests
   - Routing-Validierung
3. **Konfigurationsüberprüfung:**
   - Review von Firewall-Konfigurationen
   - Überprüfung von Router-ACLs
   - VLAN-Konfigurationsvalidierung

3.5.2 5.2 Validierungshistorie

Datum	Methode	Durchgeführt von	Ergebnis	Maßnahmen
[TODO: 2025-12-01]	Penetrationstest	[TODO: Firma]	Erfolgreich	Keine
[TODO: 2025-06-15]	Netzwerk-Scan	[TODO: Team]	1 Schwachstelle	Regel FW-042 entfernt

3.5.3 5.3 Nächste Validierung

Geplantes Datum: [TODO: Datum]
Methode: [TODO: Penetrationstest/Scan]
Durchführende Firma: [TODO: Name]

3.6 6. Wireless Networks

3.6.1 6.1 Wireless-Segmentierung

Wireless-Netzwerke:

SSID	Segment	Verschlüsselung	CDE-Zugriff	Zweck
[TODO: Corp-WiFi]	Corporate	WPA3-Enterprise	Nein	Mitarbeiter
[TODO: Guest-WiFi]	Guest	WPA3-Personal	Nein	Gäste
[TODO: CDE-WiFi]	CDE-MGMT	WPA3-Enterprise + MFA	Ja	CDE-Admin

Wichtig: Wireless-Netzwerke mit CDE-Zugriff erfordern: - WPA3 oder höher - Multi-Faktor-Authentifizierung - Separate VLAN-Segmentierung - Verschlüsselte Übertragung

3.6.2 6.2 Wireless Access Points

AP-ID	Standort	SSID	Segment	Firmware-Version
[TODO: AP-001]	[TODO: Büro]	Corp-WiFi	Corporate	[TODO: v2.1]
[TODO: AP-002]	[TODO: RZ]	CDE-WiFi	CDE-MGMT	[TODO: v2.1]

3.7 7. Remote Access

3.7.1 7.1 VPN-Konfiguration

VPN-Zugriff zum CDE:

VPN-Typ	Zielgruppe	Authentifizierung	Ziel-Segment	Verschlüsselung
[TODO: SSL-VPN]	Administratoren	MFA (Token)	CDE-MGMT	TLS 1.3
[TODO: IPSec-VPN]	Dienstleister	MFA (Zertifikat)	CDE-MGMT	AES-256

VPN-Anforderungen: - Multi-Faktor-Authentifizierung (MFA) erforderlich - Verschlüsselung: TLS 1.2+ oder IPSec mit AES-256 - Session-Timeout: [TODO: 15 Minuten Inaktivität] - Logging aller VPN-Verbindungen

3.7.2 7.2 Jump Server / Bastion Hosts

Jump Server für CDE-Zugriff:

Server-ID	Standort	Funktion	Zugriffsmethode
[TODO: JUMP-01]	CDE-MGMT	Admin-Zugriff	SSH/RDP über VPN

Jump Server-Anforderungen: - Keine direkte Internet-Verbindung - Zugriff nur über VPN mit MFA - Vollständiges Logging aller Sessions - Keine lokale Datenspeicherung

3.8 8. Monitoring und Alerting

3.8.1 8.1 Netzwerk-Monitoring

Überwachte Metriken: - Firewall-Regel-Verletzungen - Unerwartete Verbindungsversuche zum CDE - Änderungen an Firewall-Konfigurationen - Anomalien im Netzwerkverkehr

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

3.8.2 8.2 Alerting-Regeln

Alert-ID	Bedingung	Schweregrad	Benachrichtigung
[TODO: ALT-001]	Verbindung von Corporate zu CDE-CORE	Kritisch	SOC + CISO
[TODO: ALT-002]	Firewall-Regel-Änderung	Hoch	Network Team
[TODO: ALT-003]	Fehlgeschlagene VPN-Anmeldung (3x)	Mittel	Security Team

3.9 9. Änderungsmanagement

3.9.1 9.1 Änderungsprozess

Prozess für Netzwerkänderungen:

1. **Change Request:** Formale Anfrage mit Begründung
2. **Security Review:** Bewertung der PCI-DSS-Auswirkungen
3. **Testing:** Test in Nicht-Produktionsumgebung
4. **Genehmigung:** CISO-Freigabe für CDE-Änderungen
5. **Implementation:** Durchführung mit Rollback-Plan
6. **Dokumentation:** Aktualisierung dieses Dokuments
7. **Validation:** Überprüfung der Segmentierung

3.9.2 9.2 Änderungshistorie

Datum	Änderung	Begründung	Genehmigt durch	Validiert
[TODO: 2026-01-15]	Neue Firewall-Regel FW-105	Payment API	[TODO: CISO]	Ja

---

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 4

Rollen und Verantwortlichkeiten

Dokument-ID: PCI-0030
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

4.1 1. Zweck

Dieses Dokument definiert die Rollen, Verantwortlichkeiten und Zuständigkeiten für die PCI-DSS-Compliance bei AdminSend GmbH.

4.1.1 1.1 Ziele

- **Klare Verantwortlichkeiten:** Eindeutige Zuweisung von PCI-DSS-Aufgaben
- **Accountability:** Festlegung von Entscheidungsbefugnissen
- **Compliance:** Erfüllung von PCI-DSS Requirement 12.4
- **Kommunikation:** Transparente Kommunikationswege

4.2 2. Organisationsstruktur

4.2.1 2.1 Executive Management

Chief Executive Officer (CEO): - **Name:** {{ meta.roles.ceo.name }} - **E-Mail:** {{ meta.roles.ceo.email }} - **Telefon:** {{ meta.roles.ceo.phone }}

Verantwortlichkeiten: - Gesamtverantwortung für PCI-DSS-Compliance - Genehmigung des PCI-DSS-Budgets - Genehmigung der Informationssicherheitsrichtlinie - Eskalationspunkt für kritische Compliance-Themen

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

Verantwortlichkeiten: - Leitung des PCI-DSS-Compliance-Programms - Genehmigung von Sicherheitsrichtlinien und -standards - Überwachung der Compliance-Aktivitäten - Berichterstattung an Executive Management - Genehmigung von Ausnahmen (Risk Acceptance)

4.2.2 2.2 PCI-DSS Program Management

PCI-DSS Program Manager: - **Name:** [TODO: Name] - **E-Mail:** [TODO: E-Mail] - **Telefon:** [TODO: Telefon]

Verantwortlichkeiten: - Tägliche Leitung des PCI-DSS-Programms - Koordination aller Compliance-Aktivitäten - Vorbereitung von Audits und Assessments - Pflege der PCI-DSS-Dokumentation - Schulungskoordination - Liaison zu QSA und Acquiring Banks

PCI-DSS Compliance Team: - **Mitglieder:** [TODO: Liste der Teammitglieder]

Verantwortlichkeiten: - Unterstützung des Program Managers - Durchführung von Compliance-Checks - Dokumentation von Nachweisen - Koordination mit Fachabteilungen

4.2.3 2.3 IT und Operations

Chief Information Officer (CIO): - **Name:** {{ meta.roles.cio.name }} - **E-Mail:** {{ meta.roles.cio.email }} - **Telefon:** {{ meta.roles.cio.phone }}

Verantwortlichkeiten: - Verantwortung für IT-Infrastruktur und -Systeme - Genehmigung von IT-Änderungen im CDE - Bereitstellung von Ressourcen für PCI-DSS-Compliance - Eskalationspunkt für IT-bezogene Compliance-Themen

IT Security Manager: - **Name:** [TODO: Name] - **E-Mail:** [TODO: E-Mail] - **Telefon:** [TODO: Telefon]

Verantwortlichkeiten: - Implementation von Sicherheitskontrollen - Verwaltung von Firewalls und Netzwerksegmentierung - Patch Management und Vulnerability Management - Incident Response - Log-Monitoring und -Analyse

System Administrators: - **Anzahl:** [TODO: Anzahl] - **Kontakt:** [TODO: Team-E-Mail]

Verantwortlichkeiten: - Administration von CDE-Systemen - Durchführung von Sicherheitsupdates - Backup und Recovery - Einhaltung von Hardening-Standards

Network Administrators: - **Anzahl:** [TODO: Anzahl] - **Kontakt:** [TODO: Team-E-Mail]

Verantwortlichkeiten: - Verwaltung von Netzwerkkomponenten - Firewall-Konfiguration und -Wartung - Netzwerksegmentierung - VPN-Verwaltung

4.2.4 2.4 Application Development

Development Manager: - **Name:** [TODO: Name] - **E-Mail:** [TODO: E-Mail] - **Telefon:** [TODO: Telefon]

Verantwortlichkeiten: - Sichere Softwareentwicklung (Secure SDLC) - Code Reviews und Security Testing - Einhaltung von Secure Coding Standards - Vulnerability Management in Anwendungen

Developers: - **Anzahl:** [TODO: Anzahl] - **Kontakt:** [TODO: Team-E-Mail]

Verantwortlichkeiten: - Entwicklung sicherer Anwendungen - Teilnahme an Security Training - Behebung von Sicherheitslücken - Dokumentation von Anwendungen

4.2.5 2.5 Business Operations

Operations Manager: - **Name:** [TODO: Name] - **E-Mail:** [TODO: E-Mail] - **Telefon:** [TODO: Telefon]

Verantwortlichkeiten: - Geschäftsprozesse mit Karteninhaberdaten - Schulung von Mitarbeitern - Einhaltung von Betriebsverfahren - Incident Reporting

Store/Branch Managers: - **Anzahl:** [TODO: Anzahl] - **Kontakt:** [TODO: Kontaktliste]

Verantwortlichkeiten: - Physische Sicherheit an Standorten - Schulung von Kassierern/POS-Bedienern - Einhaltung von PCI-DSS-Verfahren - Meldung von Sicherheitsvorfällen

4.2.6 2.6 Human Resources

HR Manager: - **Name:** [TODO: Name] - **E-Mail:** [TODO: E-Mail] - **Telefon:** [TODO: Telefon]

Verantwortlichkeiten: - Background Checks für Mitarbeiter mit CDE-Zugriff - Onboarding und Offboarding - Schulungskoordination - Vertraulichkeitsvereinbarungen (NDAs)

4.2.7 2.7 Legal und Compliance

Legal Counsel: - **Name:** [TODO: Name] - **E-Mail:** [TODO: E-Mail] - **Telefon:** [TODO: Telefon]

Verantwortlichkeiten: - Rechtliche Beratung zu PCI-DSS - Vertragsüberprüfung (Dienstleister) - Datenschutz und Compliance - Breach Notification (rechtliche Aspekte)

Data Protection Officer (DPO): - **Name:** [TODO: Name] - **E-Mail:** [TODO: E-Mail] - **Telefon:** [TODO: Telefon]

Verantwortlichkeiten: - Datenschutz-Compliance (DSGVO) - Schnittstelle zwischen PCI-DSS und Datenschutz - Datenschutz-Folgenabschätzungen - Meldung von Datenschutzverletzungen

4.3 3. Externe Rollen

4.3.1 3.1 Qualified Security Assessor (QSA)

Firma: [TODO: QSA-Firma]
Ansprechpartner: [TODO: Name]
E-Mail: [TODO: E-Mail]
Telefon: [TODO: Telefon]
QSA-ID: [TODO: QSA-ID]

Verantwortlichkeiten: - Durchführung des jährlichen PCI-DSS-Assessments - Erstellung des Report on Compliance (ROC) - Beratung zu Compliance-Fragen - Validierung von Sicherheitskontrollen

4.3.2 3.2 Approved Scanning Vendor (ASV)

Firma: [TODO: ASV-Firma]
Ansprechpartner: [TODO: Name]
E-Mail: [TODO: E-Mail]
Telefon: [TODO: Telefon]
ASV-ID: [TODO: ASV-ID]

Verantwortlichkeiten: - Quartalsweise Vulnerability Scans - Erstellung von Scan-Berichten - Validierung von Remediation - Passing Scan Attestation

4.3.3 3.3 Penetration Testing Firm

Firma: [TODO: Pentest-Firma]
Ansprechpartner: [TODO: Name]
E-Mail: [TODO: E-Mail]
Telefon: [TODO: Telefon]

Verantwortlichkeiten: - Jährliche Penetrationstests - Segmentierungsvalidierung - Erstellung von Pentest-Berichten - Retest nach Remediation

4.3.4 3.4 Service Providers

Dienstleister	Kontakt	Rolle	PCI-DSS-Status
[TODO: Payment Processor]	[TODO: Kontakt]	Zahlungsabwicklung	AOC vorhanden
[TODO: Hosting Provider]	[TODO: Kontakt]	Server-Hosting	AOC vorhanden
[TODO: Managed Security]	[TODO: Kontakt]	SIEM/SOC	AOC vorhanden

4.4 4. RACI-Matrizen

4.4.1 4.1 PCI-DSS Requirement 1: Firewall Configuration

Aktivität	CISO	PCI Mgr	IT Sec	Network	QSA
Firewall-Richtlinie erstellen	A	R	C	C	I
Firewall-Regeln konfigurieren	C	I	A	R	I
Quartalsweise Regelüberprüfung	A	R	C	C	I
Änderungen genehmigen	A	C	R	I	I

4.4.2 4.2 PCI-DSS Requirement 3: Protect Stored Data

Aktivität	CISO	PCI Mgr	IT Sec	Dev Mgr	QSA
Verschlüsselungsrichtlinie	A	R	C	C	I
Key Management	C	I	A	R	I

Aktivität	CISO	PCI Mgr	IT Sec	Dev Mgr	QSA
Datenlöschung	C	R	A	C	I
Tokenisierung	C	R	C	A	I

4.4.3 4.3 PCI-DSS Requirement 6: Secure Development

Aktivität	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

Aktivität	CISO	PCI Mgr	IT Sec	HR	QSA
Authentifizierungsrichtlinie	A	R	C	C	I
Benutzerverwaltung	C	I	A	R	I
MFA-Implementation	C	R	A	I	I
Zugriffsentfernung (Offboarding)	C	R	A	R	I

4.4.5 4.5 PCI-DSS Requirement 10: Logging

Aktivität	CISO	PCI Mgr	IT Sec	Ops Mgr	QSA
Logging-Richtlinie	A	R	C	C	I
Log-Konfiguration	C	I	A	R	I
Tägliche Log-Überprüfung	C	R	A	C	I
Log-Retention	A	R	C	I	I

4.4.6 4.6 PCI-DSS Requirement 12: Security Policy

Aktivität	CEO	CISO	PCI Mgr	Legal	QSA
Sicherheitsrichtlinie genehmigen	A	R	C	C	I
Jährliche Risikobewertung	C	A	R	I	I
Schulungsprogramm	C	A	R	C	I
Incident Response Plan	C	A	R	C	I

Legende: - **R** (Responsible): Durchführungsverantwortung - **A** (Accountable): Gesamtverantwortung, Entscheidungsbefugnis (nur eine Person pro Aktivität) - **C** (Consulted): Konsultiert, Fachexpertise - **I** (Informed): Informiert

4.5 5. Eskalationspfade

4.5.1 5.1 Compliance-Eskalation

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

Eskalationskriterien: - Kritische Compliance-Lücken - Fehlgeschlagene Audits - Datenschutzverletzungen - Nicht behebbare Schwachstellen

4.5.2 5.2 Security Incident-Eskalation

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

Eskalationskriterien: - Verdacht auf Datenschutzverletzung - Kompromittierung von CDE-Systemen - Malware-Infektion im CDE - Unautorisierten Zugriff auf Karteninhaberdaten

4.5.3 5.3 Kontaktinformationen für Notfälle

24/7 Security Hotline: [TODO: Telefonnummer]
Security E-Mail: [TODO: security@organization.com]
Incident Response Team: [TODO: Kontaktliste]

4.6 6. Schulung und Awareness

4.6.1 6.1 Schulungsanforderungen

Rolle	Schulungsthemen	Häufigkeit	Verantwortlich
Alle Mitarbeiter	Security Awareness	Jährlich	HR + PCI Mgr
CDE-Administratoren	PCI-DSS Deep Dive	Jährlich	PCI Mgr
Entwickler	Secure Coding	Jährlich	Dev Mgr
Kassierer/POS	PCI-DSS Basics	Bei Einstellung + jährlich	Ops Mgr

4.6.2 6.2 Schulungsdokumentation

Schulungsnachweis erforderlich: - Teilnehmerliste - Schulungsmaterialien - Bestätigungen der Teilnehmer - Testergebnisse (falls zutreffend)

Aufbewahrungsfrist: [TODO: 3 Jahre]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 5

Datenfluss-Diagramme

Dokument-ID: PCI-0040
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

5.1 1. Zweck

Dieses Dokument visualisiert alle Datenflüsse von Karteninhaberdaten (CHD) innerhalb der AdminSend GmbH.

5.1.1 1.1 Ziele

- **Transparenz:** Vollständige Sichtbarkeit aller CHD-Flüsse
- **Scope-Definition:** Identifikation aller PCI-DSS-relevanten Systeme
- **Risikobewertung:** Erkennung potenzieller Schwachstellen
- **Compliance:** Erfüllung von PCI-DSS Requirement 12.5.2

5.2 2. Datenfluss-Übersicht

5.2.1 2.1 Hauptdatenflüsse

[TODO: Fügen Sie High-Level-Datenflussdiagramm ein - siehe diagrams/data_flow_overview.png]

Datenfluss-Phasen: 1. **Erfassung:** Karteneingabe am POS/Webformular 2. **Übertragung:** Transport zur Autorisierung 3. **Verarbeitung:** Autorisierung durch Acquiring Bank 4. **Speicherung:** Persistierung für Reporting (falls erforderlich) 5. **Löschung:** Sichere Entsorgung nach Aufbewahrungsfrist

5.2.2 2.2 Datenfluss-Kategorien

Kategorie	Beschreibung	Systeme	Verschlüsselung
Point of Sale	Karteneingabe in Filialen	POS-Terminals	P2PE
E-Commerce	Online-Zahlungen	Webserver, Payment Gateway	TLS 1.3
Call Center	Telefonische Bestellungen	CRM, IVR	Tokenisierung
Recurring Billing	Wiederkehrende Zahlungen	Billing System	Tokenisierung

5.3 3. Detaillierte Datenflüsse

5.3.1 3.1 Point-of-Sale-Datenfluss

[TODO: Fügen Sie POS-Datenflussdiagramm ein]

Schritte: 1. Kunde präsentiert Karte am POS-Terminal 2. Terminal liest Kartendaten (verschlüsselt) 3. Verschlüsselte Daten an Payment Gateway 4. Gateway sendet an Acquiring Bank 5. Autorisierungsantwort zurück an Terminal 6. Quittung für Kunde

Beteiligte Systeme: - POS-Terminal: [TODO: Modell/Hersteller] - Payment Gateway: [TODO: System-ID] - Acquiring Bank: [TODO: Bank-Name]

Datenschutz: - P2PE (Point-to-Point Encryption) - Keine Speicherung von Full Track Data - Nur letzte 4 Ziffern auf Quittung

5.3.2 3.2 E-Commerce-Datenfluss

[TODO: Fügen Sie E-Commerce-Datenflussdiagramm ein]

Schritte: 1. Kunde gibt Kartendaten im Webformular ein 2. HTTPS-Übertragung an Webserver 3. Weiterleitung an Payment Gateway 4. Gateway tokenisiert PAN 5. Token zurück an Webserver für Speicherung 6. Autorisierung mit Token

Beteiligte Systeme: - Webserver: [TODO: System-ID] - Payment Gateway: [TODO: System-ID] - Datenbank: [TODO: System-ID] (nur Token)

Datenschutz: - TLS 1.3 für Übertragung - Tokenisierung vor Speicherung - Keine Speicherung von CVV2

5.3.3 3.3 Call-Center-Datenfluss

[TODO: Fügen Sie Call-Center-Datenflussdiagramm ein]

Schritte: 1. Kunde nennt Kartendaten am Telefon 2. Agent gibt Daten in CRM ein (maskiert) 3. IVR-System erfasst sensible Daten 4. Direkte Übertragung an Payment Gateway 5. Token zurück an CRM

Beteiligte Systeme: - CRM-System: [TODO: System-ID] - IVR-System: [TODO: System-ID] - Payment Gateway: [TODO: System-ID]

Datenschutz: - IVR für sensible Dateneingabe - Keine Speicherung von PAN im CRM - Nur Token gespeichert

5.4 4. Systemübersicht

5.4.1 4.1 Systeme mit CHD-Zugriff

System-ID	Systemname	CHD-Typ	Funktion	Verschlüsselung
[TODO: SYS-001]	POS-Terminal	PAN (Transit)	Karteneingabe	P2PE
[TODO: SYS-002]	Payment Gateway	PAN	Autorisierung	TLS 1.3
[TODO: SYS-003]	Datenbank	Token	Speicherung	AES-256
[TODO: SYS-004]	Webserver	PAN (Transit)	E-Commerce	TLS 1.3

5.4.2 4.2 Datenübertragungsprotokolle

Verbindung	Protokoll	Verschlüsselung	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. Datenspeicherung

5.5.1 5.1 Gespeicherte Karteninhaberdaten

Datentyp	Speicherort	Verschlüsselung	Aufbewahrungsfrist	Begründung
PAN (Token)	Datenbank	AES-256	[TODO: 13 Monate]	Rückerstattungen
Karteninhaber-Name	Datenbank	AES-256	[TODO: 13 Monate]	Rückerstattungen
Transaktionsdaten	Datenbank	AES-256	[TODO: 7 Jahre]	Buchhaltung

Nicht gespeichert: - Full Track Data - CVV2/CVC2/CID - PIN/PIN Block

5.5.2 5.2 Datenlöschung

Löschprozess: 1. Automatische Identifikation abgelaufener Daten 2. Sichere Löschung (Overwrite/Crypto-Shredding) 3. Logging der Löschvorgänge 4. Quartalsweise Überprüfung

Verantwortlich: [TODO: Data Retention Manager]

5.6 6. Externe Datenflüsse

5.6.1 6.1 Acquiring Bank

Bank: [TODO: Bank-Name]
Verbindung: HTTPS/TLS 1.3
Datentyp: PAN, Transaktionsdaten
Zweck: Autorisierung und Settlement

5.6.2 6.2 Payment Processor

Processor: [TODO: Processor-Name]
Verbindung: HTTPS/TLS 1.3
Datentyp: PAN (verschlüsselt)
Zweck: Zahlungsabwicklung

5.6.3 6.3 Tokenization Service

Service: [TODO: Service-Name]
Verbindung: HTTPS/TLS 1.3
Datentyp: PAN → Token
Zweck: Scope-Reduktion

5.7 7. Datenfluss-Änderungsmanagement

5.7.1 7.1 Änderungsprozess

Bei Änderungen an Datenflüssen: 1. Aktualisierung der Diagramme 2. PCI-DSS-Impact-Assessment 3. Genehmigung durch CISO 4. Dokumentation der Änderung 5. Schulung betroffener Mitarbeiter

5.7.2 7.2 Änderungshistorie

Datum	Änderung	Begründung	Genehmigt durch
[TODO: 2026-01-15]	Tokenisierung implementiert	Scope-Reduktion	[TODO: CISO]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 6

Compliance-Programm

Dokument-ID: PCI-0050
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

6.1 1. Zweck

Dieses Dokument beschreibt das PCI-DSS-Compliance-Programm der AdminSend GmbH.

6.1.1 1.1 Ziele

- **Kontinuierliche Compliance:** Aufrechterhaltung der PCI-DSS-Compliance
- **Governance:** Strukturierte Überwachung und Steuerung
- **Risikomanagement:** Proaktive Identifikation und Behandlung von Risiken
- **Audit-Readiness:** Vorbereitung auf Assessments und Audits

6.2 2. Compliance-Governance

6.2.1 2.1 Governance-Struktur

PCI-DSS Steering Committee: - **Vorsitz:** {{ meta.roles.ciso.name }} - **Mitglieder:** CEO, CIO, PCI Program Manager, Legal, Operations Manager - **Frequenz:** Quartalsweise - **Zweck:** Strategische Entscheidungen, Budget, Risikobewertung

PCI-DSS Working Group: - **Leitung:** PCI Program Manager - **Mitglieder:** IT Security, Network, Development, Operations - **Frequenz:** Monatlich - **Zweck:** Operative Umsetzung, Problemlösung, Koordination

6.2.2 2.2 Management-Commitment

Informationssicherheitsrichtlinie: - Genehmigt durch: {{ meta.roles.ceo.name }} - Datum: [TODO: Datum] - Jährliche Überprüfung: [TODO: Monat]

PCI-DSS-Verpflichtung: AdminSend GmbH verpflichtet sich zur Einhaltung aller PCI-DSS-Anforderungen zum Schutz von Karteninhaberdaten.

6.3 3. Compliance-Aktivitäten

6.3.1 3.1 Jährliche Aktivitäten

Aktivität	Verantwortlich	Zeitraum	Status
PCI-DSS Assessment (QSA)	PCI Program Manager	[TODO: Q1]	[TODO]
Penetrationstest	IT Security	[TODO: Q2]	[TODO]
Risikobewertung	CISO	[TODO: Q3]	[TODO]
Richtlinienüberprüfung	CISO	[TODO: Q4]	[TODO]
Security Awareness Training	HR + PCI Mgr	[TODO: Laufend]	[TODO]

6.3.2 3.2 Quartalsweise Aktivitäten

Aktivität	Verantwortlich	Frequenz	Letzte Durchführung
ASV Vulnerability Scans	ASV	Quartalsweise	[TODO: Datum]
Firewall-Regelüberprüfung	Network Team	Quartalsweise	[TODO: Datum]
Steering Committee Meeting	CISO	Quartalsweise	[TODO: Datum]
Compliance-Reporting	PCI Program Manager	Quartalsweise	[TODO: Datum]

6.3.3 3.3 Monatliche Aktivitäten

Aktivität	Verantwortlich	Frequenz	Letzte Durchführung
Working Group Meeting	PCI Program Manager	Monatlich	[TODO: Datum]
Compliance-Dashboard-Review	CISO	Monatlich	[TODO: Datum]
Patch-Status-Review	IT Security	Monatlich	[TODO: Datum]

6.3.4 3.4 Tägliche Aktivitäten

Aktivität	Verantwortlich	Frequenz
Log-Überprüfung	IT Security	Täglich
Incident Monitoring	SOC	24/7
Backup-Überprüfung	System Admin	Täglich

6.4 4. Compliance-Metriken und KPIs

6.4.1 4.1 Key Performance Indicators

KPI	Zielwert	Messung	Verantwortlich
Vulnerability Remediation Time	< 30 Tage (High/Critical)	Monatlich	IT Security
Patch Compliance Rate	> 95%	Monatlich	System Admin
Security Training Completion	100%	Jährlich	HR
Failed Login Attempts	< 100/Tag	Täglich	IT Security
Firewall Rule Changes	Alle genehmigt	Monatlich	Network Team

6.4.2 4.2 Compliance-Dashboard

Überwachte Metriken: - Anzahl offener Schwachstellen (nach Schweregrad) - Patch-Status aller CDE-Systeme - Anzahl Sicherheitsvorfälle - Schulungsstatus der Mitarbeiter - Status quartalsweiser ASV-Scans - Firewall-Regel-Compliance

Dashboard-Zugriff: [TODO: URL/System]
Aktualisierung: Täglich automatisch

6.5 5. Audit und Assessment

6.5.1 5.1 Jährliches PCI-DSS Assessment

Assessment-Typ: [TODO: SAQ oder ROC]
QSA: [TODO: Firma/Name]
Letztes Assessment: [TODO: Datum]
Nächstes Assessment: [TODO: Datum]
Ergebnis: [TODO: Compliant/Non-Compliant]

Assessment-Vorbereitung: 1. Dokumentensammlung (3 Monate vor Assessment) 2. Pre-Assessment-Audit (2 Monate vor Assessment) 3. Remediation offener Punkte (1 Monat vor Assessment) 4. QSA-Assessment (geplanter Termin) 5. Nachbereitung und AOC-Erhalt

6.5.2 5.2 Attestation of Compliance (AOC)

Letzte AOC: [TODO: Datum]
Gültig bis: [TODO: Datum]
Eingereicht bei: [TODO: Acquiring Banks]

AOC-Verteilung: - Acquiring Banks - Payment Brands (falls erforderlich) - Geschäftspartner (auf Anfrage)

6.5.3 5.3 Interne Audits

Frequenz: Halbjährlich
Verantwortlich: Internal Audit Team
Scope: Stichproben aller 12 PCI-DSS-Anforderungen

Letztes Audit: [TODO: Datum]
Nächstes Audit: [TODO: Datum]

6.6 6. Risikomanagement

6.6.1 6.1 Jährliche Risikobewertung

Methodik: [TODO: z.B. ISO 27005, NIST 800-30]
Letzte Bewertung: [TODO: Datum]
Nächste Bewertung: [TODO: Datum]

Identifizierte Risiken:

Risiko-ID	Beschreibung	Wahrscheinlichkeit	Auswirkung	Maßnahmen
[TODO: R-001]	Datenschutzverletzung	Mittel	Hoch	Verschlüsselung, Monitoring
[TODO: R-002]	Insider-Bedrohung	Niedrig	Hoch	Zugriffskontrolle, Logging

6.6.2 6.2 Risikominderung

Risikominderungsstrategien: - Technische Kontrollen (Verschlüsselung, Firewalls, IDS/IPS) - Organisatorische Kontrollen (Richtlinien, Schulungen) - Physische Kontrollen (Zutrittskontrolle, Videoüberwachung) - Versicherung (Cyber-Versicherung)

6.7 7. Incident Response

6.7.1 7.1 Incident-Response-Plan

Dokumentiert in: PCI-0630 Incident Response

Incident-Kategorien: - Datenschutzverletzung (Breach) - Malware-Infektion - Unautorisierten Zugriff - Denial of Service - Physischer Sicherheitsvorfall

6.7.2 7.2 Breach Notification

Meldepflichten: - Acquiring Banks: Unverzüglich - Payment Brands: Gemäß Brand-Anforderungen - Betroffene Karteninhaber: Gemäß lokaler Gesetzgebung - Aufsichtsbehörden: Gemäß DSGVO (72 Stunden)

Verantwortlich: Legal Counsel + CISO

6.8 8. Schulung und Awareness

6.8.1 8.1 Schulungsprogramm

Zielgruppen:

Zielgruppe	Schulungsinhalt	Frequenz	Dauer
Alle Mitarbeiter	Security Awareness	Jährlich	1 Stunde
CDE-Administratoren	PCI-DSS Deep Dive	Jährlich	4 Stunden
Entwickler	Secure Coding	Jährlich	8 Stunden
Kassierer/POS	PCI-DSS Basics	Bei Einstellung	2 Stunden

6.8.2 8.2 Schulungsmaterialien

Verfügbare Materialien: - E-Learning-Module - Präsentationen - Checklisten - Poster und Infografiken - Phishing-Simulationen

Speicherort: [TODO: Intranet/LMS-URL]

6.9 9. Dokumentenmanagement

6.9.1 9.1 PCI-DSS-Dokumentation

Dokumentenregister:

Dokument-ID	Titel	Version	Letzte Aktualisierung	Owner
PCI-0010	Scope und CDE	1.0	[TODO]	PCI Mgr
PCI-0020	Netzwerksegmentierung	1.0	[TODO]	Network
PCI-0030	Rollen	1.0	[TODO]	PCI Mgr

Dokumentenaufbewahrung: Mindestens 3 Jahre
Zugriffskontrolle: Nur autorisierte Personen

6.9.2 9.2 Nachweisführung (Evidence)

Erforderliche Nachweise: - Firewall-Konfigurationen - Scan-Berichte (ASV) - Penetrationstest-Berichte - Schulungsnachweise - Log-Reviews - Änderungsprotokolle

Speicherort: [TODO: Dokumentenmanagementsystem]

6.10 10. Kontinuierliche Verbesserung

6.10.1 10.1 Verbesserungsprozess

Quellen für Verbesserungen: - Audit-Findings - Incident-Lessons-Learned - Vulnerability-Scan-Ergebnisse - Mitarbeiter-Feedback - Branchentrends

6.10.2 10.2 Verbesserungsmaßnahmen

Maßnahme	Priorität	Verantwortlich	Zieldatum	Status
[TODO: Tokenisierung]	Hoch	IT Security	[TODO]	In Arbeit
[TODO: SIEM-Upgrade]	Mittel	IT Security	[TODO]	Geplant

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 7

Firewall-Konfiguration

Dokument-ID: PCI-0100
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

7.1 1. Zweck

Dieses Dokument definiert die Firewall-Konfigurationsstandards für AdminSend GmbH gemäß PCI-DSS Requirement 1.

7.1.1 1.1 Ziele

- **Netzwerksicherheit:** Schutz des CDE durch Firewall-Kontrollen
- **Zugriffskontrolle:** Restriktion unautorisierten Netzwerkzugriffs
- **Compliance:** Erfüllung von PCI-DSS Requirement 1
- **Dokumentation:** Nachvollziehbare Firewall-Konfiguration

7.1.2 1.2 Geltungsbereich

Betroffene Systeme: - Perimeter-Firewalls (Internet-Grenze) - Interne Firewalls (CDE-Segmentierung) - Host-basierte Firewalls (Server, Workstations) - Cloud-Firewalls (falls zutreffend)

7.2 2. Firewall-Standards

7.2.1 2.1 Grundprinzipien

Default Deny: - Alle Verbindungen standardmäßig blockiert - Nur explizit genehmigte Verbindungen erlaubt - Dokumentation aller Ausnahmen erforderlich

Least Privilege: - Minimale erforderliche Zugriffsrechte - Spezifische Quell- und Ziel-IP-Adressen - Spezifische Ports und Protokolle

Defense in Depth: - Mehrere Firewall-Ebenen - Perimeter + interne Segmentierung - Host-basierte Firewalls als zusätzliche Schicht

7.2.2 2.2 Firewall-Architektur

Firewall-Ebenen:

1. **Perimeter Firewall:**
   - Schutz vor Internet-Bedrohungen
   - Eingehender und ausgehender Traffic
   - DMZ für öffentliche Dienste
2. **Internal Firewall:**
   - CDE-Segmentierung
   - Trennung von Corporate und CDE
   - Zugriffskontrolle zwischen Segmenten
3. **Host-based Firewall:**
   - Schutz einzelner Systeme
   - Zusätzliche Verteidigungsebene
   - Schutz bei Netzwerk-Kompromittierung

7.3 3. Firewall-Regelmanagement

7.3.1 3.1 Regel-Anforderungen

Jede Firewall-Regel muss enthalten: - Eindeutige Regel-ID - Quelle (IP-Adresse/Netzwerk) - Ziel (IP-Adresse/Netzwerk) - Port/Protokoll - Aktion (Allow/Deny) - Business-Begründung - Genehmiger - Erstellungsdatum - Überprüfungsdatum

7.3.2 3.2 Regel-Genehmigungsprozess

Prozess für neue Regeln:

1. **Anfrage:** Change Request mit Begründung
2. **Security Review:** Bewertung durch IT Security
3. **Genehmigung:** CISO-Freigabe für CDE-Regeln
4. **Implementation:** Konfiguration durch Network Team
5. **Dokumentation:** Aktualisierung des Regelwerks
6. **Validation:** Test der Regel

Genehmigungsmatrix:

Regel-Typ	Genehmiger	Dokumentation
CDE-bezogen	CISO	Vollständig
Corporate	IT Manager	Standard
Temporär	IT Security	Mit Ablaufdatum

7.3.3 3.3 Quartalsweise Regelüberprüfung

Überprüfungsprozess:

1. **Review aller Regeln:** Vollständige Durchsicht
2. **Validierung:** Business-Begründung noch gültig?
3. **Cleanup:** Entfernung ungenutzter Regeln
4. **Dokumentation:** Aktualisierung der Dokumentation
5. **Genehmigung:** CISO-Bestätigung

Letzte Überprüfung: [TODO: Datum]
Nächste Überprüfung: [TODO: Datum]
Verantwortlich: [TODO: Network Security Team]

7.4 4. Firewall-Konfigurationsstandards

7.4.1 4.1 Perimeter-Firewall

Eingehender Traffic (Inbound):

Service	Port	Protokoll	Quelle	Ziel	Erlaubt
HTTPS	443	TCP	Any	Web Server (DMZ)	Ja
SSH	22	TCP	Admin IPs	Jump Server	Ja (mit MFA)
Alle anderen	*	*	Any	CDE	Nein

Ausgehender Traffic (Outbound):

Service	Port	Protokoll	Quelle	Ziel	Erlaubt
HTTPS	443	TCP	CDE	Acquiring Bank	Ja
DNS	53	UDP	CDE	DNS Server	Ja
NTP	123	UDP	CDE	NTP Server	Ja
Alle anderen	*	*	CDE	Internet	Nein (Default Deny)

7.4.2 4.2 Interne Firewall (CDE-Segmentierung)

CDE → Corporate: - Standardmäßig blockiert - Ausnahmen nur mit CISO-Genehmigung - Logging aller Verbindungsversuche

Corporate → CDE: - Nur autorisierte Admin-Zugriffe - MFA erforderlich - Über Jump Server/VPN - Vollständiges Logging

7.4.3 4.3 Host-basierte Firewalls

Anforderungen: - Aktiviert auf allen CDE-Systemen - Konfiguration gemäß Hardening-Standards - Zentrale Verwaltung (falls möglich) - Logging aktiviert

Beispiel-Konfiguration (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. Verbotene Konfigurationen

Folgende Konfigurationen sind NICHT erlaubt:

- **Any-Any-Regeln:** Keine Regeln mit Quelle=Any und Ziel=Any
- **Direkte Internet-Verbindungen:** CDE-Systeme dürfen nicht direkt mit Internet kommunizieren
- **Unverschlüsselte Protokolle:** Telnet, FTP, HTTP (außer Redirect zu HTTPS)
- **Veraltete Protokolle:** SSLv2, SSLv3, TLS 1.0, TLS 1.1
- **Undokumentierte Regeln:** Alle Regeln müssen dokumentiert sein

7.6 6. Änderungsmanagement

7.6.1 6.1 Emergency Changes

Notfall-Änderungen erlaubt bei: - Aktiven Sicherheitsvorfällen - Kritischen Systemausfällen - Unmittelbarer Bedrohung

Prozess: 1. Mündliche Genehmigung durch CISO 2. Sofortige Implementation 3. Nachträgliche Dokumentation (innerhalb 24h) 4. Formale Genehmigung (innerhalb 48h)

7.6.2 6.2 Änderungshistorie

Datum	Regel-ID	Änderung	Begründung	Genehmigt durch
[TODO: 2026-01-15]	FW-105	Neue Regel	Payment API	[TODO: CISO]
[TODO: 2026-02-01]	FW-042	Entfernt	Nicht mehr benötigt	[TODO: CISO]

7.7 7. Monitoring und Alerting

7.7.1 7.1 Firewall-Logging

Logging-Anforderungen: - Alle blockierten Verbindungen - Alle erlaubten Verbindungen zum/vom CDE - Firewall-Konfigurationsänderungen - Firewall-Systemereignisse (Start, Stop, Fehler)

Log-Retention: [TODO: 90 Tage online, 1 Jahr Archiv]
Log-Forwarding: [TODO: SIEM-System]

7.7.2 7.2 Alerting-Regeln

Alert	Bedingung	Schweregrad	Benachrichtigung
Unerlaubter CDE-Zugriff	Blockierte Verbindung zu CDE	Hoch	SOC + IT Security
Firewall-Regel-Änderung	Konfigurationsänderung	Mittel	Network Team
Firewall-Ausfall	Firewall nicht erreichbar	Kritisch	SOC + CISO

7.8 8. Compliance-Validierung

7.8.1 8.1 Validierungsaktivitäten

Quartalsweise: - Firewall-Regelüberprüfung - Dokumentationsvalidierung - Ungenutzter Regel-Cleanup

Jährlich: - Penetrationstest der Firewall-Konfiguration - Segmentierungsvalidierung - Compliance-Audit

7.8.2 8.2 Validierungsdokumentation

Erforderliche Nachweise: - Firewall-Konfigurationsdateien - Regelüberprüfungsprotokolle - Änderungsprotokolle - Genehmigungsnachweise

---

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated | default("") }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 8

Zugriffskontrolle

Dokument-ID: PCI-0400
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

8.1 1. Zweck

Dieses Dokument definiert die Zugriffskontrollrichtlinien für AdminSend GmbH gemäß PCI-DSS Requirement 7.

8.1.1 1.1 Ziele

- **Need-to-Know-Prinzip:** Zugriff nur für berechtigte Personen
- **Least Privilege:** Minimale erforderliche Zugriffsrechte
- **Rollenbasierte Zugriffskontrolle:** RBAC-Implementierung
- **Compliance:** Erfüllung von PCI-DSS Requirement 7

8.1.2 1.2 Geltungsbereich

Betroffene Systeme: - Alle CDE-Systeme - Systeme mit Karteninhaberdaten - Administrative Systeme - Datenbanken mit CHD

8.2 2. Zugriffskontrollprinzipien

8.2.1 2.1 Need-to-Know

Grundsatz: - Zugriff nur für Personen mit geschäftlicher Notwendigkeit - Dokumentierte Begründung erforderlich - Regelmäßige Überprüfung der Zugriffsrechte

8.2.2 2.2 Least Privilege

Grundsatz: - Minimale erforderliche Berechtigungen - Keine unnötigen Administratorrechte - Zeitlich begrenzte privilegierte Zugriffe

8.2.3 2.3 Separation of Duties

Grundsatz: - Trennung kritischer Funktionen - Keine Einzelperson mit vollständiger Kontrolle - Vier-Augen-Prinzip für kritische Operationen

8.3 3. Rollenbasierte Zugriffskontrolle (RBAC)

8.3.1 3.1 Definierte Rollen

Rolle	Beschreibung	CDE-Zugriff	CHD-Zugriff
Payment Administrator	Vollständige Payment-System-Administration	Ja	Ja (vollständig)
System Administrator	Server- und Netzwerkadministration	Ja	Nein
Database Administrator	Datenbankverwaltung	Ja	Ja (verschlüsselt)
Application Administrator	Anwendungsverwaltung	Ja	Nein
Security Administrator	Sicherheitssystem-Administration	Ja	Nein
Kassierer	POS-Bedienung	Eingeschränkt	Ja (nur Eingabe)
Support Mitarbeiter	Kundenservice	Eingeschränkt	Ja (nur Abfrage, maskiert)
Entwickler	Softwareentwicklung	Nein	Nein
Auditor	Compliance-Prüfung	Lesezugriff	Ja (nur Logs)

8.3.2 3.2 Berechtigungsmatrix

System/Ressource	Payment Admin	Sys Admin	DB Admin	App Admin	Kassierer	Support
Payment Gateway	RWX	RW	R	RW	-	R
CDE-Datenbank	RWX	R	RWX	R	-	R (maskiert)
POS-Terminal	RW	RW	-	RW	RW	R
Firewall	RW	RWX	-	-	-	-
SIEM	RW	RW	-	-	-	R
Backup-System	RW	RWX	RW	-	-	-

Legende: R = Read, W = Write, X = Execute, - = Kein Zugriff

8.4 4. Zugriffsverwaltungsprozess

8.4.1 4.1 Zugriffsanforderung

Prozess:

1. **Antrag:** Formular mit Begründung
2. **Manager-Genehmigung:** Vorgesetzter genehmigt
3. **Security Review:** IT Security prüft
4. **CISO-Genehmigung:** Bei CDE-Zugriff erforderlich
5. **Provisionierung:** IT implementiert Zugriff
6. **Dokumentation:** Zugriff wird dokumentiert
7. **Benachrichtigung:** Benutzer wird informiert

Genehmigungsmatrix:

Zugriffs-Typ	Genehmiger	Dokumentation
CDE-Zugriff	CISO	Vollständig
CHD-Zugriff	CISO + Manager	Vollständig
Corporate-Zugriff	Manager	Standard
Temporärer Zugriff	IT Security	Mit Ablaufdatum

8.4.2 4.2 Zugriffsänderung

Prozess bei Rollenänderung:

1. **Identifikation:** Rollenänderung erkannt
2. **Bewertung:** Neue Zugriffsanforderungen
3. **Genehmigung:** Wie bei Neuantrag
4. **Entzug:** Alte Berechtigungen entfernen
5. **Provisionierung:** Neue Berechtigungen erteilen
6. **Validierung:** Zugriff testen

8.4.3 4.3 Zugriffsentzug

Prozess bei Ausscheiden:

1. **Benachrichtigung:** HR informiert IT
2. **Sofortiger Entzug:** Alle Zugänge deaktivieren
3. **Rückgabe:** Hardware und Zugangsmittel
4. **Dokumentation:** Entzug dokumentieren
5. **Validierung:** Zugriff testen (sollte blockiert sein)

Zeitrahmen: - Bei Kündigung: Sofort am letzten Arbeitstag - Bei Versetzung: Innerhalb 24 Stunden - Bei Verdacht: Sofort

8.5 5. Privilegierte Zugriffe

8.5.1 5.1 Administrative Accounts

Anforderungen: - Separate Admin-Accounts (nicht für tägliche Arbeit) - Starke Authentifizierung (MFA erforderlich) - Vollständiges Logging aller Aktionen - Regelmäßige Überprüfung

Namenskonvention: - Standard-User: `vorname.nachname` - Admin-User: `vorname.nachname-admin` - Service-Account: `svc-servicename`

8.5.2 5.2 Privileged Access Management (PAM)

PAM-System: [TODO: Name des PAM-Systems]

Funktionen: - Just-in-Time (JIT) Zugriff - Session-Recording - Passwort-Vaulting - Automatische Passwortrotation

Prozess: 1. Admin beantragt privilegierten Zugriff 2. Genehmigung durch CISO (automatisch oder manuell) 3. Zeitlich begrenzter Zugriff gewährt 4. Session wird aufgezeichnet 5. Automatischer Entzug nach Ablauf

8.5.3 5.3 Emergency Access

Break-Glass-Accounts: - Nur für Notfälle - Passwort in versiegeltem Umschlag - Verwendung muss dokumentiert werden - Passwort nach Verwendung ändern

Prozess: 1. Notfall identifiziert 2. Umschlag öffnen (mit Zeugen) 3. Zugriff verwenden 4. Incident dokumentieren 5. Passwort sofort ändern 6. CISO informieren

8.6 6. Zugriffskontrolle für Karteninhaberdaten

8.6.1 6.1 CHD-Zugriffsbeschränkungen

Vollständiger PAN-Zugriff: - Nur für autorisierte Rollen - Dokumentierte Business-Begründung - CISO-Genehmigung erforderlich - Vollständiges Logging

Maskierter PAN-Zugriff: - Nur letzte 4 Ziffern sichtbar - Für Support und Reporting - Standard-Genehmigung ausreichend

Kein PAN-Zugriff: - Alle anderen Benutzer - Entwickler (nur Testdaten) - Externe Dienstleister (ohne Notwendigkeit)

8.6.2 6.2 Datenmaskierung

Maskierungsregeln: - PAN: Nur erste 6 und letzte 4 Ziffern (z.B., 123456******1234) - Ablaufdatum: Vollständig maskiert - CVV: Niemals anzeigen (darf nicht gespeichert werden) - Karteninhaber-Name: Teilweise maskiert (z.B., Max M******)

Ausnahmen: - Payment-Administratoren (vollständiger Zugriff) - Nur mit CISO-Genehmigung - Vollständiges Logging

8.7 7. Zugriffskontrolle für Anwendungen

8.7.1 7.1 Anwendungsberechtigungen

Berechtigungsmodell: - Rollenbasierte Berechtigungen - Granulare Funktionsrechte - Keine Shared Accounts - Eindeutige Benutzer-IDs

Beispiel (Payment Application):

Funktion	Payment Admin	Kassierer	Support
Transaktion durchführen	Ja	Ja	Nein
Transaktion stornieren	Ja	Eingeschränkt	Nein
Berichte anzeigen	Ja	Nein	Ja (maskiert)
Konfiguration ändern	Ja	Nein	Nein
Benutzer verwalten	Ja	Nein	Nein

8.7.2 7.2 API-Zugriffskontrolle

API-Authentifizierung: - API-Keys mit Ablaufdatum - OAuth 2.0 für externe APIs - Mutual TLS für kritische APIs - Rate Limiting

API-Autorisierung: - Scope-basierte Berechtigungen - Minimale erforderliche Scopes - Logging aller API-Aufrufe

8.8 8. Zugriffskontrolle für Datenbanken

8.8.1 8.1 Datenbank-Berechtigungen

Berechtigungsmodell: - Separate DB-Accounts pro Anwendung - Keine Shared Accounts - Least Privilege für Anwendungen - DBA-Zugriff nur für Administration

Beispiel:

Account	Typ	Berechtigungen	Zweck
app_payment	Application	SELECT, INSERT, UPDATE	Payment-Anwendung
app_reporting	Application	SELECT	Reporting
dba_admin	DBA	ALL	Administration
backup_user	Service	SELECT	Backup

8.8.2 8.2 Verschlüsselte Spalten

CHD-Spalten: - PAN: Verschlüsselt (AES-256) - Zugriff nur über Entschlüsselungsfunktion - Logging aller Entschlüsselungen - Nur autorisierte Accounts

8.9 9. Zugriffskontrolle für Netzwerk

8.9.1 9.1 Netzwerkzugriff

Zugriffsmethoden: - VPN für Remote-Zugriff - Jump Server für Admin-Zugriff - Keine direkte Internet-Verbindung zu CDE

Authentifizierung: - Multi-Faktor-Authentifizierung (MFA) - Zertifikatsbasierte Authentifizierung - Starke Passwörter

8.9.2 9.2 Netzwerksegmentierung

Zugriffskontrolle zwischen Segmenten: - Firewall-Regeln - ACLs auf Switches - Micro-Segmentierung

8.10 10. Zugriffskontrolle für physischen Zugang

8.10.1 10.1 Rechenzentrum

Zugriffskontrolle: - Badge-System - Biometrische Authentifizierung - Begleitpflicht für Besucher - Logging aller Zutritte

Autorisierte Personen: - Datacenter-Personal - Autorisierte Administratoren - Wartungspersonal (mit Begleitung)

8.10.2 10.2 Büroräume mit CDE-Zugriff

Zugriffskontrolle: - Gesperrte Räume - Badge-Zugang - Besucherprotokoll

8.11 11. Zugriffskontrolle für Dienstleister

8.11.1 11.1 Dienstleister-Zugriff

Anforderungen: - Separate Accounts für jeden Dienstleister - Zeitlich begrenzter Zugriff - Vollständiges Logging - PCI-DSS AOC erforderlich

Genehmigungsprozess: 1. Dienstleister-Vertrag mit PCI-Klauseln 2. AOC-Validierung 3. CISO-Genehmigung 4. Zeitlich begrenzter Zugriff 5. Überwachung während Zugriff

8.11.2 11.2 Remote-Support

Prozess: - Nur nach Genehmigung - Session-Recording - Begleitung durch internen Admin - Sofortiger Entzug nach Abschluss

8.12 12. Zugriffskontrolle-Überwachung

8.12.1 12.1 Logging

Geloggte Ereignisse: - Erfolgreiche Anmeldungen - Fehlgeschlagene Anmeldungen - Privilegierte Aktionen - Zugriff auf CHD - Berechtigungsänderungen

Log-Retention: [TODO: 90 Tage online, 1 Jahr Archiv]

8.12.2 12.2 Alerting

Alert	Bedingung	Schweregrad	Benachrichtigung
Mehrfache fehlgeschlagene Logins	>5 in 15 Min	Mittel	SOC
Admin-Login außerhalb Geschäftszeiten	Nach 22:00 Uhr	Mittel	SOC + Manager
CHD-Zugriff	Jeder Zugriff	Niedrig	SIEM
Berechtigungsänderung	Jede Änderung	Mittel	IT Security

8.13 13. Zugriffskontrolle-Reviews

8.13.1 13.1 Quartalsweise Überprüfung

Überprüfungsprozess:

1. **Benutzer-Review:** Alle Benutzer mit CDE-Zugriff
2. **Berechtigungs-Review:** Alle Berechtigungen validieren
3. **Inaktive Accounts:** Identifizieren und deaktivieren
4. **Dokumentation:** Ergebnisse dokumentieren
5. **Genehmigung:** CISO-Bestätigung

Letzte Überprüfung: [TODO: Datum]
Nächste Überprüfung: [TODO: Datum]
Verantwortlich: [TODO: IT Security Team]

8.13.2 13.2 Rezertifizierung

Jährliche Rezertifizierung: - Alle Benutzer mit CDE-Zugriff - Manager bestätigt Business-Notwendigkeit - IT Security validiert Berechtigungen - CISO genehmigt

8.14 14. Compliance-Validierung

8.14.1 14.1 Validierungsaktivitäten

Quartalsweise: - Zugriffskontrolle-Review - Inaktive Account-Cleanup - Berechtigungsdokumentation

Jährlich: - Vollständige Rezertifizierung - Penetrationstest - Compliance-Audit

8.14.2 14.2 Validierungsdokumentation

Erforderliche Nachweise: - Zugriffskontrollrichtlinien - Berechtigungsmatrix - Genehmigungsnachweise - Review-Protokolle - Rezertifizierungsnachweise

---

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 9

Benutzerauthentifizierung

Dokument-ID: PCI-0410
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

9.1 1. Zweck

Dieses Dokument definiert die Authentifizierungsrichtlinien für AdminSend GmbH gemäß PCI-DSS Requirement 8.

9.1.1 1.1 Ziele

- **Eindeutige Identifikation:** Jeder Benutzer eindeutig identifizierbar
- **Starke Authentifizierung:** Multi-Faktor-Authentifizierung (MFA)
- **Sichere Passwörter:** Passwortrichtlinien durchsetzen
- **Compliance:** Erfüllung von PCI-DSS Requirement 8

9.1.2 1.2 Geltungsbereich

Betroffene Systeme: - Alle CDE-Systeme - Administrative Systeme - Anwendungen mit CHD-Zugriff - Remote-Zugriffssysteme

9.2 2. Benutzeridentifikation

9.2.1 2.1 Eindeutige Benutzer-IDs

Anforderungen: - Jeder Benutzer hat eindeutige ID - Keine Shared Accounts - Keine Generic Accounts (außer dokumentierte Ausnahmen) - Benutzer-ID darf nicht wiederverwendet werden

Namenskonvention: - Format: `vorname.nachname` - Bei Duplikaten: `vorname.nachname2` - Service-Accounts: `svc-servicename` - Admin-Accounts: `vorname.nachname-admin`

9.2.2 2.2 Verbotene Account-Typen

Nicht erlaubt: - Shared Accounts (mehrere Personen, ein Account) - Generic Accounts (z.B., "admin", "user", "test") - Group Accounts - Vendor Default Accounts (müssen deaktiviert werden)

Ausnahmen: - Notfall-Accounts (Break-Glass) - dokumentiert - Service-Accounts - dokumentiert und überwacht - Konsolen-Zugriff (nur mit Logging)

9.3 3. Authentifizierungsmethoden

9.3.1 3.1 Multi-Faktor-Authentifizierung (MFA)

MFA erforderlich für: - Alle CDE-Zugriffe - Administrative Zugriffe - Remote-Zugriffe (VPN, Jump Server) - Privilegierte Accounts - Zugriff auf CHD

MFA-Faktoren:

1. **Etwas, das Sie wissen:**
   - Passwort
   - PIN
2. **Etwas, das Sie haben:**
   - Hardware-Token
   - Software-Token (Authenticator App)
   - Smart Card
   - SMS (nur als Backup)
3. **Etwas, das Sie sind:**
   - Biometrie (Fingerabdruck, Gesichtserkennung)

MFA-Implementierung: - Mindestens 2 verschiedene Faktoren - Faktoren müssen unabhängig sein - MFA-System: [TODO: Name des MFA-Systems]

9.3.2 3.2 Passwort-Authentifizierung

Passwortanforderungen:

- **Mindestlänge:** 12 Zeichen (15 für Admin-Accounts)
- **Komplexität:**
  - Großbuchstaben (A-Z)
  - Kleinbuchstaben (a-z)
  - Ziffern (0-9)
  - Sonderzeichen (!@#$%^&*)
- **Keine Wörterbuch-Wörter**
- **Keine persönlichen Informationen** (Name, Geburtsdatum, etc.)
- **Keine Wiederholung** der letzten 4 Passwörter

Passwortänderung: - Alle 90 Tage für Standard-Benutzer - Alle 90 Tage für Admin-Accounts - Sofort bei Verdacht auf Kompromittierung - Bei Erstanmeldung

Passwort-Speicherung: - Nur als Hash (bcrypt, PBKDF2, Argon2) - Niemals im Klartext - Salt für jeden Hash - Keine reversible Verschlüsselung

9.3.3 3.3 Zertifikatsbasierte Authentifizierung

Verwendung: - Server-zu-Server-Kommunikation - API-Authentifizierung - VPN-Zugriff (zusätzlich zu MFA)

Anforderungen: - Zertifikate von vertrauenswürdiger CA - Regelmäßige Erneuerung - Widerrufsprüfung (CRL/OCSP) - Sichere Schlüsselspeicherung

9.4 4. Account-Management

9.4.1 4.1 Account-Erstellung

Prozess: 1. Genehmigter Zugriffsantrag 2. Eindeutige Benutzer-ID erstellen 3. Temporäres Passwort generieren 4. MFA-Registrierung 5. Benutzer benachrichtigen 6. Passwortänderung bei Erstanmeldung erzwingen

9.4.2 4.2 Account-Deaktivierung

Automatische Deaktivierung: - Nach 90 Tagen Inaktivität - Bei Ausscheiden des Mitarbeiters - Bei Rollenänderung (alter Account)

Manuelle Deaktivierung: - Bei Sicherheitsvorfällen - Bei Verdacht auf Kompromittierung - Auf Anfrage des Managers

Prozess: 1. Account deaktivieren (nicht löschen) 2. Alle Sessions beenden 3. Zugriff validieren (sollte blockiert sein) 4. Dokumentieren

9.4.3 4.3 Account-Löschung

Zeitrahmen: - 90 Tage nach Deaktivierung - Nach Abschluss von Audits/Untersuchungen - Nach Aufbewahrungspflicht

Prozess: 1. Bestätigung, dass Account nicht mehr benötigt 2. Backup der Account-Daten (falls erforderlich) 3. Account löschen 4. Dokumentieren

9.5 5. Passwort-Management

9.5.1 5.1 Passwort-Reset

Self-Service-Reset: - Über Identity Management System - Nach erfolgreicher Identitätsprüfung - Sicherheitsfragen oder E-Mail-Verifizierung - MFA-Verifizierung

Helpdesk-Reset: - Identitätsprüfung erforderlich - Temporäres Passwort - Passwortänderung bei nächster Anmeldung erzwingen - Dokumentation des Resets

9.5.2 5.2 Passwort-Sperrung

Account-Sperrung nach: - 6 fehlgeschlagenen Anmeldeversuchen - Sperrung für 30 Minuten - Oder manuelle Entsperrung durch Admin

Entsperrung: - Automatisch nach 30 Minuten - Oder durch Helpdesk nach Identitätsprüfung - Dokumentation der Entsperrung

9.5.3 5.3 Passwort-Vault

Für privilegierte Passwörter: - Zentrale Passwort-Vault-Lösung - Automatische Passwortrotation - Check-out/Check-in-Prozess - Session-Recording - Vollständiges Logging

Vault-System: [TODO: Name des Vault-Systems]

9.6 6. Session-Management

9.6.1 6.1 Session-Timeouts

Inaktivitäts-Timeout: - 15 Minuten für CDE-Systeme - 30 Minuten für Corporate-Systeme - 5 Minuten für privilegierte Sessions

Maximale Session-Dauer: - 8 Stunden für Standard-Benutzer - 4 Stunden für Admin-Sessions - Re-Authentifizierung erforderlich

9.6.2 6.2 Session-Sicherheit

Anforderungen: - Eindeutige Session-IDs - Session-ID-Rotation nach Login - Sichere Session-Cookies (HttpOnly, Secure, SameSite) - Session-Invalidierung bei Logout - Keine Session-IDs in URLs

9.6.3 6.3 Concurrent Sessions

Beschränkungen: - Maximal 2 gleichzeitige Sessions pro Benutzer - Nur 1 privilegierte Session gleichzeitig - Warnung bei neuer Session - Option zum Beenden alter Sessions

9.7 7. Remote-Authentifizierung

9.7.1 7.1 VPN-Zugriff

Authentifizierung: - Benutzername + Passwort - Plus MFA (Hardware-Token oder Authenticator App) - Zertifikatsbasierte Authentifizierung (optional)

Autorisierung: - Nur autorisierte Benutzer - Zugriff auf spezifische Netzwerksegmente - Vollständiges Logging

9.7.2 7.2 Jump Server

Authentifizierung: - MFA erforderlich - Privilegierte Accounts - Session-Recording - Zeitlich begrenzter Zugriff

Zugriffskontrolle: - Nur von autorisierten Quell-IPs - Nur zu autorisierten Ziel-Systemen - Vollständiges Logging

9.8 8. Anwendungs-Authentifizierung

9.8.1 8.1 Web-Anwendungen

Authentifizierung: - Benutzername + Passwort - MFA für CDE-Anwendungen - Session-Management - HTTPS erforderlich

Sicherheitsmaßnahmen: - Schutz vor Brute-Force (Rate Limiting) - CAPTCHA nach mehreren Fehlversuchen - Account-Sperrung - Sichere Passwort-Speicherung

9.8.2 8.2 API-Authentifizierung

Methoden: - API-Keys (mit Ablaufdatum) - OAuth 2.0 - JWT (JSON Web Tokens) - Mutual TLS

Anforderungen: - Keine API-Keys in Code - Rotation von API-Keys - Scope-basierte Autorisierung - Rate Limiting

9.9 9. Service-Account-Management

9.9.1 9.1 Service-Accounts

Anforderungen: - Eindeutige Service-Account-IDs - Dokumentierte Verwendung - Starke Passwörter (32+ Zeichen) - Regelmäßige Passwortrotation (90 Tage) - Keine interaktiven Logins

Namenskonvention: - Format: `svc-servicename` - Beispiel: `svc-payment-gateway`

9.9.2 9.2 Service-Account-Überwachung

Monitoring: - Alle Service-Account-Aktivitäten loggen - Alerts bei ungewöhnlichen Aktivitäten - Regelmäßige Überprüfung der Verwendung - Deaktivierung ungenutzter Accounts

9.10 10. Authentifizierungs-Logging

9.10.1 10.1 Geloggte Ereignisse

Erfolgreiche Authentifizierung: - Benutzer-ID - Zeitstempel - Quell-IP-Adresse - Ziel-System - Authentifizierungsmethode

Fehlgeschlagene Authentifizierung: - Benutzer-ID (oder Versuch) - Zeitstempel - Quell-IP-Adresse - Ziel-System - Fehlergrund

Weitere Ereignisse: - Passwortänderungen - Account-Sperrungen - Account-Entsperrungen - MFA-Registrierung - Privilegierte Aktionen

9.10.2 10.2 Log-Retention

Aufbewahrung: - 90 Tage online - 1 Jahr Archiv - Unveränderlich (WORM)

Log-Forwarding: - An SIEM-System - Echtzeitübertragung - Verschlüsselte Übertragung

9.11 11. Authentifizierungs-Monitoring

9.11.1 11.1 Alerting

Alert	Bedingung	Schweregrad	Benachrichtigung
Mehrfache fehlgeschlagene Logins	>5 in 15 Min	Mittel	SOC
Admin-Login außerhalb Geschäftszeiten	Nach 22:00 Uhr	Mittel	SOC + Manager
MFA-Fehler	>3 Fehler	Niedrig	SOC
Account-Sperrung	Jede Sperrung	Niedrig	Helpdesk
Privilegierter Zugriff	Jeder Zugriff	Niedrig	SIEM
Passwortänderung	Außerhalb Geschäftszeiten	Niedrig	SIEM

9.11.2 11.2 Anomalie-Erkennung

Überwachung: - Ungewöhnliche Login-Zeiten - Ungewöhnliche Quell-IPs - Geografische Anomalien - Mehrfache gleichzeitige Logins - Privilegierte Zugriffe

9.12 12. Vendor Default Accounts

9.12.1 12.1 Default Account Management

Anforderungen: - Alle Default Accounts identifizieren - Default Accounts deaktivieren oder löschen - Falls erforderlich: Passwort ändern - Dokumentation aller Default Accounts

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

9.12.2 12.2 Default Account Inventory

System	Default Account	Status	Aktion
[TODO: System 1]	admin	Deaktiviert	Gelöscht
[TODO: System 2]	root	Aktiv	Passwort geändert
[TODO: System 3]	Administrator	Deaktiviert	Umbenannt

9.13 13. Authentifizierungs-Testing

9.13.1 13.1 Penetrationstests

Jährlich: - Authentifizierungsmechanismen testen - Brute-Force-Angriffe simulieren - MFA-Bypass-Versuche - Session-Management-Tests

9.13.2 13.2 Vulnerability Scans

Quartalsweise: - Schwache Passwörter identifizieren - Default Accounts identifizieren - Authentifizierungs-Schwachstellen

9.14 14. Compliance-Validierung

9.14.1 14.1 Validierungsaktivitäten

Quartalsweise: - Passwortrichtlinien-Compliance - MFA-Implementierung validieren - Inaktive Accounts identifizieren - Default Accounts überprüfen

Jährlich: - Vollständige Authentifizierungs-Audit - Penetrationstest - Compliance-Assessment

9.14.2 14.2 Validierungsdokumentation

Erforderliche Nachweise: - Authentifizierungsrichtlinien - MFA-Konfiguration - Passwortrichtlinien-Konfiguration - Account-Management-Protokolle - Penetrationstest-Berichte

---

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated | default }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 10

Physische Sicherheit

Dokument-ID: PCI-0420
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

10.1 1. Zweck

Dieses Dokument definiert die physischen Sicherheitskontrollen für AdminSend GmbH gemäß PCI-DSS Requirement 9.

10.1.1 1.1 Ziele

- **Physischer Schutz:** Schutz von CDE-Systemen vor unbefugtem Zugriff
- **Zutrittskontrolle:** Restriktion des physischen Zugangs
- **Medien-Sicherheit:** Sichere Handhabung von Datenträgern
- **Compliance:** Erfüllung von PCI-DSS Requirement 9

10.1.2 1.2 Geltungsbereich

Betroffene Standorte: - Rechenzentren mit CDE-Systemen - Serverräume - Büros mit POS-Terminals - Lagerräume für Medien

10.2 2. Physische Zutrittskontrolle

10.2.1 2.1 Zutrittskontrollsysteme

Implementierte Systeme: - Badge-System: [TODO: Name des Systems] - Biometrische Authentifizierung: [TODO: Typ] - Videoüberwachung: [TODO: Anzahl Kameras] - Alarmsystem: [TODO:

Name des Systems]

Anforderungen: - Eindeutige Identifikation jeder Person - Logging aller Zutritte - Automatische Sperrung nach Geschäftszeiten - Alarmierung bei unbefugtem Zutritt

10.2.2 2.2 Zutrittsberechtigung

Berechtigungsstufen:

Stufe	Berechtigung	Bereiche	Personen
Stufe 1	Vollzugriff	Alle Bereiche	Facility Manager, CISO
Stufe 2	CDE-Zugriff	Rechenzentrum, Serverräume	IT-Administratoren
Stufe 3	Eingeschränkt	Büros mit POS	Kassierer, Support
Stufe 4	Begleitet	Alle Bereiche	Besucher, Dienstleister

Genehmigungsprozess: 1. Antrag durch Manager 2. Security-Prüfung 3. CISO-Genehmigung (für CDE-Bereiche) 4. Badge-Ausgabe 5. Dokumentation

10.2.3 2.3 Zutrittskontrolle Rechenzentrum

Anforderungen: - Zwei-Faktor-Authentifizierung (Badge + Biometrie) - Mantrap/Schleuse - Videoüberwachung (24/7) - Alarmierung bei unbefugtem Zutritt - Logging aller Zutritte

Autorisierte Personen: - Datacenter-Personal - Autorisierte IT-Administratoren - Wartungspersonal (nur mit Begleitung)

Besucherregelung: - Voranmeldung erforderlich - Begleitpflicht - Besucherausweis - Logging

10.3 3. Besuchermanagement

10.3.1 3.1 Besucheranmeldung

Prozess: 1. Voranmeldung durch Gastgeber 2. Identitätsprüfung bei Ankunft 3. Besucherausweis ausgeben 4. Sicherheitsbelehrung 5. Begleitung durch autorisierten Mitarbeiter 6. Rückgabe des Ausweises bei Verlassen

Besucherausweis: - Deutlich sichtbar - Zeitlich begrenzt - Eindeutige Nummer - Foto (optional)

10.3.2 3.2 Besucherbegleitung

Anforderungen: - Ständige Begleitung in CDE-Bereichen - Begleiter muss autorisiert sein - Keine unbeaufsichtigten Besucher - Dokumentation der Begleitung

Ausnahmen: - Öffentliche Bereiche (Empfang, Cafeteria) - Nur nach Sicherheitsbelehrung

10.3.3 3.3 Besucherprotokoll

Geloggte Informationen: - Name des Besuchers - Firma - Zweck des Besuchs - Gastgeber - Ankunftszeit - Abfahrtszeit - Besuchte Bereiche - Begleiter

Aufbewahrung: 90 Tage

10.4 4. Mitarbeiter-Identifikation

10.4.1 4.1 Mitarbeiterausweise

Anforderungen: - Foto-ID - Name - Mitarbeiternummer - Abteilung - Gültigkeitsdatum - Sichtbar zu tragen

Ausgabe: - Bei Einstellung - Nach Identitätsprüfung - Dokumentation

Rückgabe: - Bei Ausscheiden - Bei Verlust (Sperrung + Neuausgabe)

10.4.2 4.2 Unterscheidung Mitarbeiter/Besucher

Maßnahmen: - Unterschiedliche Ausweisfarben - Deutliche Kennzeichnung "BESUCHER" - Zeitlich begrenzte Besucherausweise

10.5 5. Videoüberwachung

10.5.1 5.1 Kamerastandorte

Überwachte Bereiche: - Alle Eingänge zum Rechenzentrum - Serverräume - Bereiche mit POS-Terminals - Lagerräume für Medien - Parkplätze (optional)

Kamera-Spezifikationen: - Mindestauflösung: 1080p - Nachtsicht-fähig - Bewegungserkennung - Manipulationsschutz

10.5.2 5.2 Aufzeichnung und Speicherung

Anforderungen: - Kontinuierliche Aufzeichnung (24/7) - Aufbewahrung: 90 Tage - Sichere Speicherung (verschlüsselt) - Zugriffskontrolle auf Aufzeichnungen - Backup der Aufzeichnungen

Zugriff auf Aufzeichnungen: - Nur autorisiertes Personal - Logging aller Zugriffe - Genehmigung durch Security Manager

10.5.3 5.3 Datenschutz

Maßnahmen: - Hinweisschilder auf Videoüberwachung - Datenschutzerklärung - Keine Überwachung von Privatbereichen (Toiletten, Umkleiden) - Einhaltung DSGVO

10.6 6. Medien-Handling

10.6.1 6.1 Medien-Klassifizierung

Klassifizierungsstufen:

Stufe	Beschreibung	Beispiele	Handhabung
Kritisch	CHD im Klartext	Backup-Tapes mit unverschlüsselten CHD	Verschlüsselt, gesichert
Vertraulich	CHD verschlüsselt	Verschlüsselte Backups	Gesichert
Intern	Keine CHD	Systemlogs	Standard
Öffentlich	Keine sensiblen Daten	Marketing-Material	Keine Einschränkung

10.6.2 6.2 Medien-Lagerung

Anforderungen: - Gesicherter Lagerraum - Zutrittskontrolle - Klimatisierung - Brandschutz - Inventarverwaltung

Lagerraum-Spezifikationen: - Feuerfeste Schränke für kritische Medien - Verschlossene Schränke - Zutrittskontrolle (Badge-System) - Videoüberwachung - Logging aller Zugriffe

10.6.3 6.3 Medien-Transport

Interner Transport: - Versiegelte Container - Begleitperson - Dokumentation (Übergabeprotokoll)

Externer Transport: - Verschlüsselte Medien - Versiegelte Container - Vertrauenswürdiger Kurier - Tracking - Versicherung - Dokumentation

Kurier-Anforderungen: - Hintergrundprüfung - Vertraulichkeitsvereinbarung - Versicherung - Tracking-System

10.7 7. Medien-Vernichtung

10.7.1 7.1 Vernichtungsmethoden

Papier: - Kreuzschnitt-Schredder (DIN 66399 P-4 oder höher) - Für CHD: P-5 oder höher - Sichere Entsorgung der Schnipsel

Elektronische Medien:

Medientyp	Methode	Standard
Festplatten	Degaussing + physische Zerstörung	NIST 800-88
SSDs	Kryptografisches Löschen + Zerstörung	NIST 800-88
USB-Sticks	Physische Zerstörung	NIST 800-88
CDs/DVDs	Schreddern	DIN 66399 O-4
Backup-Tapes	Degaussing + Schreddern	NIST 800-88

Zertifizierung: - Vernichtungszertifikat erforderlich - Dokumentation aller vernichteten Medien - Seriennummern erfassen

10.7.2 7.2 Vernichtungsdienstleister

Anforderungen: - Zertifizierter Dienstleister (z.B., DIN 66399) - Vertraulichkeitsvereinbarung - Vor-Ort-Vernichtung oder sichere Abholung - Vernichtungszertifikat - Versicherung

Dienstleister: [TODO: Name des Dienstleisters]

10.7.3 7.3 Vernichtungsprotokoll

Geloggte Informationen: - Datum der Vernichtung - Medientyp - Seriennummer (falls vorhanden) - Vernichtungsmethode - Durchgeführt von - Zertifikatsnummer

Aufbewahrung: 3 Jahre

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

10.8.1 8.1 POS-Terminal-Schutz

Physische Sicherheit: - Manipulationsschutz (Tamper-evident Seals) - Regelmäßige Inspektion - Sichere Befestigung - Videoüberwachung des Bereichs

Inspektion: - Täglich vor Geschäftsbeginn - Nach Wartung - Bei Verdacht auf Manipulation

Checkliste: - [ ] Tamper-Seal intakt - [ ] Keine ungewöhnlichen Geräte angeschlossen - [ ] Keine Beschädigungen - [ ] Firmware-Version korrekt

10.8.2 8.2 POS-Terminal-Inventar

Inventarverwaltung: - Liste aller POS-Terminals - Seriennummern - Standorte - Verantwortliche Personen - Wartungshistorie

Quartalsweise Überprüfung: - Inventar validieren - Standorte überprüfen - Tamper-Seals prüfen - Dokumentation

10.8.3 8.3 POS-Terminal-Wartung

Wartungsprozess: 1. Wartung ankündigen 2. Begleitung durch autorisierten Mitarbeiter 3. Dokumentation aller Aktivitäten 4. Neue Tamper-Seals anbringen 5. Funktionstest 6. Dokumentation

10.9 9. Medien-Backup

10.9.1 9.1 Backup-Medien-Sicherheit

Anforderungen: - Verschlüsselte Backups - Sichere Lagerung - Offsite-Lagerung - Zutrittskontrolle - Inventarverwaltung

Lagerung: - Onsite: Feuerfester Tresor - Offsite: Sicheres Rechenzentrum oder Tresorraum

10.9.2 9.2 Backup-Medien-Transport

Prozess: - Verschlüsselte Medien - Versiegelte Container - Vertrauenswürdiger Kurier - Übergabeprotokoll - Dokumentation

10.10 10. Arbeitsplatz-Sicherheit

10.10.1 10.1 Clean Desk Policy

Anforderungen: - Keine sensiblen Dokumente auf Schreibtischen - Bildschirme sperren bei Abwesenheit - Dokumente in verschlossenen Schränken - Keine Passwörter auf Notizzetteln

Kontrollen: - Regelmäßige Inspektionen - Sensibilisierung der Mitarbeiter

10.10.2 10.2 Bildschirm-Sichtschutz

Anforderungen: - Privacy-Filter für Bildschirme mit CHD - Bildschirme nicht von außen einsehbar - Automatische Bildschirmsperre (15 Minuten)

10.11 11. Notfallzugang

10.11.1 11.1 Break-Glass-Verfahren

Prozess: - Versiegelter Umschlag mit Notfall-Zugangsdaten - Lagerung in Tresor - Zugriff nur mit Zeugen - Dokumentation jeder Verwendung - Sofortige Passwortänderung nach Verwendung

Dokumentation: - Datum und Uhrzeit - Grund für Notfallzugang - Durchgeführt von - Zeuge - Durchgeführte Aktionen

10.11.2 11.2 Notfall-Evakuierung

Prozess: - Evakuierungsplan - Sammelplätze - Verantwortliche Personen - Regelmäßige Übungen

Sicherheitsmaßnahmen: - Automatische Sperrung aller Systeme - Aktivierung Alarmsystem - Benachrichtigung Security

10.12 12. Compliance-Validierung

10.12.1 12.1 Validierungsaktivitäten

Quartalsweise: - POS-Terminal-Inspektion - Medien-Inventar - Besucherprotokoll-Review - Videoüberwachungs-Test

Jährlich: - Physische Sicherheits-Audit - Penetrationstest (physisch) - Mitarbeiter-Sensibilisierung

10.12.2 12.2 Validierungsdokumentation

Erforderliche Nachweise: - Zutrittskontroll-Protokolle - Besucherprotokolle - POS-Inspektionsprotokolle - Medien-Vernichtungszertifikate - Videoaufzeichnungen (90 Tage)

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 11

Logging und Monitoring

Dokument-ID: PCI-0500
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

11.1 1. Zweck

Dieses Dokument definiert die Logging- und Monitoring-Anforderungen für AdminSend GmbH gemäß PCI-DSS Requirement 10.

11.1.1 1.1 Ziele

- **Nachvollziehbarkeit:** Alle Zugriffe auf CDE und CHD loggen
- **Anomalie-Erkennung:** Verdächtige Aktivitäten identifizieren
- **Incident Response:** Forensische Untersuchungen ermöglichen
- **Compliance:** Erfüllung von PCI-DSS Requirement 10

11.1.2 1.2 Geltungsbereich

Betroffene Systeme: - Alle CDE-Systeme - Systeme mit CHD-Zugriff - Netzwerkkomponenten - Sicherheitssysteme

11.2 2. Logging-Anforderungen

11.2.1 2.1 Zu loggende Ereignisse

Benutzer-Zugriffe: - Alle Anmeldungen (erfolgreich und fehlgeschlagen) - Alle Abmeldungen - Privilegierte Aktionen - Zugriff auf CHD - Berechtigungsänderungen

System-Ereignisse: - System-Starts und -Stops - Konfigurationsänderungen - Software-Installationen - Patch-Installationen - Dienst-Starts und -Stops

Netzwerk-Ereignisse: - Firewall-Regel-Änderungen - Blockierte Verbindungen - VPN-Verbindungen - IDS/IPS-Alerts

Sicherheits-Ereignisse: - Antivirus-Detektionen - Sicherheitsrichtlinien-Verletzungen - Account-Sperrungen - Passwortänderungen

Datenbank-Ereignisse: - Alle Zugriffe auf CHD-Tabellen - Schema-Änderungen - Privilegierte Datenbankoperationen - Fehlgeschlagene Zugriffe

11.2.2 2.2 Log-Einträge-Format

Erforderliche Felder: - **Benutzer-ID:** Wer hat die Aktion durchgeführt? - **Ereignistyp:** Was ist passiert? - **Zeitstempel:** Wann ist es passiert? (synchronisierte Zeit) - **Erfolg/Fehler:** War die Aktion erfolgreich? - **Quelle:** Von wo kam die Aktion? (IP-Adresse, Hostname) - **Ziel:** Welches System/Ressource war betroffen? - **Zusätzliche Details:** Relevante Kontextinformationen

Beispiel:

```
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-Implementierung

SIEM-System: [TODO: Name des SIEM-Systems]

Funktionen: - Zentrale Log-Sammlung - Echtzeitanalyse - Korrelation von Ereignissen - Alerting - Reporting - Forensische Suche

Architektur: - Log-Quellen → Log-Forwarder → SIEM - Verschlüsselte Übertragung (TLS 1.2+) - Redundante SIEM-Server - Sichere Log-Speicherung

11.3.2 3.2 Log-Forwarding

Konfiguration: - Alle CDE-Systeme senden Logs an SIEM - Echtzeitübertragung (< 5 Minuten Verzögerung) - Verschlüsselte Übertragung - Authentifizierung der Log-Quellen

Log-Forwarder: - Syslog (RFC 5424) - Windows Event Forwarding - Agent-basiert (z.B., Splunk Forwarder, Elastic Beats)

11.3.3 3.3 Log-Parsing und -Normalisierung

Anforderungen: - Einheitliches Log-Format - Parsing aller relevanten Felder - Normalisierung von Zeitstempeln - Anreicherung mit Kontext (z.B., Geo-IP)

11.4 4. Log-Retention

11.4.1 4.1 Aufbewahrungsfristen

Online-Speicherung: - 90 Tage in SIEM (schneller Zugriff) - Volltext-Suche möglich - Echtzeitanalyse

Archiv-Speicherung: - 1 Jahr in Archiv - Komprimiert - Verschlüsselt - WORM-Speicher (Write Once Read Many)

Langzeit-Archivierung: - Nach gesetzlichen Anforderungen - Sichere Lagerung - Dokumentation

11.4.2 4.2 Log-Backup

Anforderungen: - Tägliche Backups der Logs - Offsite-Lagerung - Verschlüsselte Backups - Regelmäßige Restore-Tests

11.5 5. Log-Integrität

11.5.1 5.1 Schutz vor Manipulation

Maßnahmen: - WORM-Speicher für Logs - Digitale Signaturen - Hash-Werte für Log-Dateien - Zugriffskontrolle auf Logs - Logging von Log-Zugriffen

Validierung: - Regelmäßige Integritätsprüfung - Automatische Alerts bei Manipulation - Forensische Untersuchung bei Verdacht

11.5.2 5.2 Log-Zugriffskontrolle

Berechtigungen: - Nur autorisiertes Personal - Read-Only-Zugriff für die meisten Benutzer - Vollzugriff nur für Log-Administratoren - Logging aller Log-Zugriffe

Rollen: - Log-Administrator: Vollzugriff - Security-Analyst: Lesezugriff, Suche, Alerting - Auditor: Lesezugriff - Standard-Benutzer: Kein Zugriff

11.6 6. Zeitsynchronisation

11.6.1 6.1 NTP-Konfiguration

Anforderungen: - Alle Systeme synchronisiert mit NTP - Interne NTP-Server - Externe NTP-Quellen (Stratum 1 oder 2) - Redundante NTP-Server

NTP-Server: - Primär: [TODO: IP-Adresse] - Sekundär: [TODO: IP-Adresse] - Externe Quelle: [TODO: z.B., ptbtime1.ptb.de]

Zeitzone: - UTC für alle Logs - Lokale Zeitzone für Anzeige (mit UTC-Offset)

11.6.2 6.2 Zeitabweichungs-Monitoring

Überwachung: - Maximale Abweichung: 1 Sekunde - Alerts bei Abweichung $>$ 1 Sekunde - Automatische Korrektur - Logging von Zeitänderungen

11.7 7. Monitoring und Alerting

11.7.1 7.1 Security Monitoring

24/7 Monitoring: - Security Operations Center (SOC) - Echtzeitüberwachung aller Alerts - Incident Response bei kritischen Alerts - Eskalation nach Schweregrad

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

11.7.2 7.2 Alerting-Regeln

Kritische Alerts:

Alert	Bedingung	Aktion	Eskalation
Mehrfache fehlgeschlagene Logins	>10 in 5 Min	Sofortige Untersuchung	SOC → CISO
Unbefugter CDE-Zugriff	Blockierte Verbindung zu CDE	Sofortige Untersuchung	SOC → IT Security
Malware-Detektion	Antivirus-Alert	Isolation des Systems	SOC → IT Security
Datenexfiltration	Große Datenübertragung	Verbindung blockieren	SOC → CISO
Privilegierte Aktion	Root/Admin-Aktion	Logging, Review	SOC
Firewall-Regel-Änderung	Konfigurationsänderung	Validierung	SOC → Network Team

Hohe Alerts: - Admin-Login außerhalb Geschäftszeiten - Zugriff auf CHD - Konfigurationsänderungen - Neue Software-Installation

Mittlere Alerts: - Fehlgeschlagene Authentifizierung - Passwortänderung - Account-Sperrung

Niedrige Alerts: - Informative Ereignisse - Routine-Aktivitäten

11.7.3 7.3 Alert-Response

Prozess: 1. Alert empfangen 2. Schweregrad bewerten 3. Initiale Untersuchung 4. Eskalation (falls erforderlich) 5. Incident Response (falls erforderlich) 6. Dokumentation 7. Follow-up

Response-Zeiten: - Kritisch: Sofort (< 15 Minuten) - Hoch: < 1 Stunde - Mittel: < 4 Stunden - Niedrig: < 24 Stunden

11.8 8. Log-Review

11.8.1 8.1 Tägliche Log-Review

Prozess: - Automatisierte Analyse durch SIEM - Review kritischer Alerts - Identifikation von Anomalien - Dokumentation von Findings

Verantwortlich: SOC-Team

11.8.2 8.2 Wöchentliche Log-Review

Prozess: - Review aller Alerts der Woche - Trend-Analyse - Identifikation von Mustern - Optimierung von Alerting-Regeln

Verantwortlich: Senior SOC-Analyst

11.8.3 8.3 Monatliche Log-Review

Prozess: - Umfassende Analyse aller Logs - Compliance-Validierung - Reporting an Management - Identifikation von Verbesserungen

Verantwortlich: IT Security Manager

11.9 9. Use Cases und Korrelationsregeln

11.9.1 9.1 Definierte Use Cases

Authentifizierung: - Brute-Force-Angriffe - Credential Stuffing - Ungewöhnliche Login-Zeiten - Geografische Anomalien

Zugriffskontrolle: - Unbefugte Zugriffe - Privilegien-Eskalation - Lateral Movement

Datenexfiltration: - Große Datenübertragungen - Ungewöhnliche Datenzugriffe - Zugriff auf viele Datensätze

Malware: - Antivirus-Detektionen - Verdächtige Prozesse - Command & Control-Kommunikation

Insider-Bedrohungen: - Ungewöhnliche Benutzeraktivitäten - Zugriff außerhalb Arbeitszeiten - Massendownloads

11.9.2 9.2 Korrelationsregeln

Beispiel-Regel: Brute-Force-Angriff

```
IF (fehlgeschlagene_logins > 10 IN 5 Minuten)
AND (gleiche_quell_ip)
THEN
  ALERT "Brute-Force-Angriff erkannt"
  SEVERITY = CRITICAL
  ACTION = Block_IP
```

Beispiel-Regel: Privilegien-Eskalation

```
IF (benutzer_erhält_admin_rechte)
AND (benutzer_führt_privilegierte_aktion_aus IN 10 Minuten)
THEN
  ALERT "Mögliche Privilegien-Eskalation"
  SEVERITY = HIGH
  ACTION = Investigate
```

11.10 10. Audit Trails

11.10.1 10.1 Audit Trail-Anforderungen

Für alle CHD-Zugriffe: - Vollständige Audit Trails - Unveränderlich - Nachvollziehbar - Zeitlich geordnet

Informationen: - Wer hat zugegriffen? - Wann wurde zugegriffen? - Welche Daten wurden zugegriffen? - Welche Aktion wurde durchgeführt? - War die Aktion erfolgreich?

11.10.2 10.2 Audit Trail-Review

Prozess: - Regelmäßige Review (täglich für kritische Systeme) - Identifikation von Anomalien - Dokumentation von Findings - Follow-up bei Auffälligkeiten

11.11 11. Forensische Untersuchungen

11.11.1 11.1 Log-Analyse für Forensik

Prozess: 1. Incident identifiziert 2. Relevante Logs sammeln 3. Timeline erstellen 4. Ursachenanalyse 5. Dokumentation 6. Lessons Learned

Tools: - SIEM-Forensik-Funktionen - Log-Analyse-Tools - Timeline-Analyse-Tools

11.11.2 11.2 Chain of Custody

Anforderungen: - Dokumentation aller Log-Zugriffe - Unveränderlichkeit der Logs - Nachvollziehbare Beweiskette - Rechtssichere Dokumentation

11.12 12. Compliance-Validierung

11.12.1 12.1 Validierungsaktivitäten

Täglich: - Log-Review - Alert-Response - Anomalie-Erkennung

Wöchentlich: - Trend-Analyse - Use Case-Validierung

Monatlich: - Umfassende Log-Review - Compliance-Reporting

Quartalsweise: - Log-Retention-Validierung - SIEM-Konfiguration-Review

Jährlich: - Vollständige Logging-Audit - Penetrationstest - Compliance-Assessment

11.12.2 12.2 Validierungsdokumentation

Erforderliche Nachweise: - Logging-Konfiguration - SIEM-Konfiguration - Log-Review-Protokolle - Alert-Response-Protokolle - Forensische Untersuchungsberichte

---

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 12

Netzwerksicherheitstests

Dokument-ID: PCI-0510
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

12.1 1. Zweck

Dieses Dokument definiert die Netzwerksicherheitstests für AdminSend GmbH gemäß PCI-DSS Requirement 11.

12.1.1 1.1 Ziele

- **Schwachstellen-Identifikation:** Regelmäßige Vulnerability Scans
- **Penetrationstests:** Jährliche Sicherheitstests
- **Intrusion Detection:** IDS/IPS-Implementierung
- **Compliance:** Erfüllung von PCI-DSS Requirement 11

12.1.2 1.2 Geltungsbereich

Betroffene Systeme: - Alle CDE-Systeme - Perimeter-Systeme - Interne Netzwerke - Webanwendungen

12.2 2. Vulnerability Scanning

12.2.1 2.1 Quartalsweise Scans

Anforderungen: - Quartalsweise externe Scans durch ASV - Quartalsweise interne Scans - Nach signifikanten Änderungen - Alle Systeme im CDE

ASV (Approved Scanning Vendor): - Name: [TODO: ASV-Name] - Kontakt: [TODO: Kontakt] - Letzte Scan: [TODO: Datum] - Nächste Scan: [TODO: Datum]

12.2.2 2.2 Externe Vulnerability Scans

Prozess: 1. ASV-Scan beauftragen 2. Scan durchführen lassen 3. Ergebnisse analysieren 4. Schwachstellen beheben 5. Re-Scan durchführen 6. Passing Scan erreichen 7. ASV-Bericht archivieren

Passing Scan-Kriterien: - Keine Schwachstellen mit CVSS 4.0 - Alle kritischen Schwachstellen behoben - ASV-Bestätigung

12.2.3 2.3 Interne Vulnerability Scans

Prozess: - Quartalsweise Scans aller internen Systeme - Authentifizierte Scans (mit Credentials) - Vollständige Netzwerk-Scans - Schwachstellen-Priorisierung - Remediation-Plan

Scan-Tool: [TODO: Name des Scan-Tools]

Scan-Umfang: - Alle CDE-Systeme - Alle Systeme mit CHD-Zugriff - Netzwerkkomponenten - Datenbanken - Webanwendungen

12.2.4 2.4 Schwachstellen-Management

Priorisierung:

CVSS-Score	Schweregrad	Remediation-Frist
9.0 - 10.0	Kritisch	7 Tage
7.0 - 8.9	Hoch	30 Tage
4.0 - 6.9	Mittel	90 Tage
0.1 - 3.9	Niedrig	180 Tage

Remediation-Prozess: 1. Schwachstelle identifiziert 2. Risikobewertung 3. Remediation-Plan erstellen 4. Patch/Fix implementieren 5. Validierung 6. Dokumentation

12.3 3. Penetrationstests

12.3.1 3.1 Jährliche Penetrationstests

Anforderungen: - Jährlich durch qualifizierte Tester - Nach signifikanten Änderungen - Externe und interne Tests - Netzwerk- und Anwendungs-Tests

Penetrationstest-Firma: - Name: [TODO: Firma] - Kontakt: [TODO: Kontakt] - Letzter Test: [TODO: Datum] - Nächster Test: [TODO: Datum]

12.3.2 3.2 Externe Penetrationstests

Umfang: - Perimeter-Systeme - Öffentlich zugängliche Webanwendungen - VPN-Zugänge - E-Mail-Systeme

Methodik: - Black-Box-Testing - Exploitation von Schwachstellen - Social Engineering (optional) - Dokumentation aller Findings

12.3.3 3.3 Interne Penetrationstests

Umfang: - CDE-Netzwerk - Interne Anwendungen - Lateral Movement-Tests - Privilegien-Eskalation

Methodik: - Gray-Box-Testing - Authentifizierte Tests - Exploitation - Post-Exploitation

12.3.4 3.4 Segmentierungstests

Anforderungen: - Validierung der Netzwerksegmentierung - Versuche, CDE-Grenzen zu überschreiten - Firewall-Regel-Validierung - Dokumentation der Ergebnisse

Prozess: 1. Segmentierung dokumentieren 2. Test-Szenarien definieren 3. Penetrationstest durchführen 4. Ergebnisse analysieren 5. Schwachstellen beheben 6. Re-Test 7. Dokumentation

12.4 4. Intrusion Detection/Prevention

12.4.1 4.1 IDS/IPS-Implementierung

Anforderungen: - IDS/IPS an allen CDE-Grenzen - Echtzeitüberwachung - Automatische Alerts - Regelmäßige Signatur-Updates

IDS/IPS-Systeme:

System	Typ	Standort	Funktion
[TODO: IDS-01]	Network IDS	Perimeter	Erkennung
[TODO: IPS-01]	Network IPS	CDE-Grenze	Prävention
[TODO: HIDS-01]	Host IDS	CDE-Server	Erkennung

12.4.2 4.2 IDS/IPS-Signaturen

Anforderungen: - Aktuelle Signaturen - Tägliche Updates - Custom Signaturen für bekannte Bedrohungen - Regelmäßige Überprüfung

Update-Prozess: 1. Signatur-Updates herunterladen 2. In Testumgebung testen 3. In Produktion deployen 4. Validierung 5. Dokumentation

12.4.3 4.3 IDS/IPS-Alerting

Alert-Kategorien: - Kritisch: Sofortige Aktion erforderlich - Hoch: Untersuchung innerhalb 1 Stunde - Mittel: Untersuchung innerhalb 4 Stunden - Niedrig: Review innerhalb 24 Stunden

Alert-Response: - Automatische Benachrichtigung an SOC - Initiale Untersuchung - Eskalation bei Bedarf - Incident Response - Dokumentation

12.5 5. File Integrity Monitoring (FIM)

12.5.1 5.1 FIM-Implementierung

Anforderungen: - FIM auf allen CDE-Systemen - Überwachung kritischer Dateien - Echtzeitüberwachung - Automatische Alerts

FIM-Tool: [TODO: Name des FIM-Tools]

12.5.2 5.2 Überwachte Dateien

Kritische Dateien: - Systemdateien - Konfigurationsdateien - Anwendungsdateien - Logdateien - Datenbank-Dateien

Beispiele: - `/etc/passwd`, `/etc/shadow` (Linux) - `C:\Windows\System32\config\SAM` (Windows) - Firewall-Konfigurationen - Webserver-Konfigurationen - Datenbank-Konfigurationen

12.5.3 5.3 FIM-Alerting

Alerts bei: - Dateiänderungen - Dateilöschungen - Neue Dateien - Berechtigungsänderungen - Eigentümeränderungen

Alert-Response: 1. Alert empfangen 2. Änderung validieren 3. Autorisierte Änderung? (Change Request) 4. Falls nicht autorisiert: Incident Response 5. Dokumentation

12.6 6. Change Detection

12.6.1 6.1 Change Detection-Mechanismen

Anforderungen: - Automatische Erkennung von Änderungen - Vergleich mit Baseline - Alerting bei unautorisierten Änderungen - Dokumentation aller Änderungen

Überwachte Änderungen: - Konfigurationsänderungen - Software-Installationen - Patch-Installationen - Benutzer-Änderungen - Berechtigungsänderungen

12.6.2 6.2 Baseline-Management

Prozess: 1. Initiale Baseline erstellen 2. Baseline dokumentieren 3. Regelmäßige Validierung 4. Aktualisierung nach genehmigten Änderungen 5. Dokumentation

Baseline-Komponenten: - Systemkonfiguration - Installierte Software - Netzwerkkonfiguration - Benutzer und Berechtigungen - Dienste und Prozesse

12.7 7. Wireless Security Testing

12.7.1 7.1 Wireless Access Point Detection

Anforderungen: - Quartalsweise Scans nach Wireless APs - Erkennung von Rogue APs - Validierung autorisierter APs - Dokumentation

Scan-Methoden: - Wireless Scanner - Physische Inspektionen - Netzwerk-Scans

12.7.2 7.2 Wireless Security Standards

Anforderungen für autorisierte WLANs: - WPA3 oder WPA2 mit AES - Starke Authentifizierung (802.1X) - Separate VLAN für WLAN - Keine Verbindung zu CDE ohne zusätzliche Kontrollen

12.8 8. Web Application Security Testing

12.8.1 8.1 Anwendungssicherheitstests

Anforderungen: - Jährliche Sicherheitstests - Nach signifikanten Änderungen - OWASP Top 10-Abdeckung - Authentifizierte und unauthentifizierte Tests

Test-Methoden: - Automatisierte Scans (DAST) - Manuelle Penetrationstests - Code-Reviews (SAST) - Fuzzing

12.8.2 8.2 OWASP Top 10

Zu testende Schwachstellen: 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-Simulationen

Anforderungen: - Regelmäßige Phishing-Tests - Verschiedene Szenarien - Mitarbeiter-Sensibilisierung - Dokumentation der Ergebnisse

Prozess: 1. Phishing-Kampagne planen 2. E-Mails versenden 3. Klickraten messen 4. Mitarbeiter schulen 5. Dokumentation

12.9.2 9.2 Physical Social Engineering

Tests: - Tailgating-Versuche - Badge-Cloning - Dumpster Diving - Pretexting

Dokumentation: - Erfolgreiche Angriffe - Schwachstellen identifizieren - Verbesserungsmaßnahmen - Mitarbeiter-Sensibilisierung

12.10 10. Compliance-Validierung

12.10.1 10.1 Validierungsaktivitäten

Quartalsweise: - Vulnerability Scans (extern und intern) - Wireless AP-Scans - FIM-Validierung

Jährlich: - Penetrationstests (extern und intern) - Segmentierungstests - Web Application Security Tests - Social Engineering Tests

12.10.2 10.2 Validierungsdokumentation

Erforderliche Nachweise: - ASV-Scan-Berichte (4 pro Jahr) - Interne Scan-Berichte (4 pro Jahr) - Penetrationstest-Berichte (1 pro Jahr) - Segmentierungstest-Berichte - FIM-Konfiguration und Logs - IDS/IPS-Konfiguration und Logs

---

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 13

Informationssicherheitsrichtlinie

Dokument-ID: PCI-0600
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

13.1 1. Zweck

Dieses Dokument definiert die Informationssicherheitsrichtlinie für AdminSend GmbH gemäß PCI-DSS Requirement 12.

13.1.1 1.1 Ziele

- **Security Governance:** Etablierung eines Sicherheits-Frameworks
- **Risikomanagement:** Systematische Risikoidentifikation und -behandlung
- **Compliance:** Erfüllung von PCI-DSS Requirement 12
- **Awareness:** Sensibilisierung aller Mitarbeiter

13.1.2 1.2 Geltungsbereich

Betroffene Personen: - Alle Mitarbeiter - Alle Dienstleister - Alle Personen mit Zugriff auf CDE oder CHD

13.2 2. Informationssicherheitsrichtlinie

13.2.1 2.1 Sicherheitsziele

Vertraulichkeit: - Schutz von Karteninhaberdaten vor unbefugtem Zugriff - Zugriffskontrolle nach Need-to-Know-Prinzip - Verschlüsselung sensibler Daten

Integrität: - Schutz vor unbefugter Änderung - Validierung von Datenänderungen - Audit Trails für alle Änderungen

Verfügbarkeit: - Sicherstellung der Systemverfügbarkeit - Business Continuity Planning - Disaster Recovery

13.2.2 2.2 Sicherheitsprinzipien

Defense in Depth: - Mehrschichtige Sicherheitskontrollen - Keine Single Point of Failure - Redundanz kritischer Systeme

Least Privilege: - Minimale erforderliche Berechtigungen - Regelmäßige Überprüfung - Zeitlich begrenzte privilegierte Zugriffe

Separation of Duties: - Trennung kritischer Funktionen - Vier-Augen-Prinzip - Keine Einzelperson mit vollständiger Kontrolle

Secure by Default: - Sichere Standardkonfigurationen - Deaktivierung unnötiger Dienste - Härtung aller Systeme

13.3 3. Rollen und Verantwortlichkeiten

13.3.1 3.1 Governance-Struktur

Executive Management: - Gesamtverantwortung für Informationssicherheit - Genehmigung der Sicherheitsrichtlinien - Bereitstellung von Ressourcen

CISO (Chief Information Security Officer): - Verantwortlich für Sicherheitsprogramm - Überwachung der Compliance - Incident Response-Koordination - Reporting an Executive Management

PCI-DSS Program Manager: - Verantwortlich für PCI-DSS-Compliance - Koordination von Assessments - Dokumentation und Nachweisführung - Liaison zu QSA und Acquiring Banks

IT Security Team: - Implementierung von Sicherheitskontrollen - Security Monitoring - Vulnerability Management - Incident Response

IT Operations: - Systemadministration - Patch Management - Backup und Recovery - Change Management

Alle Mitarbeiter: - Einhaltung der Sicherheitsrichtlinien - Meldung von Sicherheitsvorfällen - Teilnahme an Security Awareness Training

13.3.2 3.2 RACI-Matrix

Aktivität	Executive	CISO	PCI Manager	IT Security	IT Ops	Mitarbeiter
Richtlinien-Genehmigung	A	R	C	C	I	I
Sicherheitskontrollen	C	A	C	R	R	I
Compliance-Monitoring	I	A	R	C	I	I

Aktivität	Executive	CISO	PCI Manager	IT Security	IT Ops	Mitarbeiter
Incident Response	I	A	C	R	C	R
Security Awareness	C	A	C	R	I	R

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

13.4 4. Risikomanagement

13.4.1 4.1 Risikoanalyse-Prozess

Jährliche Risikoanalyse: 1. Asset-Identifikation 2. Bedrohungsidentifikation 3. Schwachstellenanalyse 4. Risikobewertung 5. Risikobehandlung 6. Dokumentation

Risikobewertung: - Eintrittswahrscheinlichkeit (1-5) - Auswirkung (1-5) - Risiko-Score = Wahrscheinlichkeit × Auswirkung

Risiko-Matrix:

Risiko-Score	Kategorie	Behandlung
20-25	Kritisch	Sofortige Maßnahmen
15-19	Hoch	Maßnahmen innerhalb 30 Tage
10-14	Mittel	Maßnahmen innerhalb 90 Tage
5-9	Niedrig	Überwachung
1-4	Sehr niedrig	Akzeptieren

13.4.2 4.2 Risikobehandlung

Optionen: - **Vermeiden:** Aktivität einstellen - **Reduzieren:** Kontrollen implementieren - **Übertragen:** Versicherung, Outsourcing - **Akzeptieren:** Risiko bewusst akzeptieren (mit Genehmigung)

Risikoakzeptanz: - Nur durch CISO oder Executive Management - Dokumentierte Begründung - Regelmäßige Überprüfung - Zeitlich begrenzt

13.5 5. Security Awareness Program

13.5.1 5.1 Schulungsprogramm

Pflichtschulungen: - Onboarding-Schulung (bei Einstellung) - Jährliche Auffrischungsschulung - Rollenspezifische Schulungen - Ad-hoc-Schulungen bei Bedarf

Schulungsinhalte: - PCI-DSS-Grundlagen - Umgang mit Karteninhaberdaten - Passwort-Sicherheit - Phishing-Erkennung - Social Engineering - Incident Reporting - Clean Desk Policy - Acceptable Use Policy

13.5.2 5.2 Schulungsdokumentation

Erforderliche Nachweise: - Schulungsteilnahme-Listen - Schulungsmaterialien - Schulungszertifikate - Wissenstests - Auffrischungsschulungen

Tracking: - Schulungsdatenbank - Automatische Erinnerungen - Compliance-Reporting

13.5.3 5.3 Awareness-Kampagnen

Regelmäßige Kampagnen: - Monatliche Security-Newsletter - Phishing-Simulationen - Security-Poster - Intranet-Artikel - Team-Meetings

13.6 6. Incident Response

13.6.1 6.1 Incident Response Plan

Phasen: 1. **Preparation:** Vorbereitung und Training 2. **Detection:** Erkennung von Incidents 3. **Analysis:** Analyse und Bewertung 4. **Containment:** Eindämmung 5. **Eradication:** Beseitigung 6. **Recovery:** Wiederherstellung 7. **Post-Incident:** Lessons Learned

Incident Response Team: - Incident Response Manager - IT Security Analysts - IT Operations - Legal/Compliance - PR/Communications - Executive Management (bei Major Incidents)

13.6.2 6.2 Incident-Klassifizierung

Schweregrade:

Schweregrad	Beschreibung	Beispiele	Response-Zeit
Kritisch	Massive Auswirkung	Datenexfiltration, Ransomware	Sofort
Hoch	Signifikante Auswirkung	Malware-Infektion, Unauthorized Access	$<$ 1 Stunde
Mittel	Moderate Auswirkung	Phishing-Erfolg, Policy-Verletzung	$<$ 4 Stunden
Niedrig	Geringe Auswirkung	Verdächtige Aktivität	$<$ 24 Stunden

13.6.3 6.3 Incident Reporting

Meldepflicht: - Alle Mitarbeiter müssen Incidents melden - Meldung an IT Security oder Helpdesk - Keine Angst vor Konsequenzen bei Meldung - Schnelle Meldung ist wichtig

Meldekanäle: - E-Mail: [TODO: security@organization.com] - Telefon: [TODO: +49 XXX XXXXXXX] - Incident-Portal: [TODO: URL] - Helpdesk: [TODO: Telefon]

13.6.4 6.4 Breach Notification

Bei Datenschutzverletzungen: - Benachrichtigung der Acquiring Banks - Benachrichtigung der Kartenmarken - Benachrichtigung der Datenschutzbehörde (DSGVO) - Benachrichtigung betroffener Karteninhaber - Forensische Untersuchung

Zeitrahmen: - Acquiring Banks: Sofort - Kartenmarken: Gemäß Vorgaben - Datenschutzbehörde: 72 Stunden (DSGVO) - Karteninhaber: Ohne unangemessene Verzögerung

13.7 7. Dienstleister-Management

13.7.1 7.1 Dienstleister-Auswahl

Due Diligence: - PCI-DSS-Compliance-Status prüfen - AOC (Attestation of Compliance) anfordern - Sicherheitskontrollen bewerten - Vertragliche Sicherheitsanforderungen

Anforderungen: - PCI-DSS-compliant (falls CHD-Zugriff) - Aktuelle AOC - Incident Response-Prozess - Versicherung

13.7.2 7.2 Dienstleister-Überwachung

Jährliche Überprüfung: - AOC-Validierung - Sicherheitskontrollen-Review - Incident-Review - Vertragskonformität

Dokumentation: - Liste aller Dienstleister - AOCs - Verträge mit PCI-Klauseln - Review-Protokolle

13.7.3 7.3 Dienstleister-Verträge

Erforderliche Klauseln: - PCI-DSS-Compliance-Verpflichtung - Incident Notification - Audit-Rechte - Datenschutz (DSGVO) - Haftung - Kündigung bei Non-Compliance

13.8 8. Dokumentenmanagement

13.8.1 8.1 Dokumentenlenkung

Anforderungen: - Versionskontrolle - Genehmigungsprozess - Regelmäßige Reviews - Archivierung alter Versionen

Dokumenten-Lifecycle: 1. Erstellung 2. Review 3. Genehmigung 4. Veröffentlichung 5. Jährlicher Review 6. Aktualisierung oder Archivierung

13.8.2 8.2 Dokumenten-Aufbewahrung

Aufbewahrungsfristen: - Richtlinien: Aktuell + 3 Jahre - Audit-Berichte: 3 Jahre - Logs: 1 Jahr - Incident-Berichte: 3 Jahre - Schulungsnachweise: 3 Jahre

13.9 9. Compliance-Monitoring

13.9.1 9.1 Kontinuierliche Überwachung

Monitoring-Aktivitäten: - Tägliches Security Monitoring - Wöchentliche Compliance-Checks - Monatliche Compliance-Reports - Quartalsweise Reviews - Jährliche Assessments

13.9.2 9.2 Compliance-Reporting

Berichte: - Monatlicher Compliance-Status an CISO - Quartalsweiser Bericht an Executive Management - Jährlicher Compliance-Bericht - Ad-hoc-Berichte bei Incidents

13.9.3 9.3 Interne Audits

Jährliche Audits: - Alle PCI-DSS-Requirements - Stichproben-basiert - Dokumentation von Findings - Korrekturmaßnahmen - Follow-up

13.10 10. Richtlinien-Review

13.10.1 10.1 Jährlicher Review

Prozess: 1. Alle Richtlinien reviewen 2. Änderungen identifizieren 3. Aktualisierungen vornehmen 4. Genehmigung einholen 5. Kommunikation an Mitarbeiter 6. Schulungen aktualisieren

Verantwortlich: CISO

13.10.2 10.2 Ad-hoc-Reviews

Anlässe: - Signifikante Änderungen im CDE - Neue Bedrohungen - Regulatorische Änderungen - Nach Major Incidents - Audit-Findings

13.11 11. Compliance-Validierung

13.11.1 11.1 Validierungsaktivitäten

Quartalsweise: - Richtlinien-Compliance-Checks - Schulungsstatus-Review - Dienstleister-AOC-Validierung

Jährlich: - Vollständige Risikoanalyse - Interne Audits - QSA-Assessment - Richtlinien-Review

13.11.2 11.2 Validierungsdokumentation

Erforderliche Nachweise: - Informationssicherheitsrichtlinie - Risikoanalyse-Berichte - Schulungsnachweise - Incident Response-Protokolle - Dienstleister-AOCs - Audit-Berichte

---

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 14

Anhang: Nachweisregister

Dokument-ID: PCI-0700
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

14.1 1. Zweck

Dieses Dokument dient als zentrales Register aller Nachweise für die PCI-DSS-Compliance von AdminSend GmbH.

14.1.1 1.1 Verwendung

- **Audit-Vorbereitung:** Schneller Zugriff auf alle Nachweise
- **Compliance-Tracking:** Übersicht über Dokumentenstatus
- **Gap-Analyse:** Identifikation fehlender Nachweise

14.2 2. Nachweisregister nach Requirements

14.2.1 2.1 Requirement 1: Firewall und Netzwerksicherheit

Nachweis	Dokument	Speicherort	Letzte Aktualisierung	Status
Firewall-Konfiguration	PCI-0100	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Firewall-Regelwerk	Firewall-Rules.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]

Nachweis	Dokument	Speicherort	Letzte Aktualisierung	Status
Netzwerkdiagramm	Network-Diagram.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Quartalsweise Regel-Reviews	FW-Review-Q1-2026.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Change-Protokolle	Change-Log-2026.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]

14.2.2 2.2 Requirement 2: Sichere Konfigurationen

Nachweis	Dokument	Speicherort	Letzte Aktualisierung	Status
Hardening-Standards	Hardening-Guide.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Konfigurationsbaselines	Config-Baselines.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Vendor Default-Accounts	Default-Accounts.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
System-Inventar	Asset-Inventory.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]

14.2.3 2.3 Requirement 3: Schutz gespeicherter Karteninhaberdaten

Nachweis	Dokument	Speicherort	Letzte Aktualisierung	Status
Datenspeicherungsrichtlinie	Data-Retention-Policy.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Verschlüsselungsstandards	Encryption-Standards.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Key-Management-Verfahren	Key-Management.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
CHD-Inventar	CHD-Inventory.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]

Nachweis	Dokument	Speicherort	Letzte Aktualisierung	Status
Datenflussdiagramme	Data-Flow-Diagrams.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]

14.2.4 2.4 Requirement 4: Verschlüsselung bei Übertragung

Nachweis	Dokument	Speicherort	Letzte Aktualisierung	Status
Verschlüsselungsrichtlinie	Transmission-Encryption.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
TLS-Konfigurationen	TLS-Config.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Zertifikatsverwaltung	Certificate-Management.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Scan-Berichte (TLS)	TLS-Scan-Report.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]

14.2.5 2.5 Requirement 5: Malware-Schutz

Nachweis	Dokument	Speicherort	Letzte Aktualisierung	Status
Antivirus-Richtlinie	Antivirus-Policy.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
AV-Konfiguration	AV-Configuration.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
AV-Update-Protokolle	AV-Update-Logs.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Malware-Detektionen	Malware-Incidents.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]

14.2.6 2.6 Requirement 6: Sichere Systeme und Anwendungen

Nachweis	Dokument	Speicherort	Letzte Aktualisierung	Status
Patch-Management-Richtlinie	Patch-Management.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]

Nachweis	Dokument	Speicherort	Letzte Aktualisierung	Status
Patch-Protokolle	Patch-Logs-2026.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Vulnerability-Scan-Berichte	Vuln-Scan-Q1-2026.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Secure SDLC-Richtlinie	Secure-SDLC.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Code-Review-Berichte	Code-Review-2026.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Change-Management-Protokolle	Change-Management-2026.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]

14.2.7 2.7 Requirement 7: Zugriffskontrolle

Nachweis	Dokument	Speicherort	Letzte Aktualisierung	Status
Zugriffskontrollrichtlinie	PCI-0400	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Berechtigungsmatrix	Access-Matrix.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Zugriffsanträge	Access-Requests-2026.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Quartalsweise Access-Reviews	Access-Review-Q1-2026.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Rezertifizierungsnachweise	Recertification-2026.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]

14.2.8 2.8 Requirement 8: Identifikation und Authentifizierung

Nachweis	Dokument	Speicherort	Letzte Aktualisierung	Status
Authentifizierungsrichtlinie	PCI-0410	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]

Nachweis	Dokument	Speicherort	Letzte Aktualisierung	Status
Passwortrichtlinie	Password-Policy.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
MFA-Konfiguration	MFA-Configuration.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Benutzer-Inventar	User-Inventory.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Account-Management-Protokolle	Account-Management-2026.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]

14.2.9 2.9 Requirement 9: Physische Sicherheit

Nachweis	Dokument	Speicherort	Letzte Aktualisierung	Status
Physische Sicherheitsrichtlinie	PCI-0420	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Zutrittskontroll-Protokolle	Access-Control-Logs-2026.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Besucherprotokolle	Visitor-Logs-2026.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
POS-Inspektionsprotokolle	POS-Inspection-Q1-2026.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Medien-Vernichtungszertifikate	Media-Destruction-2026.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Videoüberwachungs-Protokolle	CCTV-Logs-2026.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]

14.2.10 2.10 Requirement 10: Logging und Monitoring

Nachweis	Dokument	Speicherort	Letzte Aktualisierung	Status
Logging-Richtlinie	PCI-0500	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]

Nachweis	Dokument	Speicherort	Letzte Aktualisierung	Status
SIEM-Konfiguration	SIEM-Configuration.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Log-Review-Protokolle	Log-Review-2026.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Alerting-Regeln	Alerting-Rules.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Incident-Response-Protokolle	Incident-Response-2026.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
NTP-Konfiguration	NTP-Configuration.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]

14.2.11 2.11 Requirement 11: Sicherheitstests

Nachweis	Dokument	Speicherort	Letzte Aktualisierung	Status
Sicherheitstest-Richtlinie	PCI-0510	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
ASV-Scan-Berichte	ASV-Scan-Q1-2026.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Interne Scan-Berichte	Internal-Scan-Q1-2026.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Penetrationstest-Berichte	Pentest-2026.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Segmentierungstest-Berichte	Segmentation-Test-2026.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
FIM-Konfiguration	FIM-Configuration.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
IDS/IPS-Konfiguration	IDS-IPS-Configuration.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Wireless-Scan-Berichte	Wireless-Scan-Q1-2026.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]

14.2.12 2.12 Requirement 12: Informationssicherheitsrichtlinie

Nachweis	Dokument	Speicherort	Letzte Aktualisierung	Status
Informationssicherheitsrichtlinie	PCI-0600	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Risikoanalyse-Berichte	Risk-Assessment-2026.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Schulungsnachweise	Training-Records-2026.xlsx	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Incident Response Plan	Incident-Response-Plan.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Dienstleister-AOCs	Vendor-AOCs-2026.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Dienstleister-Verträge	Vendor-Contracts.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
Interne Audit-Berichte	Internal-Audit-2026.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]
QSA-Assessment-Berichte	QSA-Report-2026.pdf	[TODO: Pfad]	[TODO: Datum]	[TODO: Aktuell/Veraltet]

14.3 3. Dokumentenstatus-Tracking

14.3.1 3.1 Dokumenten-Lifecycle

Status	Beschreibung	Nächste Aktion
Aktuell	Dokument ist aktuell und gültig	Jährlicher Review
Review fällig	Jährlicher Review steht an	Review durchführen
Veraltet	Dokument ist nicht mehr aktuell	Aktualisierung erforderlich
In Bearbeitung	Dokument wird gerade aktualisiert	Fertigstellung
Fehlend	Dokument existiert nicht	Erstellung erforderlich

14.3.2 3.2 Review-Zeitplan

Dokument-Typ	Review-Frequenz	Verantwortlich
Richtlinien	Jährlich	CISO

Dokument-Typ	Review-Frequenz	Verantwortlich
Verfahren	Jährlich	IT Security Manager
Konfigurationen	Quartalsweise	IT Operations
Scan-Berichte	Quartalsweise	IT Security
Audit-Berichte	Nach jedem Audit	PCI Manager

14.4 4. Audit-Vorbereitung

14.4.1 4.1 Checkliste für QSA-Assessment

- ☐ Alle Nachweise aktuell
- ☐ Alle Dokumente zugänglich
- ☐ Alle Reviews durchgeführt
- ☐ Alle Scans aktuell (< 90 Tage)
- ☐ Alle Schulungen dokumentiert
- ☐ Alle Incidents dokumentiert
- ☐ Alle Dienstleister-AOCs aktuell
- ☐ Alle Change-Protokolle vollständig

14.4.2 4.2 Fehlende Nachweise

Requirement	Fehlender Nachweis	Priorität	Fälligkeitsdatum	Verantwortlich
[TODO]	[TODO]	[TODO: Hoch/Mittel/Niedrig]	[TODO: Datum]	[TODO: Name]

14.5 5. Dokumenten-Archivierung

14.5.1 5.1 Archivierungsrichtlinie

Aufbewahrungsfristen: - Richtlinien: Aktuell + 3 Jahre - Audit-Berichte: 3 Jahre - Scan-Berichte: 1 Jahr - Logs: 1 Jahr - Schulungsnachweise: 3 Jahre - Incident-Berichte: 3 Jahre

Archivierungsort: [TODO: Speicherort für archivierte Dokumente]

14.5.2 5.2 Archivierte Dokumente

Dokument	Archivierungsdatum	Aufbewahrungsfrist bis	Speicherort
[TODO]	[TODO: Datum]	[TODO: Datum]	[TODO: Pfad]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 15

Anhang: Glossar und Abkürzungen

Dokument-ID: PCI-0710
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Genehmigt durch: CIO
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}

15.1 1. Zweck

Dieses Dokument definiert alle Begriffe und Abkürzungen, die in der PCI-DSS-Dokumentation von AdminSend GmbH verwendet werden.

15.2 2. PCI-DSS-Begriffe

15.2.1 A

Acquiring Bank (Acquirer) - Bank, die Zahlungskarten-Transaktionen für Händler verarbeitet - Verantwortlich für PCI-DSS-Compliance des Händlers

AOC (Attestation of Compliance) - Bestätigung der PCI-DSS-Compliance - Ausgestellt von QSA oder durch Self-Assessment

ASV (Approved Scanning Vendor) - Von PCI SSC zugelassener Anbieter für Vulnerability Scans - Führt quartalsweise externe Scans durch

Authentication - Prozess der Identitätsverifizierung - Typischerweise durch Passwort, Token oder Biometrie

Authorization - Prozess der Berechtigungsprüfung - Bestimmt, welche Aktionen ein Benutzer durchführen darf

15.2.2 C

Cardholder Data (CHD) - Karteninhaberdaten - Umfasst PAN, Karteninhabername, Ablaufdatum, Service Code

Cardholder Data Environment (CDE) - Umgebung, die Karteninhaberdaten speichert, verarbeitet oder überträgt - Umfasst Systeme, Netzwerke, Personen und Prozesse

CDE Segmentation - Netzwerksegmentierung zur Isolation des CDE - Reduziert Compliance-Scope

CVV/CVC/CVV2/CVC2 - Card Verification Value/Code - 3-4-stelliger Sicherheitscode - Darf NICHT nach Autorisierung gespeichert werden

15.2.3 D

Data Retention - Datenspeicherungsrichtlinie - Definiert, wie lange Daten gespeichert werden dürfen

Default Account - Herstellerseitig vorkonfigurierter Account - Muss deaktiviert oder Passwort geändert werden

DMZ (Demilitarized Zone) - Netzwerksegment zwischen Internet und internem Netzwerk - Für öffentlich zugängliche Dienste

15.2.4 E

Encryption - Verschlüsselung von Daten - Erforderlich für gespeicherte und übertragene CHD

Encryption Key - Schlüssel zur Ver- und Entschlüsselung - Muss sicher gespeichert und verwaltet werden

15.2.5 F

FIM (File Integrity Monitoring) - Dateiintegritätsüberwachung - Erkennt unbefugte Änderungen an kritischen Dateien

Firewall - Netzwerksicherheitsgerät - Kontrolliert Datenverkehr zwischen Netzwerksegmenten

15.2.6 H

Hashing - Einweg-Verschlüsselung - Für Passwort-Speicherung

Hardening - Härtung von Systemen - Entfernung unnötiger Dienste und Funktionen

15.2.7 I

IDS/IPS (Intrusion Detection/Prevention System) - System zur Erkennung und Verhinderung von Angriffen - Erforderlich an allen CDE-Grenzen

Incident Response - Reaktion auf Sicherheitsvorfälle - Strukturierter Prozess zur Behandlung von Incidents

15.2.8 K

Key Management - Verwaltung kryptografischer Schlüssel - Umfasst Generierung, Speicherung, Rotation, Vernichtung

15.2.9 L

Least Privilege - Prinzip der minimalen Berechtigungen - Benutzer erhalten nur erforderliche Zugriffsrechte

Logging - Protokollierung von Ereignissen - Erforderlich für alle Zugriffe auf CDE und CHD

15.2.10 M

Malware - Schadsoftware - Viren, Trojaner, Ransomware, etc.

Merchant - Händler, der Zahlungskarten akzeptiert - Unterliegt PCI-DSS-Compliance

MFA (Multi-Factor Authentication) - Mehr-Faktor-Authentifizierung - Erforderlich für CDE-Zugriffe

15.2.11 N

Need-to-Know - Prinzip des berechtigten Wissens - Zugriff nur bei geschäftlicher Notwendigkeit

Network Segmentation - Netzwerksegmentierung - Trennung von CDE und Corporate-Netzwerk

NTP (Network Time Protocol) - Protokoll zur Zeitsynchronisation - Erforderlich für korrekte Zeitstempel in Logs

15.2.12 P

PA-DSS (Payment Application Data Security Standard) - Sicherheitsstandard für Zahlungsanwendungen - Ergänzt PCI-DSS

PAN (Primary Account Number) - Primäre Kontonummer - 13-19-stellige Kartennummer - Kernstück der Karteninhaberdaten

Penetration Test - Sicherheitstest durch simulierte Angriffe - Jährlich erforderlich

PCI DSS (Payment Card Industry Data Security Standard) - Sicherheitsstandard für Zahlungskartenindustrie - Definiert Anforderungen zum Schutz von Karteninhaberdaten

PCI SSC (Payment Card Industry Security Standards Council) - Organisation, die PCI-DSS entwickelt und verwaltet

POS (Point of Sale) - Verkaufsstelle - Terminal zur Karteneingabe

15.2.13 Q

QSA (Qualified Security Assessor) - Qualifizierter Sicherheitsprüfer - Führt PCI-DSS-Assessments durch

15.2.14 R

RBAC (Role-Based Access Control) - Rollenbasierte Zugriffskontrolle - Berechtigungen basierend auf Rollen

Risk Assessment - Risikoanalyse - Jährlich erforderlich

ROC (Report on Compliance) - Compliance-Bericht - Erstellt von QSA nach Assessment

15.2.15 S

SAD (Sensitive Authentication Data) - Sensitive Authentifizierungsdaten - Full Track Data, CVV, PIN - Darf NICHT nach Autorisierung gespeichert werden

SAQ (Self-Assessment Questionnaire) - Selbstbewertungsfragebogen - Für kleinere Händler ohne QSA-Assessment

Scope - Geltungsbereich der PCI-DSS-Compliance - Alle Systeme, die CHD speichern, verarbeiten oder übertragen

Segmentation - Siehe Network Segmentation

Service Provider - Dienstleister, der CHD im Auftrag verarbeitet - Unterliegt PCI-DSS-Compliance

SIEM (Security Information and Event Management) - System zur zentralen Log-Verwaltung und -Analyse

Strong Cryptography - Starke Verschlüsselung - Mindestens AES-128, RSA-2048

15.2.16 T

Tokenization - Ersetzung von PAN durch Token - Reduziert Compliance-Scope

TLS (Transport Layer Security) - Verschlüsselungsprotokoll für Datenübertragung - Mindestens TLS 1.2 erforderlich

Track Data - Magnetstreifendaten - Track 1 und Track 2 - Darf NICHT nach Autorisierung gespeichert werden

15.2.17 V

Vulnerability - Schwachstelle in System oder Anwendung - Muss identifiziert und behoben werden

Vulnerability Scan - Schwachstellen-Scan - Quartalsweise erforderlich (extern und intern)

15.2.18 W

WAF (Web Application Firewall) - Firewall für Webanwendungen - Schutz vor OWASP Top 10

WORM (Write Once Read Many) - Speicher, der nur einmal beschrieben werden kann - Für Log-Speicherung zur Integritätssicherung

15.3 3. Abkürzungen

Abkürzung	Bedeutung
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
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
DSGVO	Datenschutz-Grundverordnung (GDPR)
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

Abkürzung	Bedeutung
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
ROC	Report on Compliance
RPO	Recovery Point Objective
RSA	Rivest-Shamir-Adleman (Verschlüsselungsalgorithmus)
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 (veraltet, durch TLS ersetzt)
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. Organisationsspezifische Begriffe

[TODO: Fügen Sie hier organisationsspezifische Begriffe und Abkürzungen hinzu]

Begriff/Abkürzung	Bedeutung
[TODO]	[TODO]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage