Contents

Chapter 1

NIST 800-53 Security and Privacy Controls Handbuch

Dokument-Metadaten

- **Erstellt am:** 2026-02-10
- **Autor:** Andreas Huemmer [andreas.huemmer@adminsend.de]
- **Version:** 0.0.5
- **Typ:** NIST 800-53-Handbuch

---

ewpage

Chapter 2

Systemkategorisierung

Dokument-ID: NIST-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 beschreibt die Kategorisierung des Informationssystems {{ meta.nist.system_name }} gemäß FIPS 199 und NIST SP 800-60.

2.1.1 1.1 Ziele

- **FIPS 199-Konformität:** Kategorisierung nach Sicherheitszielen (Vertraulichkeit, Integrität, Verfügbarkeit)
- **Risikobewertung:** Bestimmung der potenziellen Auswirkungen bei Sicherheitsverletzungen
- **Baseline-Auswahl:** Grundlage für die Auswahl der Sicherheitskontrollen
- **Compliance:** Erfüllung bundesweiter Anforderungen

2.1.2 1.2 Referenzen

- **FIPS 199:** Standards for Security Categorization of Federal Information and Information Systems
- **NIST SP 800-60 Vol. 1 Rev. 1:** Guide for Mapping Types of Information and Information Systems to Security Categories
- **NIST SP 800-60 Vol. 2 Rev. 1:** Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories
- **NIST SP 800-53 Rev. 5:** Security and Privacy Controls for Information Systems and Organizations

2.2 2. Systeminformationen

2.2.1 2.1 Systemidentifikation

Systemname: {{ meta.nist.system_name }}
System-ID: {{ meta.nist.system_id }}
System Owner: [TODO: Name] ([TODO: E-Mail])
Authorizing Official (AO): {{ meta.roles.ao.name }} ({{ meta.roles.ao.email }})
Information System Security Officer (ISSO): {{ meta.roles.isso.name }} ({{ meta.roles.isso.email }})

2.2.2 2.2 Systembeschreibung

Zweck: [TODO: Beschreibung des Systemzwecks]

Funktionen: - [TODO: Hauptfunktion 1] - [TODO: Hauptfunktion 2] - [TODO: Hauptfunktion 3]

Benutzer: - **Interne Benutzer:** [TODO: Anzahl und Rollen] - **Externe Benutzer:** [TODO: Anzahl und Rollen] - **Privilegierte Benutzer:** [TODO: Anzahl und Rollen]

2.2.3 2.3 Informationstypen

Informationstyp	Beschreibung	Quelle (NIST 800-60)
[TODO: Typ 1]	[TODO: Beschreibung]	[TODO: C.2.x.x]
[TODO: Typ 2]	[TODO: Beschreibung]	[TODO: C.3.x.x]
[TODO: Typ 3]	[TODO: Beschreibung]	[TODO: C.4.x.x]

2.3 3. FIPS 199 Kategorisierung

2.3.1 3.1 Sicherheitsziele und Impact Levels

Die Kategorisierung erfolgt nach den drei Sicherheitszielen:

2.3.1.1 3.1.1 Vertraulichkeit (Confidentiality)

Definition: Schutz vor unbefugter Offenlegung von Informationen.

Impact Level: [TODO: Low / Moderate / High]

Begründung: [TODO: Beschreiben Sie die potenziellen Auswirkungen einer unbefugten Offenlegung]

Beispiele für Auswirkungen: - **Low:** Begrenzte negative Auswirkungen auf Organisationsoperationen, -vermögen oder -personen - **Moderate:** Ernsthafte negative Auswirkungen - **High:** Schwerwiegende oder katastrophale negative Auswirkungen

Spezifische Auswirkungen für dieses System: - [TODO: Auswirkung 1] - [TODO: Auswirkung 2] - [TODO: Auswirkung 3]

2.3.1.2 3.1.2 Integrität (Integrity)

Definition: Schutz vor unbefugter Änderung oder Zerstörung von Informationen.

Impact Level: [TODO: Low / Moderate / High]

Begründung: [TODO: Beschreiben Sie die potenziellen Auswirkungen einer unbefugten Änderung]

Spezifische Auswirkungen für dieses System: - [TODO: Auswirkung 1] - [TODO: Auswirkung 2] - [TODO: Auswirkung 3]

2.3.1.3 3.1.3 Verfügbarkeit (Availability)

Definition: Sicherstellung des rechtzeitigen und zuverlässigen Zugriffs auf Informationen.

Impact Level: [TODO: Low / Moderate / High]

Begründung: [TODO: Beschreiben Sie die potenziellen Auswirkungen eines Verfügbarkeitsverlusts]

Spezifische Auswirkungen für dieses System: - [TODO: Auswirkung 1] - [TODO: Auswirkung 2] - [TODO: Auswirkung 3]

2.3.2 3.2 Gesamtkategorisierung

FIPS 199 Security Category:

```
SC {{ meta.nist.system_name }} = {(confidentiality, [TODO: impact]), (integrity, [TODO: impact]
```

Beispiel:

```
SC Information System = {(confidentiality, MODERATE), (integrity, MODERATE), (availability, LOW
```

Overall System Categorization: [TODO: Low / Moderate / High]

> **Hinweis:** Die Gesamtkategorisierung entspricht dem höchsten Impact Level der drei Sicherheitsziele (High-Water Mark).

2.4 4. Kategorisierung nach Informationstypen

2.4.1 4.1 Informationstyp-Analyse

Für jeden Informationstyp wird die Kategorisierung gemäß NIST SP 800-60 durchgeführt:

2.4.1.1 Informationstyp 1: [TODO: Name]

Beschreibung: [TODO: Beschreibung des Informationstyps]

NIST 800-60 Referenz: [TODO: C.x.x.x]

Sicherheitsziel	Provisional Impact	Angepasster Impact	Begründung
Vertraulichkeit	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: Begründung]
Integrität	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: Begründung]

Sicherheitsziel	Provisional Impact	Angepasster Impact	Begründung
Verfügbarkeit	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: Begründung]

2.4.1.2 Informationstyp 2: [TODO: Name]

Beschreibung: [TODO: Beschreibung des Informationstyps]

NIST 800-60 Referenz: [TODO: C.x.x.x]

Sicherheitsziel	Provisional Impact	Angepasster Impact	Begründung
Vertraulichkeit	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: Begründung]
Integrität	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: Begründung]
Verfügbarkeit	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: Begründung]

2.4.2 4.2 Aggregierte Kategorisierung

Methode: High-Water Mark (höchster Impact Level über alle Informationstypen)

Sicherheitsziel	Aggregierter Impact
Vertraulichkeit	[TODO: Low / Moderate / High]
Integrität	[TODO: Low / Moderate / High]
Verfügbarkeit	[TODO: Low / Moderate / High]

2.5 5. Baseline-Auswahl

2.5.1 5.1 NIST 800-53 Baseline

Basierend auf der Gesamtkategorisierung wird folgende Baseline ausgewählt:

Ausgewählte Baseline: [TODO: Low / Moderate / High Baseline]

Baseline-Kontrollen: - **Low Baseline:** NIST SP 800-53B, Appendix A - **Moderate Baseline:** NIST SP 800-53B, Appendix B - **High Baseline:** NIST SP 800-53B, Appendix C

2.5.2 5.2 Tailoring

Tailoring-Aktivitäten: - **Hinzugefügte Kontrollen:** [TODO: Liste zusätzlicher Kontrollen] - **Entfernte Kontrollen:** [TODO: Liste entfernter Kontrollen mit Begründung] - **Angepasste Kontrollen:** [TODO: Liste angepasster Kontrollen]

2.6 6. Kategorisierungsprozess

2.6.1 6.1 Prozessschritte

1. **Systemidentifikation:** Identifikation des zu kategorisierenden Systems
2. **Informationstyp-Identifikation:** Identifikation aller verarbeiteten Informationstypen
3. **Provisional Impact:** Bestimmung der provisorischen Impact Levels gemäß NIST 800-60
4. **Impact-Anpassung:** Anpassung basierend auf organisationsspezifischen Faktoren
5. **Aggregation:** Aggregation zu Gesamtkategorisierung
6. **Dokumentation:** Dokumentation der Kategorisierung
7. **Genehmigung:** Genehmigung durch Authorizing Official

2.6.2 6.2 Beteiligte Rollen

Rolle	Name	Verantwortlichkeit
System Owner	[TODO: Name]	Systemverantwortung
Information Owner	[TODO: Name]	Informationsverantwortung
ISSO	{{ meta.roles.isso.name }}	Sicherheitsbewertung
ISSM	{{ meta.roles.issm.name }}	Sicherheitsmanagement
Authorizing Official (AO)	{{ meta.roles.ao.name }}	Genehmigung

2.6.3 6.3 Kategorisierungsdatum

Initiale Kategorisierung: [TODO: Datum]
Letzte Überprüfung: [TODO: Datum]
Nächste Überprüfung: [TODO: Datum]

2.7 7. Auswirkungsanalyse

2.7.1 7.1 Vertraulichkeitsverlust

Potenzielle Auswirkungen bei unbefugter Offenlegung:

Bereich	Auswirkung	Schweregrad
Organisationsoperationen	[TODO: Beschreibung]	[TODO: L/M/H]
Organisationsvermögen	[TODO: Beschreibung]	[TODO: L/M/H]
Personen	[TODO: Beschreibung]	[TODO: L/M/H]
Nationale Sicherheit	[TODO: Beschreibung]	[TODO: L/M/H]

2.7.2 7.2 Integritätsverlust

Potenzielle Auswirkungen bei unbefugter Änderung:

Bereich	Auswirkung	Schweregrad
Organisationsoperationen	[TODO: Beschreibung]	[TODO: L/M/H]
Organisationsvermögen	[TODO: Beschreibung]	[TODO: L/M/H]

Bereich	Auswirkung	Schweregrad
Personen	[TODO: Beschreibung]	[TODO: L/M/H]
Nationale Sicherheit	[TODO: Beschreibung]	[TODO: L/M/H]

2.7.3 7.3 Verfügbarkeitsverlust

Potenzielle Auswirkungen bei Systemausfall:

Bereich	Auswirkung	Schweregrad
Organisationsoperationen	[TODO: Beschreibung]	[TODO: L/M/H]
Organisationsvermögen	[TODO: Beschreibung]	[TODO: L/M/H]
Personen	[TODO: Beschreibung]	[TODO: L/M/H]
Nationale Sicherheit	[TODO: Beschreibung]	[TODO: L/M/H]

2.8 8. Genehmigung

2.8.1 8.1 Kategorisierungsgenehmigung

Kategorisierung genehmigt durch:

Name: {{ meta.roles.ao.name }}
Titel: Authorizing Official (AO)
Datum: [TODO: Datum]
Unterschrift: [TODO: Unterschrift oder elektronische Genehmigung]

2.8.2 8.2 Überprüfungsintervall

Überprüfungsfrequenz: [TODO: Jährlich / Bei signifikanten Änderungen]

Auslöser für Neukategorisierung: - Signifikante Änderungen am System - Neue Informationstypen - Änderungen in der Bedrohungslandschaft - Organisatorische Änderungen - Gesetzliche oder regulatorische Änderungen

2.9 9. Anhang

2.9.1 9.1 FIPS 199 Impact Level Definitionen

Low Impact: > The potential impact is LOW if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

Moderate Impact: > The potential impact is MODERATE if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

High Impact: > The potential impact is HIGH if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

2.9.2 9.2 Kategorisierungsmatrix

Informationstyp	Vertraulichkeit	Integrität	Verfügbarkeit	Gesamt
[TODO: Typ 1]	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: L/M/H]
[TODO: Typ 2]	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: L/M/H]
[TODO: Typ 3]	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: L/M/H]
System Gesamt	**[TODO: L/M/H]**	**[TODO: L/M/H]**	**[TODO: L/M/H]**	**[TODO: L/M/H]**

Dokumenthistorie:

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

ewpage

Chapter 3

Geltungsbereich und Systemgrenzen

Dokument-ID: NIST-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 definiert den Geltungsbereich und die Autorisierungsgrenzen des Informationssystems {{ meta.nist.system_name }}.

3.1.1 1.1 Ziele

- **Scope-Definition:** Klare Abgrenzung des Systems
- **Autorisierungsgrenze:** Definition der Autorisierungsgrenze
- **Komponenten-Identifikation:** Identifikation aller Systemkomponenten
- **Schnittstellen:** Dokumentation externer Schnittstellen

3.1.2 1.2 Referenzen

- **NIST SP 800-37 Rev. 2:** Risk Management Framework for Information Systems and Organizations
- **NIST SP 800-53 Rev. 5:** Security and Privacy Controls
- **NIST SP 800-18 Rev. 1:** Guide for Developing Security Plans

3.2 2. Systemidentifikation

3.2.1 2.1 Systeminformationen

Systemname: {{ meta.nist.system_name }}
System-ID: {{ meta.nist.system_id }}
FIPS 199 Kategorisierung: [TODO: Low / Moderate / High]
System Owner: [TODO: Name]
Authorizing Official (AO): {{ meta.roles.ao.name }}

3.2.2 2.2 Systembeschreibung

Zweck: [TODO: Beschreibung des Systemzwecks]

Hauptfunktionen: - [TODO: Funktion 1] - [TODO: Funktion 2] - [TODO: Funktion 3]

Geschäftsprozesse: - [TODO: Prozess 1] - [TODO: Prozess 2]

3.3 3. Autorisierungsgrenze

3.3.1 3.1 Definition der Autorisierungsgrenze

Die Autorisierungsgrenze umfasst alle Komponenten, die unter einer einzigen Autorisierungsentscheidung fallen.

Autorisierungsgrenze: [TODO: Beschreibung der Grenze]

Eingeschlossene Komponenten: - [TODO: Komponente 1] - [TODO: Komponente 2] - [TODO: Komponente 3]

Ausgeschlossene Komponenten: - [TODO: Komponente 1 - Begründung] - [TODO: Komponente 2 - Begründung]

3.3.2 3.2 Netzwerkdiagramm

[TODO: Fügen Sie Netzwerkdiagramm ein, das die Autorisierungsgrenze zeigt]

3.4 4. Systemkomponenten

3.4.1 4.1 Hardware-Komponenten

Komponente	Typ	Standort	Funktion	Kritikalität
[TODO: Server 1]	Server	[TODO: RZ1]	[TODO: Funktion]	[TODO: H/M/L]
[TODO: Firewall 1]	Netzwerk	[TODO: RZ1]	[TODO: Funktion]	[TODO: H/M/L]

3.4.2 4.2 Software-Komponenten

Komponente	Version	Hersteller	Funktion	Lizenz
[TODO: OS]	[TODO: Version]	[TODO: Vendor]	Betriebssystem	[TODO: Lizenz]
[TODO: App]	[TODO: Version]	[TODO: Vendor]	Anwendung	[TODO: Lizenz]

3.4.3 4.3 Datenkomponenten

Datentyp	Klassifizierung	Speicherort	Retention	Backup
[TODO: Daten 1]	[TODO: Klassifizierung]	[TODO: Ort]	[TODO: Zeit]	[TODO: Ja/Nein]

3.5 5. Externe Schnittstellen

3.5.1 5.1 Systemverbindungen

Verbundenes System	Verbindungstyp	Protokoll	Zweck	Autorisierung
[TODO: System 1]	[TODO: Typ]	[TODO: Protokoll]	[TODO: Zweck]	[TODO: ATO-Nummer]

3.5.2 5.2 Datenflüsse

Eingehende Datenflüsse: - [TODO: Quelle → Ziel: Beschreibung]

Ausgehende Datenflüsse: - [TODO: Quelle → Ziel: Beschreibung]

3.6 6. Standorte

3.6.1 6.1 Physische Standorte

Standort-ID	Standortname	Adresse	Komponenten	Sicherheitslevel
[TODO: LOC-01]	[TODO: Name]	[TODO: Adresse]	[TODO: Liste]	[TODO: Level]

3.7 7. Personal

3.7.1 7.1 Benutzerrollen

Rolle	Anzahl	Zugriffslevel	Begründung
[TODO: Admin]	[TODO: Anzahl]	Privilegiert	Administration
[TODO: User]	[TODO: Anzahl]	Standard	Normale Nutzung

3.7.2 7.2 Externe Benutzer

Benutzergruppe	Organisation	Zugriffsmethode	Zweck
[TODO: Partner]	[TODO: Org]	[TODO: VPN]	[TODO: Zweck]

3.8 8. Genehmigung

Genehmigt durch: {{ meta.roles.ao.name }}
Datum: [TODO: Datum]

Dokumenthistorie:

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

ewpage

Chapter 4

Rollen und Verantwortlichkeiten

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

4.1 1. Zweck

Dieses Dokument definiert die Rollen und Verantwortlichkeiten für das Risk Management Framework (RMF) und die Sicherheit des Systems {{ meta.nist.system_name }}.

4.2 2. RMF-Rollen

4.2.1 2.1 Authorizing Official (AO)

Name: {{ meta.roles.ao.name }}
E-Mail: {{ meta.roles.ao.email }}

Verantwortlichkeiten: - Autorisierungsentscheidung für das System - Akzeptanz des Sicherheitsrisikos - Genehmigung des System Security Plan (SSP) - Überwachung des Sicherheitsstatus

4.2.2 2.2 Information System Security Officer (ISSO)

Name: {{ meta.roles.isso.name }}
E-Mail: {{ meta.roles.isso.email }}

Verantwortlichkeiten: - Tägliche Sicherheitsoperationen - Implementierung von Sicherheitskontrollen - Incident Response - Sicherheitsüberwachung

4.2.3 2.3 Information System Security Manager (ISSM)

Name: {{ meta.roles.issm.name }}
E-Mail: {{ meta.roles.issm.email }}

Verantwortlichkeiten: - Sicherheitsprogramm-Management - Richtlinienentwicklung - Compliance-Überwachung - Risikomanagement

4.2.4 2.4 System Owner

Name: [TODO: Name]
E-Mail: [TODO: E-Mail]

Verantwortlichkeiten: - Gesamtverantwortung für das System - Geschäftsprozess-Verantwortung - Budget und Ressourcen - Systemänderungen genehmigen

4.2.5 2.5 Security Control Assessor (SCA)

Name: [TODO: Name/Firma]
E-Mail: [TODO: E-Mail]

Verantwortlichkeiten: - Unabhängige Bewertung der Sicherheitskontrollen - Erstellung des Security Assessment Report (SAR) - Identifikation von Schwachstellen - Empfehlungen für Verbesserungen

4.3 3. RACI-Matrix

Aktivität	AO	ISSO	ISSM	System Owner	SCA
System Categorization	A	C	R	C	I
Control Selection	A	R	C	C	I
Control Implementation	I	R	C	A	I
Control Assessment	I	C	C	I	R
Authorization Decision	R	C	C	C	I
Continuous Monitoring	A	R	C	C	I

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

---

Dokumenthistorie:

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

ewpage

Chapter 5

Risk Management Framework (RMF)

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

5.1 1. Zweck

Dieses Dokument beschreibt die Anwendung des NIST Risk Management Framework (RMF) auf das System {{ meta.nist.system_name }}.

5.2 2. RMF-Übersicht

5.2.1 2.1 RMF-Schritte

Das RMF besteht aus sieben Schritten:

1. **Prepare:** Vorbereitung auf RMF-Aktivitäten
2. **Categorize:** Systemkategorisierung nach FIPS 199
3. **Select:** Auswahl der Sicherheitskontrollen
4. **Implement:** Implementierung der Kontrollen
5. **Assess:** Bewertung der Kontrollen
6. **Authorize:** Autorisierungsentscheidung
7. **Monitor:** Kontinuierliche Überwachung

5.3 3. RMF-Schritt 1: Prepare

Status: [TODO: Not Started / In Progress / Complete]

Aktivitäten: - Organisationsweite Vorbereitung - Systemebene Vorbereitung - Identifikation von Common Controls

Ergebnisse: - [TODO: Liste der Ergebnisse]

5.4 4. RMF-Schritt 2: Categorize

Status: [TODO: Not Started / In Progress / Complete]
FIPS 199 Kategorisierung: [TODO: Low / Moderate / High]

Dokument: Siehe NIST-0010 Systemkategorisierung

Genehmigt durch: {{ meta.roles.ao.name }}
Datum: [TODO: Datum]

5.5 5. RMF-Schritt 3: Select

Status: [TODO: Not Started / In Progress / Complete]
Baseline: [TODO: Low / Moderate / High Baseline]

Ausgewählte Kontrollen: - Baseline-Kontrollen: [TODO: Anzahl] - Zusätzliche Kontrollen: [TODO: Anzahl] - Gesamt: [TODO: Anzahl]

Tailoring: - Hinzugefügte Kontrollen: [TODO: Liste] - Entfernte Kontrollen: [TODO: Liste]

5.6 6. RMF-Schritt 4: Implement

Status: [TODO: Not Started / In Progress / Complete]

Implementierungsstatus: - Implementiert: [TODO: Anzahl / Prozent] - In Arbeit: [TODO: Anzahl / Prozent] - Geplant: [TODO: Anzahl / Prozent]

Dokument: Siehe NIST-0021 System Security Plan (SSP)

5.7 7. RMF-Schritt 5: Assess

Status: [TODO: Not Started / In Progress / Complete]

Assessment-Informationen: - Assessor: [TODO: Name/Firma] - Assessment-Datum: [TODO: Datum] - Assessment-Methoden: [TODO: Interview, Examine, Test]

Ergebnisse: - Erfüllte Kontrollen: [TODO: Anzahl / Prozent] - Teilweise erfüllte Kontrollen: [TODO: Anzahl / Prozent] - Nicht erfüllte Kontrollen: [TODO: Anzahl / Prozent]

Dokument: Siehe NIST-0810 Security Assessment Report (SAR)

5.8 8. RMF-Schritt 6: Authorize

Status: [TODO: Not Started / In Progress / Complete]

Authorization to Operate (ATO): - ATO-Status: [TODO: Granted / Denied / Conditional] - ATO-Datum: [TODO: Datum] - ATO-Gültigkeit: [TODO: 3 Jahre] - Nächste Reauthorization: [TODO: Datum]

Authorizing Official: {{ meta.roles.ao.name }}

Risikobewertung: - Gesamtrisiko: [TODO: Low / Moderate / High] - Akzeptiertes Risiko: [TODO: Beschreibung]

Dokument: Authorization Decision Document

5.9 9. RMF-Schritt 7: Monitor

Status: [TODO: Not Started / In Progress / Complete]

Continuous Monitoring: - Monitoring-Strategie: Siehe NIST-0050 - Monitoring-Frequenz: [TODO: Kontinuierlich / Monatlich / Quartalsweise] - Reporting: [TODO: Monatlich an AO]

Aktivitäten: - Sicherheitsstatusüberwachung - Änderungsmanagement - Compliance-Überprüfung - Incident Response

5.10 10. Zeitplan

RMF-Schritt	Geplanter Start	Geplantes Ende	Tatsächliches Ende	Status
Prepare	[TODO: Datum]	[TODO: Datum]	[TODO: Datum]	[TODO: Status]
Categorize	[TODO: Datum]	[TODO: Datum]	[TODO: Datum]	[TODO: Status]
Select	[TODO: Datum]	[TODO: Datum]	[TODO: Datum]	[TODO: Status]
Implement	[TODO: Datum]	[TODO: Datum]	[TODO: Datum]	[TODO: Status]
Assess	[TODO: Datum]	[TODO: Datum]	[TODO: Datum]	[TODO: Status]
Authorize	[TODO: Datum]	[TODO: Datum]	[TODO: Datum]	[TODO: Status]
Monitor	[TODO: Datum]	Kontinuierlich	N/A	[TODO: Status]

Dokumenthistorie:

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

ewpage

Chapter 6

Continuous Monitoring Strategy

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

6.1 1. Zweck

Dieses Dokument beschreibt die Strategie für die kontinuierliche Überwachung (Continuous Monitoring) des Systems {{ meta.nist.system_name }}.

6.2 2. Continuous Monitoring-Übersicht

6.2.1 2.1 Ziele

- **Sicherheitsstatus:** Kontinuierliche Überwachung des Sicherheitsstatus
- **Risikomanagement:** Frühzeitige Erkennung von Risiken
- **Compliance:** Sicherstellung der fortlaufenden Compliance
- **Incident Detection:** Schnelle Erkennung von Sicherheitsvorfällen

6.2.2 2.2 Referenzen

- **NIST SP 800-137:** Information Security Continuous Monitoring (ISCM)
- **NIST SP 800-53 Rev. 5:** CA-7 Continuous Monitoring

6.3 3. Monitoring-Strategie

6.3.1 3.1 Monitoring-Bereiche

Bereich	Beschreibung	Frequenz	Verantwortlich
Schwachstellen	Vulnerability Scanning	[TODO: Wöchentlich]	[TODO: ISSO]
Konfiguration	Configuration Compliance	[TODO: Täglich]	[TODO: ISSO]
Patches	Patch Status	[TODO: Wöchentlich]	[TODO: System Admin]
Zugriffe	Access Control Review	[TODO: Monatlich]	[TODO: ISSO]
Logs	Log Analysis	[TODO: Täglich]	[TODO: SOC]
Incidents	Incident Tracking	[TODO: Kontinuierlich]	[TODO: ISSO]

6.3.2 3.2 Monitoring-Tools

Tool	Zweck	Hersteller	Version
[TODO: Vulnerability Scanner]	Schwachstellenscans	[TODO: Vendor]	[TODO: Version]
[TODO: SIEM]	Log-Analyse	[TODO: Vendor]	[TODO: Version]
[TODO: Configuration Management]	Konfigurationsüberwachung	[TODO: Vendor]	[TODO: Version]

6.4 4. Metriken und Indikatoren

6.4.1 4.1 Sicherheitsmetriken

Metrik	Zielwert	Messmethode	Reporting-Frequenz
Kritische Schwachstellen	0	Vulnerability Scan	Wöchentlich
Patch-Compliance	> 95%	Patch Management System	Monatlich
Konfigurationsabweichungen	< 5%	Configuration Scanner	Wöchentlich
Incident Response Time	< 1 Stunde	Incident Tracking	Monatlich

6.4.2 4.2 Compliance-Indikatoren

Indikator	Beschreibung	Schwellenwert
Control Effectiveness	Prozentsatz wirksamer Kontrollen	> 90%

Indikator	Beschreibung	Schwellenwert
POA&M Completion	Abgeschlossene POA&M-Items	$> 80\%$
Assessment Findings	Offene Assessment-Findings	< 10

6.5 5. Reporting

6.5.1 5.1 Reporting-Struktur

Monatliche Berichte an AO: - Sicherheitsstatus-Zusammenfassung - Metriken und Trends - Neue Risiken und Schwachstellen - POA&M-Status - Empfehlungen

Quartalsweise Berichte: - Umfassende Sicherheitsbewertung - Compliance-Status - Änderungen am System - Reauthorization-Vorbereitung

6.5.2 5.2 Eskalation

Eskalationskriterien: - Kritische Schwachstellen - Sicherheitsvorfälle - Compliance-Verstöße - Signifikante Systemänderungen

Eskalationspfad: 1. ISSO → ISSM 2. ISSM → AO 3. AO → Senior Leadership

6.6 6. Änderungsmanagement

6.6.1 6.1 Änderungskategorien

Kategorie	Beschreibung	Genehmigung erforderlich
Signifikant	Auswirkung auf Autorisierung	AO
Moderat	Auswirkung auf Sicherheitskontrollen	ISSO
Minor	Keine Sicherheitsauswirkung	System Owner

6.6.2 6.2 Änderungsprozess

1. Änderungsantrag
2. Sicherheitsbewertung
3. Genehmigung
4. Implementierung
5. Verifikation
6. Dokumentation

6.7 7. Reauthorization

Reauthorization-Intervall: [TODO: 3 Jahre]
Nächste Reauthorization: [TODO: Datum]

Reauthorization-Auslöser: - Ablauf der ATO - Signifikante Systemänderungen - Neue Bedrohungen - Compliance-Anforderungen

Dokumenthistorie:

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

ewpage

Chapter 7

Access Control Policy

Dokument-ID: NIST-0100
Control Family: Access Control (AC)
Control: AC-1
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Letzte Aktualisierung: {{ meta.document.last_updated }}

7.1 1. Control Description

AC-1 Policy and Procedures

The organization develops, documents, and disseminates access control policy and procedures.

7.2 2. Control Implementation

7.2.1 2.1 Access Control Policy

Policy Statement: [TODO: Beschreiben Sie die Zugriffssteuerungsrichtlinie der Organisation]

Scope: [TODO: Geltungsbereich]
Roles and Responsibilities: [TODO: Rollen]
Compliance: [TODO: Compliance-Anforderungen]

7.2.2 2.2 Access Control Procedures

Procedures: - [TODO: Prozedur 1] - [TODO: Prozedur 2] - [TODO: Prozedur 3]

7.3 3. Control Enhancements

[TODO: Liste anwendbarer Control Enhancements]

7.4 4. Implementation Status

Status: [TODO: Implemented / Partially Implemented / Planned / Not Applicable]
Implementation Date: [TODO: Datum]
Responsible: [TODO: Name/Rolle]

7.5 5. Assessment

Assessment Method: [TODO: Examine / Interview / Test]
Assessment Status: [TODO: Satisfied / Other than Satisfied / Not Applicable]
Findings: [TODO: Beschreibung]

Dokumenthistorie:

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

ewpage

Chapter 8

Account Management

Dokument-ID: NIST-0110
Control Family: Access Control (AC)
Control: AC-2
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Letzte Aktualisierung: {{ meta.document.last_updated }}

8.1 1. Control Description

AC-2 Account Management

The organization manages information system accounts including identification, authorization, monitoring, and termination.

8.2 2. Control Implementation

8.2.1 2.1 Account Types

Account Type	Description	Approval Required
Individual	Personal user accounts	Manager
Group	Shared group accounts	ISSO
System	Service accounts	System Owner
Guest	Temporary access	ISSO
Privileged	Administrative accounts	ISSM

8.2.2 2.2 Account Management Process

Account Creation: 1. Access request submitted 2. Manager approval 3. ISSO review 4. Account provisioning 5. User notification

Account Modification: - Role changes require manager approval - Privilege escalation requires ISSO approval

Account Termination: - Immediate termination upon separation - Automated deprovisioning within 24 hours

8.2.3 2.3 Account Monitoring

Monitoring Activities: - Inactive accounts reviewed monthly - Privileged account usage logged - Failed login attempts monitored - Account anomalies investigated

8.3 3. Control Enhancements

AC-2(1) Automated System Account Management: [TODO: Implemented / Not Implemented]
AC-2(2) Automated Temporary and Emergency Account Management: [TODO: Implemented / Not Implemented]
AC-2(3) Disable Accounts: [TODO: Implemented / Not Implemented]
AC-2(4) Automated Audit Actions: [TODO: Implemented / Not Implemented]

8.4 4. Implementation Status

Status: [TODO: Implemented / Partially Implemented / Planned]
Implementation Date: [TODO: Datum]
Responsible: {{ meta.roles.isso.name }}

8.5 5. Assessment

Assessment Method: Examine, Interview, Test
Assessment Status: [TODO: Satisfied / Other than Satisfied]
Findings: [TODO: Beschreibung]

Dokumenthistorie:

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

ewpage

Chapter 9

Zugriffsdurchsetzung

Dokument-ID: NIST-0120
Kontrollfamilie: Zugriffskontrolle (AC)
Kontrolle: AC-3
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

9.1 1. Kontrollbeschreibung

AC-3 Zugriffsdurchsetzung

Das Informationssystem setzt genehmigte Autorisierungen für den logischen Zugriff auf Informationen und Systemressourcen gemäß den geltenden Zugriffskontrollrichtlinien durch.

9.2 2. Kontrollimplementierung

9.2.1 2.1 Zugriffsdurchsetzungsmechanismen

Durchsetzungsmethoden: - Rollenbasierte Zugriffskontrolle (RBAC) - Obligatorische Zugriffskontrolle (MAC) - Diskretionäre Zugriffskontrolle (DAC) - Attributbasierte Zugriffskontrolle (ABAC)

[TODO: Beschreiben Sie die implementierten Zugriffskontrollmechanismen]

9.2.2 2.2 Autorisierungsrichtlinien

Richtlinienrahmen: [TODO: Beschreiben Sie die Autorisierungsrichtlinien]

Zugriffsentscheidungskriterien: - [TODO: Kriterium 1] - [TODO: Kriterium 2] - [TODO: Kriterium 3]

9.2.3 2.3 Technische Implementierung

Systemkomponenten: [TODO: Liste der Systeme mit Zugriffskontrolle]

Durchsetzungspunkte: [TODO: Beschreibung der Durchsetzungspunkte]

9.3 3. Kontrollerweiterungen

- **AC-3(1):** Eingeschränkter Zugriff auf privilegierte Funktionen
- **AC-3(2):** Duale Autorisierung
- **AC-3(3):** Obligatorische Zugriffskontrolle
- **AC-3(4):** Diskretionäre Zugriffskontrolle
- **AC-3(7):** Rollenbasierte Zugriffskontrolle
- **AC-3(8):** Widerruf von Zugriffsautorisierungen

[TODO: Markieren Sie zutreffende Erweiterungen]

9.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

9.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 10

Informationsfluss-Durchsetzung

Dokument-ID: NIST-0130
Kontrollfamilie: Zugriffskontrolle (AC)
Kontrolle: AC-4
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

10.1 1. Kontrollbeschreibung

AC-4 Informationsfluss-Durchsetzung

Das Informationssystem setzt genehmigte Autorisierungen zur Steuerung des Informationsflusses innerhalb des Systems und zwischen verbundenen Systemen durch.

10.2 2. Kontrollimplementierung

10.2.1 2.1 Informationsfluss-Richtlinien

Flusssteuerungsmechanismen: - Netzwerksegmentierung - Firewalls und Zugriffskontrolllisten - Data Loss Prevention (DLP) - Verschlüsselung - Sicherheitsgateways

[TODO: Beschreiben Sie die Informationsfluss-Richtlinien]

10.2.2 2.2 Flusssteuerungspunkte

Kontrollpunkte: | Kontrollpunkt | Typ | Richtlinie | Status | |————|—|————|——| | [TODO] | [TODO] | [TODO] | [TODO] |

10.2.3 2.3 Informationsfluss-Beschränkungen

Beschränkungen: - Datenklassifizierung und Kennzeichnung - Trennung von Produktions- und Entwicklungsumgebungen - Einschränkungen für externe Verbindungen - Kontrolle von Datenexporten

[TODO: Definieren Sie spezifische Beschränkungen]

10.2.4 2.4 Überwachung und Durchsetzung

Überwachungsmaßnahmen: [TODO: Beschreiben Sie Überwachungs- und Durchsetzungsverfahren]

10.3 3. Kontrollerweiterungen

- **AC-4(1):** Objektsicherheitsattribute
- **AC-4(2):** Verarbeitungsdomänen
- **AC-4(3):** Dynamische Informationsfluss-Kontrolle
- **AC-4(4):** Inhaltsprüfung verschlüsselter Informationen
- **AC-4(8):** Sicherheitsrichtlinienfilter

[TODO: Markieren Sie zutreffende Erweiterungen]

10.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

10.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 11

Aufgabentrennung

Dokument-ID: NIST-0140
Kontrollfamilie: Zugriffskontrolle (AC)
Kontrolle: AC-5
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

11.1 1. Kontrollbeschreibung

AC-5 Aufgabentrennung

Die Organisation trennt Aufgaben von Einzelpersonen, um das Potenzial für Betrug und Fehler zu reduzieren.

11.2 2. Kontrollimplementierung

11.2.1 2.1 Aufgabentrennungsrichtlinie

Trennungsprinzipien: - Keine einzelne Person kontrolliert alle kritischen Phasen einer Transaktion - Trennung von Entwicklungs-, Test- und Produktionsumgebungen - Trennung von Sicherheits- und Systemadministrationsfunktionen - Trennung von Genehmigungs- und Ausführungsfunktionen

[TODO: Definieren Sie organisationsspezifische Trennungsanforderungen]

11.2.2 2.2 Kritische Funktionen

Funktionen mit Trennungsanforderungen: | Funktion | Getrennte Rollen | Begründung | |———-|————–|————| | [TODO] | [TODO] | [TODO] |

11.2.3 2.3 Kompensationskontrollen

Wenn Trennung nicht möglich: - Verstärkte Überwachung - Detaillierte Protokollierung - Regelmäßige Überprüfungen - Managementgenehmigung

[TODO: Beschreiben Sie Kompensationskontrollen]

11.3 3. Kontrollerweiterungen

- **AC-5(1):** Automatisierte Unterstützung

[TODO: Markieren Sie zutreffende Erweiterungen]

11.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

11.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 12

Geringste Privilegien

Dokument-ID: NIST-0150
Kontrollfamilie: Zugriffskontrolle (AC)
Kontrolle: AC-6
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

12.1 1. Kontrollbeschreibung

AC-6 Geringste Privilegien

Die Organisation wendet das Prinzip der geringsten Privilegien an und erlaubt nur autorisierte Zugriffe für Benutzer (oder Prozesse, die im Namen von Benutzern handeln), die für die Erfüllung zugewiesener Aufgaben notwendig sind.

12.2 2. Kontrollimplementierung

12.2.1 2.1 Prinzip der geringsten Privilegien

Implementierungsansatz: - Standardbenutzerkonten ohne administrative Rechte - Privilegierte Zugriffe nur bei Bedarf - Zeitlich begrenzte Privilegienerweiterungen - Regelmäßige Überprüfung von Berechtigungen

[TODO: Beschreiben Sie die Implementierung]

12.2.2 2.2 Privilegierte Funktionen

Privilegierte Rollen: | Rolle | Privilegien | Begründung | Genehmigung | |——-|————-|——————|————-| | [TODO] | [TODO] | [TODO] | [TODO] |

12.2.3 2.3 Zugriffskontrollmechanismen

Mechanismen: - Rollenbasierte Zugriffskontrolle (RBAC) - Just-in-Time (JIT) Zugriff - Privileged Access Management (PAM) - Regelmäßige Zugriffszertifizierung

[TODO: Spezifizieren Sie verwendete Mechanismen]

12.2.4 2.4 Überwachung privilegierter Zugriffe

Überwachungsmaßnahmen: [TODO: Beschreiben Sie Überwachungsverfahren]

12.3 3. Kontrollerweiterungen

- **AC-6(1):** Autorisierung von Zugriff auf Sicherheitsfunktionen
- **AC-6(2):** Nicht-privilegierter Zugriff für nicht sicherheitsrelevante Funktionen
- **AC-6(3):** Netzwerkzugriff auf privilegierte Befehle
- **AC-6(5):** Privilegierte Konten
- **AC-6(7):** Überprüfung von Benutzerrechten
- **AC-6(9):** Protokollierung der Verwendung privilegierter Funktionen
- **AC-6(10):** Verbot nicht-privilegierter Benutzer, Sicherheitsfunktionen auszuführen

[TODO: Markieren Sie zutreffende Erweiterungen]

12.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

12.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated | default('') }}	{{ meta.defaults.author }}	Ersterstellung

ewpage

Chapter 13

Security Awareness and Training

Dokument-ID: NIST-0200
Control Family: Awareness and Training (AT)
Control: AT-1, AT-2, AT-3, AT-4
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Letzte Aktualisierung: {{ meta.document.last_updated }}

13.1 1. Control Description

AT-1 Policy and Procedures
AT-2 Literacy Training and Awareness
AT-3 Role-Based Training
AT-4 Training Records

The organization provides security awareness training and role-based security training.

13.2 2. Control Implementation

13.2.1 2.1 Security Awareness Program

Training Topics: - Information security policies - Phishing and social engineering - Password security - Physical security - Incident reporting - Data protection

Training Frequency: - Initial training: Upon hire - Annual refresher training - Ad-hoc training: As needed

13.2.2 2.2 Role-Based Training

Role	Training Requirements	Frequency
All Users	Security Awareness	Annual
Privileged Users	Advanced Security	Annual
Developers	Secure Coding	Annual
ISSO/ISSM	Security Management	Annual
Incident Responders	Incident Response	Semi-annual

13.2.3 2.3 Training Records

Record Retention: [TODO: 3 years]
Records Include: - Training date - Training topic - Attendee name - Completion status - Assessment results

13.3 3. Implementation Status

Status: [TODO: Implemented / Partially Implemented / Planned]
Training Platform: [TODO: Platform name]
Completion Rate: [TODO: Percentage]

Dokumenthistorie:

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

ewpage

Chapter 14

Rollenbasierte Schulung

Dokument-ID: NIST-0210
Kontrollfamilie: Sensibilisierung und Schulung (AT)
Kontrolle: AT-3
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

14.1 1. Kontrollbeschreibung

AT-3 Rollenbasierte Schulung

Die Organisation bietet rollenbasierte Sicherheits- und Datenschutzschulungen für Personal mit zugewiesenen Sicherheitsrollen und -verantwortlichkeiten an.

14.2 2. Kontrollimplementierung

14.2.1 2.1 Rollenbasiertes Schulungsprogramm

Schulungsanforderungen nach Rolle: | Rolle | Schulungsthemen | Häufigkeit | Dauer | |——-|——————|————|——-| | Systemadministratoren | Sichere Konfiguration, Patch-Management, Zugriffskontrolle | Jährlich | [TODO] | | Sicherheitspersonal | Bedrohungsanalyse, Incident Response, Forensik | Jährlich | [TODO] | | Entwickler | Sichere Programmierung, SDLC-Sicherheit, Code-Review | Jährlich | [TODO] | | Manager | Risikomanagement, Compliance, Richtliniendurchsetzung | Jährlich | [TODO] | | [TODO] | [TODO] | [TODO] | [TODO] |

14.2.2 2.2 Schulungsinhalte

Kernthemen: - Rollenspezifische Sicherheitsverantwortlichkeiten - Anwendbare Sicherheitsrichtlinien und -verfahren - Sicherheitstechnologien und -werkzeuge - Bedrohungslandschaft und Angriffsvektoren - Verfahren zur Meldung von Vorfällen

[TODO: Detaillieren Sie Schulungsinhalte für jede Rolle]

14.2.3 2.3 Schulungsdurchführung

Durchführungsmethoden: - Präsenzschulungen - Online-Kurse - Workshops und Labore - Training on the Job - Zertifizierungsprogramme

[TODO: Spezifizieren Sie Durchführungsmethoden]

14.2.4 2.4 Schulungsnachweise

Dokumentation: - Schulungsabschlussnachweise - Bewertungsergebnisse - Zertifizierungsverfolgung - Auffrischungsschulungsplan

[TODO: Beschreiben Sie Verfahren zur Aufzeichnung]

14.3 3. Kontrollerweiterungen

- **AT-3(1):** Umgebungskontrollen
- **AT-3(2):** Physische Sicherheitskontrollen
- **AT-3(3):** Praktische Übungen
- **AT-3(4):** Verdächtige Kommunikation und anomales Systemverhalten
- **AT-3(5):** Verarbeitung personenbezogener Daten

[TODO: Markieren Sie zutreffende Erweiterungen]

14.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

14.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 15

Audit and Accountability Policy

Dokument-ID: NIST-0220
Control Family: Audit and Accountability (AU)
Control: AU-1, AU-2, AU-3
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Letzte Aktualisierung: {{ meta.document.last_updated }}

15.1 1. Control Description

AU-1 Policy and Procedures
AU-2 Audit Events
AU-3 Content of Audit Records

The organization implements audit and accountability controls to track system activity.

15.2 2. Control Implementation

15.2.1 2.1 Auditable Events

Security-Relevant Events: - Successful and failed login attempts - Account management actions - Privilege escalation - System configuration changes - Data access and modifications - Security policy changes

15.2.2 2.2 Audit Record Content

Required Information: - Event type - Date and time - User/process identity - Source and destination - Event outcome (success/failure) - Additional details

15.2.3 2.3 Audit Log Management

Log Retention: [TODO: 90 days online, 1 year archive]
Log Protection: Encrypted, access-controlled
Log Review: Daily for critical systems

15.3 3. Implementation Status

Status: [TODO: Implemented / Partially Implemented / Planned]
SIEM Solution: [TODO: Tool name]
Log Sources: [TODO: Number of sources]

Dokumenthistorie:

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

ewpage

Chapter 16

Audit-Ereignisse

Dokument-ID: NIST-0230
Kontrollfamilie: Audit und Rechenschaftspflicht (AU)
Kontrolle: AU-2
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

16.1 1. Kontrollbeschreibung

AU-2 Audit-Ereignisse

Die Organisation bestimmt, dass das Informationssystem in der Lage ist, bestimmte Ereignisse zu auditieren, und koordiniert die Sicherheitsauditfunktion mit anderen Organisationseinheiten.

16.2 2. Kontrollimplementierung

16.2.1 2.1 Auditierbare Ereignisse

Ereigniskategorien: - Kontoverwaltungsereignisse - Authentifizierungs- und Autorisierungsereignisse - Privilegienerweiterungsereignisse - System- und Anwendungszugriffsereignisse - Konfigurationsänderungen - Sicherheitsrichtlinienänderungen - Datenzugriff und -änderung - Netzwerkaktivität - Systemstart und -herunterfahren

[TODO: Spezifizieren Sie auditierbare Ereignisse für Ihre Organisation]

16.2.2 2.2 Ereignisauswahlkriterien

Auswahlbegründung: | Ereignistyp | Begründung | Häufigkeit | |————-|————|————| | Fehlgeschlagene Anmeldeversuche | Erkennung unbefugter Zugriffsversuche | Echtzeit | | Privilegienänderungen | Überwachung der Privilegienerweiterung | Echtzeit | | Konfigurationsänderun-

gen | Verfolgung von Systemänderungen | Echtzeit | | Datenzugriff | Überwachung des Zugriffs auf sensible Daten | Echtzeit | | [TODO] | [TODO] | [TODO] |

16.2.3 2.3 Audit-Koordination

Koordinationsaktivitäten: - Überprüfung der Auditanforderungen mit Stakeholdern - Koordination mit dem Incident-Response-Team - Abstimmung mit Compliance-Anforderungen - Integration mit SIEM-Systemen

[TODO: Beschreiben Sie Koordinationsverfahren]

16.2.4 2.4 Audit-Überprüfung und -Aktualisierungen

Überprüfungsplan: [TODO: z.B. Vierteljährlich]
Aktualisierungsauslöser: - Neue identifizierte Bedrohungen - Änderungen der Compliance-Anforderungen - Erkenntnisse aus Vorfällen - Technologieänderungen

[TODO: Definieren Sie Überprüfungs- und Aktualisierungsverfahren]

16.3 3. Kontrollerweiterungen

- **AU-2(1):** Zusammenstellung von Audit-Aufzeichnungen aus mehreren Quellen
- **AU-2(2):** Auswahl von Audit-Ereignissen nach Komponente
- **AU-2(3):** Überprüfungen und Aktualisierungen
- **AU-2(4):** Privilegierte Funktionen

[TODO: Markieren Sie zutreffende Erweiterungen]

16.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

16.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 17

Audit-Log-Speicherung und Schutz

Dokument-ID: NIST-0240
Kontrollfamilie: Audit und Rechenschaftspflicht (AU)
Kontrolle: AU-4, AU-9
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

17.1 1. Kontrollbeschreibung

AU-4 Audit-Log-Speicherkapazität

Die Organisation weist Audit-Log-Speicherkapazität gemäß den Anforderungen zur Aufbewahrung von Audit-Aufzeichnungen zu.

AU-9 Schutz von Audit-Informationen

Das Informationssystem schützt Audit-Informationen und Audit-Tools vor unbefugtem Zugriff, Änderung und Löschung.

17.2 2. Kontrollimplementierung

17.2.1 2.1 Speicherkapazitätsplanung

Kapazitätsanforderungen: | System | Tägliches Volumen | Aufbewahrungsdauer | Erforderliche Kapazität | |——–|——————-|——————|——————–| | [TODO] | [TODO] | [TODO] | [TODO] |

Überwachung: - Automatische Kapazitätsüberwachung - Warnungen bei Schwellenwertüberschreitung - Automatische Archivierung

[TODO: Beschreiben Sie Kapazitätsplanung und -überwachung]

17.2.2 2.2 Schutzmaßnahmen

Zugriffskontrollen: - Eingeschränkter Zugriff auf Audit-Logs - Rollenbasierte Berechtigungen - Privileged Access Management

Integritätsschutz: - Digitale Signaturen - Schreibgeschützte Speicherung - Kryptografische Hashes

Verfügbarkeitsschutz: - Redundante Speicherung - Regelmäßige Backups - Disaster Recovery

[TODO: Spezifizieren Sie Schutzmaßnahmen]

17.2.3 2.3 Audit-Tool-Schutz

Geschützte Tools: [TODO: Liste der geschützten Audit-Tools]

Schutzmaßnahmen: [TODO: Beschreiben Sie Schutzmaßnahmen für Tools]

17.3 3. Kontrollerweiterungen

AU-4: - **AU-4(1):** Übertragung auf alternatives System

AU-9: - **AU-9(1):** Hardware-Schreibschutz - **AU-9(2):** Sicherung von Audit-Informationen - **AU-9(3):** Kryptografischer Schutz - **AU-9(4):** Zugriff durch Teilmenge privilegierter Benutzer - **AU-9(5):** Dual-Autorisierung - **AU-9(6):** Schreibzugriff auf Audit-Informationen

[TODO: Markieren Sie zutreffende Erweiterungen]

17.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

17.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated | default('') }}	{{ meta.defaults.author }}	Ersterstellung

ewpage

Chapter 18

Audit-Überprüfung und Analyse

Dokument-ID: NIST-0250
Kontrollfamilie: Audit und Rechenschaftspflicht (AU)
Kontrolle: AU-6, AU-7
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

18.1 1. Kontrollbeschreibung

AU-6 Audit-Aufzeichnungsüberprüfung, -analyse und -berichterstattung

Die Organisation überprüft und analysiert Informationssystem-Audit-Aufzeichnungen regelmäßig auf Hinweise auf unangemessene oder ungewöhnliche Aktivitäten.

AU-7 Audit-Aufzeichnungsreduzierung und Berichtserstellung

Das Informationssystem bietet eine Audit-Aufzeichnungsreduzierungs- und Berichtserstellungsfunktion.

18.2 2. Kontrollimplementierung

18.2.1 2.1 Überprüfungs- und Analyseprozess

Überprüfungshäufigkeit: [TODO: z.B. Täglich, Wöchentlich]
Verantwortliche Rollen: [TODO: Rollen]

Analysemethoden: - Automatisierte Analyse mit SIEM - Manuelle Überprüfung kritischer Ereignisse - Korrelation mit Bedrohungsinformationen - Trendanalyse

[TODO: Beschreiben Sie Überprüfungs- und Analyseverfahren]

18.2.2 2.2 Berichterstattung

Berichtstypen: | Berichtstyp | Häufigkeit | Empfänger | Inhalt | |————-|————|————|———| | [TODO] | [TODO] | [TODO] | [TODO] |

18.2.3 2.3 Reduzierungs- und Filterfunktionen

Filtermechanismen: - Zeitbasierte Filter - Ereignistypfilter - Schweregrad-basierte Filter - Benutzer-/System-basierte Filter

[TODO: Spezifizieren Sie Filterfunktionen]

18.2.4 2.4 Eskalation und Reaktion

Eskalationskriterien: [TODO: Definieren Sie Kriterien für Eskalation]

Reaktionsverfahren: [TODO: Beschreiben Sie Reaktionsverfahren]

18.3 3. Kontrollerweiterungen

AU-6: - **AU-6(1):** Automatisierte Prozess-Integration - **AU-6(3):** Korrelation mit physischen Zugriffsereignissen - **AU-6(4):** Zentrale Überprüfung und Analyse - **AU-6(5):** Integration mit Schwachstellenscans - **AU-6(6):** Korrelation mit Bedrohungsinformationen - **AU-6(7):** Erlaubte Aktionen - **AU-6(10):** Audit-Level-Anpassung

AU-7: - **AU-7(1):** Automatische Verarbeitung - **AU-7(2):** Automatische Sortierung und Suche

[TODO: Markieren Sie zutreffende Erweiterungen]

18.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

18.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 19

Configuration Management Policy

Dokument-ID: NIST-0300
Control Family: Configuration Management (CM)
Control: CM-1, CM-2, CM-3
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Letzte Aktualisierung: {{ meta.document.last_updated }}

19.1 1. Control Description

CM-1 Policy and Procedures
CM-2 Baseline Configuration
CM-3 Configuration Change Control

The organization establishes and maintains baseline configurations and controls changes.

19.2 2. Control Implementation

19.2.1 2.1 Baseline Configuration

Configuration Items: - Operating systems - Applications - Network devices - Security tools - Databases

Baseline Documentation: - Hardware inventory - Software inventory - Network topology - Security settings

19.2.2 2.2 Configuration Change Control

Change Process: 1. Change request submission 2. Impact analysis 3. Security review 4. Approval 5. Implementation 6. Verification 7. Documentation

Change Categories: - Emergency changes - Standard changes - Normal changes

19.2.3 2.3 Configuration Monitoring

Monitoring Methods: - Automated configuration scanning - Manual configuration reviews - Change detection alerts

Review Frequency: [TODO: Weekly / Monthly]

19.3 3. Implementation Status

Status: [TODO: Implemented / Partially Implemented / Planned]
Configuration Management Tool: [TODO: Tool name]
Baseline Compliance: [TODO: Percentage]

Dokumenthistorie:

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

ewpage

Chapter 20

Konfigurations-Baseline und Einstellungen

Dokument-ID: NIST-0310
Kontrollfamilie: Konfigurationsmanagement (CM)
Kontrolle: CM-2, CM-6, CM-7
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

20.1 1. Kontrollbeschreibung

CM-2 Baseline-Konfiguration

Die Organisation entwickelt, dokumentiert und pflegt eine aktuelle Baseline-Konfiguration des Informationssystems.

CM-6 Konfigurationseinstellungen

Die Organisation legt obligatorische Konfigurationseinstellungen für IT-Produkte fest, implementiert und dokumentiert sie.

CM-7 Geringste Funktionalität

Die Organisation konfiguriert das Informationssystem so, dass nur wesentliche Funktionen bereitgestellt werden.

20.2 2. Kontrollimplementierung

20.2.1 2.1 Baseline-Konfiguration

Baseline-Komponenten: | Komponente | Baseline-Version | Letzte Überprüfung | Status | |——————|——————|——————-|——| | [TODO] | [TODO] | [TODO] | [TODO] |

Baseline-Dokumentation: [TODO: Beschreiben Sie Baseline-Dokumentation]

20.2.2 2.2 Konfigurationseinstellungen

Sicherheitseinstellungen: - Betriebssystem-Härtung - Anwendungskonfiguration - Netzwerkgeräte-Konfiguration - Datenbank-Sicherheitseinstellungen

Konfigurationsstandards: [TODO: Referenzieren Sie anwendbare Standards (z.B. CIS Benchmarks, DISA STIGs)]

20.2.3 2.3 Geringste Funktionalität

Deaktivierte Funktionen: - Nicht benötigte Dienste - Nicht verwendete Ports und Protokolle - Unnötige Software - Nicht erforderliche Funktionen

[TODO: Listen Sie deaktivierte Funktionen auf]

20.2.4 2.4 Konfigurationsüberprüfung

Überprüfungshäufigkeit: [TODO: z.B. Monatlich]
Überprüfungsmethoden: - Automatisierte Scans - Manuelle Überprüfungen - Compliance-Checks

[TODO: Beschreiben Sie Überprüfungsverfahren]

20.3 3. Kontrollerweiterungen

CM-2: - **CM-2(1):** Überprüfungen und Aktualisierungen - **CM-2(2):** Automatisierung zur Unterstützung aktueller Informationen - **CM-2(3):** Aufbewahrung früherer Konfigurationen - **CM-2(7):** Konfigurierte Systeme, Komponenten oder Geräte für hochriskante Bereiche

CM-6: - **CM-6(1):** Automatisierte zentrale Verwaltung, Anwendung und Überprüfung - **CM-6(2):** Reaktion auf unbefugte Änderungen

CM-7: - **CM-7(1):** Periodische Überprüfung - **CM-7(2):** Verhinderung der Programmausführung - **CM-7(5):** Autorisierte Software / Whitelisting

[TODO: Markieren Sie zutreffende Erweiterungen]

20.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

20.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 21

Konfigurations-Änderungssteuerung

Dokument-ID: NIST-0320
Kontrollfamilie: Konfigurationsmanagement (CM)
Kontrolle: CM-3, CM-4, CM-5
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

21.1 1. Kontrollbeschreibung

CM-3 Konfigurationsänderungssteuerung

Die Organisation bestimmt die Arten von Änderungen am Informationssystem, die konfigurationsgesteuert sind, überprüft vorgeschlagene konfigurationsgesteuerte Änderungen und genehmigt oder lehnt solche Änderungen ab.

21.2 2. Kontrollimplementierung

21.2.1 2.1 Änderungssteuerungsprozess

Änderungstypen: [TODO: Definieren Sie Änderungstypen]

Genehmigungsworkflow: [TODO: Beschreiben Sie Genehmigungsprozess]

21.2.2 2.2 Änderungsdokumentation

[TODO: Beschreiben Sie Dokumentationsanforderungen]

21.2.3 2.3 Änderungstests

[TODO: Beschreiben Sie Testanforderungen]

21.3 3. Kontrollerweiterungen

- **CM-3(1):** Automatisierte Dokumentation
- **CM-3(2):** Test/Validierung/Dokumentation von Änderungen
- **CM-4:** Auswirkungsanalysen
- **CM-5:** Zugriffsbeschränkungen für Änderungen

[TODO: Markieren Sie zutreffende Erweiterungen]

21.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

21.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 22

Contingency Planning Policy

Dokument-ID: NIST-0330
Control Family: Contingency Planning (CP)
Control: CP-1, CP-2, CP-9
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Letzte Aktualisierung: {{ meta.document.last_updated }}

22.1 1. Control Description

CP-1 Policy and Procedures
CP-2 Contingency Plan
CP-9 System Backup

The organization develops and maintains contingency plans and backup procedures.

22.2 2. Control Implementation

22.2.1 2.1 Contingency Plan

Plan Components: - Roles and responsibilities - Recovery procedures - Communication plan - Alternate processing site - Reconstitution procedures

Recovery Objectives: - Recovery Time Objective (RTO): [TODO: Hours] - Recovery Point Objective (RPO): [TODO: Hours]

22.2.2 2.2 Backup Procedures

Backup Types: - Full backups: [TODO: Weekly] - Incremental backups: [TODO: Daily] - Differential backups: [TODO: As needed]

Backup Storage: - Primary: [TODO: Location] - Secondary: [TODO: Offsite location]

Backup Testing: [TODO: Quarterly]

22.2.3 2.3 Contingency Plan Testing

Testing Frequency: [TODO: Annual]
Testing Methods: - Tabletop exercises - Functional tests - Full-scale exercises

22.3 3. Implementation Status

Status: [TODO: Implemented / Partially Implemented / Planned]
Last Test Date: [TODO: Datum]
Next Test Date: [TODO: Datum]

Dokumenthistorie:

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

ewpage

Chapter 23

Notfallplan und Ausweichstandorte

Dokument-ID: NIST-0340
Kontrollfamilie: Notfallplanung (CP)
Kontrollen: CP-2, CP-6, CP-7
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

23.1 1. Kontrollbeschreibung

Dieses Dokument umfasst Notfallplanung und Ausweichstandort-Kontrollen: - **CP-2:** Notfallplan - **CP-6:** Alternativer Speicherstandort - **CP-7:** Alternativer Verarbeitungsstandort

23.2 2. Kontrollimplementierung

23.2.1 2.1 Notfallplan (CP-2)

Plankomponenten: - Wesentliche Missionen und Geschäftsfunktionen - Wiederherstellungsziele (RTO/RPO) - Wiederherstellungsprioritäten - Rollen und Verantwortlichkeiten - Kontaktinformationen - Alternative Einrichtungen - Wiederherstellungsverfahren - Technische Notfalloperationen

[TODO: Entwickeln Sie einen umfassenden Notfallplan]

Planverteilung: - Schlüsselpersonal: [TODO: Liste] - Alternativer Speicherort: [TODO: Standort] - Zugriffskontrollen: [TODO: Definieren]

Planüberprüfung und -aktualisierungen: - Überprüfungshäufigkeit: [TODO: z.B. Jährlich] - Aktualisierungsauslöser: [TODO: Auslöser auflisten] - Genehmigungsbehörde: [TODO: Rolle]

Plantests: - Testhäufigkeit: [TODO: z.B. Jährlich] - Testtypen: Tabletop, funktional, vollständig - Testdokumentation: [TODO: Anforderungen]

23.2.2 2.2 Alternativer Speicherstandort (CP-6)

Standortdetails: - Standort: [TODO: Geografischer Standort] - Typ: Hot/Warm/Cold Site - Entfernung vom Primärstandort: [TODO: Meilen/km] - Kapazität: [TODO: Speicherkapazität]

Datenreplikation: - Replikationsmethode: [TODO: Synchron/Asynchron] - Replikationshäufigkeit: [TODO: Echtzeit/Geplant] - Replizierte Datentypen: [TODO: Liste]

Zugriff und Sicherheit: - Physische Sicherheit: [TODO: Maßnahmen] - Logische Zugriffskontrollen: [TODO: Kontrollen] - Umgebungskontrollen: [TODO: Anforderungen]

Vereinbarungen: [TODO: Dokumentieren Sie Vereinbarungen]

23.2.3 2.3 Alternativer Verarbeitungsstandort (CP-7)

Verarbeitungsstandort-Details: - Standort: [TODO: Geografischer Standort] - Typ: Hot/Warm/Cold Site - Entfernung vom Primärstandort: [TODO: Meilen/km] - Kapazität: [TODO: Verarbeitungskapazität]

Standortfähigkeiten: [TODO: Detaillieren Sie Standortfähigkeiten]

Aktivierungsverfahren: [TODO: Definieren Sie Aktivierungsverfahren]

23.3 3. Kontrollerweiterungen

- **CP-2(1):** Koordination mit verwandten Plänen
- **CP-2(2):** Kapazitätsplanung
- **CP-2(3):** Wiederaufnahme von Missions- und Geschäftsfunktionen
- **CP-6(1):** Trennung vom Primärstandort
- **CP-7(1):** Trennung vom Primärstandort

[TODO: Markieren Sie zutreffende Erweiterungen]

23.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

23.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 24

System-Backup und Wiederherstellung

Dokument-ID: NIST-0350
Kontrollfamilie: Notfallplanung (CP)
Kontrollen: CP-9, CP-10
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

24.1 1. Kontrollbeschreibung

CP-9 System-Backup

Die Organisation führt Backups von Benutzerinformationen und Systeminformationen durch.

CP-10 Systemwiederherstellung und -wiederaufbau

Die Organisation bietet die Wiederherstellung und Wiederaufbau des Informationssystems in einen bekannten Zustand.

24.2 2. Kontrollimplementierung

24.2.1 2.1 Backup-Strategie

Backup-Typen: - Vollständige Backups - Inkrementelle Backups - Differentielle Backups

Backup-Zeitplan: | Datentyp | Häufigkeit | Aufbewahrung | Standort | |———-|———–|———–|———-| | [TODO] | [TODO] | [TODO] | [TODO] |

24.2.2 2.2 Backup-Schutz

Schutzmaßnahmen: - Verschlüsselung - Zugriffskontrolle - Physische Sicherheit

[TODO: Beschreiben Sie Schutzmaßnahmen]

24.2.3 2.3 Wiederherstellungsverfahren

Wiederherstellungsschritte: [TODO: Definieren Sie Wiederherstellungsverfahren]

Wiederherstellungstests: [TODO: Beschreiben Sie Testverfahren]

24.3 3. Kontrollerweiterungen

- **CP-9(1):** Tests auf Zuverlässigkeit/Integrität
- **CP-9(2):** Testwiederherstellung mit Stichproben
- **CP-9(3):** Separate Speicherung für kritische Informationen
- **CP-9(5):** Übertragung an alternativen Speicherstandort
- **CP-10(2):** Transaktion-Wiederherstellung

[TODO: Markieren Sie zutreffende Erweiterungen]

24.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

24.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 25

Identification and Authentication Policy

Dokument-ID: NIST-0400
Control Family: Identification and Authentication (IA)
Control: IA-1, IA-2, IA-5
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Letzte Aktualisierung: {{ meta.document.last_updated }}

25.1 1. Control Description

IA-1 Policy and Procedures
IA-2 Identification and Authentication (Organizational Users)
IA-5 Authenticator Management

The organization uniquely identifies and authenticates users.

25.2 2. Control Implementation

25.2.1 2.1 User Identification

Identification Methods: - Unique user IDs - No shared accounts (except approved exceptions) - User ID format: [TODO: Format]

25.2.2 2.2 Authentication Methods

Authentication Factors: - Something you know (password) - Something you have (token, smart card) - Something you are (biometric)

Multi-Factor Authentication (MFA): - Required for: [TODO: Privileged access, remote access] - MFA methods: [TODO: Methods]

25.2.3 2.3 Password Requirements

Password Policy: - Minimum length: [TODO: 12 characters] - Complexity: [TODO: Requirements] - Maximum age: [TODO: 90 days] - Password history: [TODO: 24 passwords] - Account lockout: [TODO: 5 failed attempts]

25.2.4 2.4 Authenticator Management

Authenticator Lifecycle: - Initial distribution - Periodic renewal - Revocation upon termination - Lost/stolen procedures

25.3 3. Implementation Status

Status: [TODO: Implemented / Partially Implemented / Planned]
MFA Coverage: [TODO: Percentage]
Password Compliance: [TODO: Percentage]

Dokumenthistorie:

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

ewpage

Chapter 26

Benutzer- und Geräte-Authentifizierung

Dokument-ID: NIST-0410
Kontrollfamilie: Identifizierung und Authentifizierung (IA)
Kontrollen: IA-2, IA-3, IA-4, IA-6, IA-8
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

26.1 1. Kontrollbeschreibung

Dieses Dokument umfasst Identifizierungs- und Authentifizierungskontrollen für Benutzer und Geräte.

26.2 2. Kontrollimplementierung

26.2.1 2.1 Benutzerauthentifizierung (IA-2)

Authentifizierungsmethoden: - Passwörter - Multi-Faktor-Authentifizierung (MFA) - Biometrische Authentifizierung - Zertifikatsbasierte Authentifizierung

[TODO: Beschreiben Sie implementierte Methoden]

26.2.2 2.2 Geräteauthentifizierung (IA-3)

Geräteidentifizierung: [TODO: Beschreiben Sie Geräteauthentifizierungsmechanismen]

26.2.3 2.3 Identifikatorverwaltung (IA-4)

Identifikatorrichtlinien: [TODO: Definieren Sie Identifikatorverwaltungsrichtlinien]

26.2.4 2.4 Authentifizierungs-Feedback (IA-6)

Feedback-Kontrollen: [TODO: Beschreiben Sie Feedback-Mechanismen]

26.2.5 2.5 Nicht-organisatorische Benutzer (IA-8)

Externe Benutzerauthentifizierung: [TODO: Beschreiben Sie Authentifizierung für externe Benutzer]

26.3 3. Kontrollerweiterungen

- **IA-2(1):** Multi-Faktor-Authentifizierung für Netzwerkzugriff
- **IA-2(2):** Multi-Faktor-Authentifizierung für nicht-privilegierten Zugriff
- **IA-2(3):** Multi-Faktor-Authentifizierung für lokalen Zugriff
- **IA-2(8):** Replay-resistente Authentifizierung
- **IA-2(12):** Akzeptanz von PIV-Anmeldeinformationen

[TODO: Markieren Sie zutreffende Erweiterungen]

26.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

26.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 27

Authentifikator-Verwaltung

Dokument-ID: NIST-0420
Kontrollfamilie: Identifizierung und Authentifizierung (IA)
Kontrollen: IA-5, IA-7
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

27.1 1. Kontrollbeschreibung

IA-5 Authentifikator-Verwaltung

Die Organisation verwaltet Informationssystem-Authentifikatoren.

IA-7 Kryptografische Modul-Authentifizierung

Das Informationssystem implementiert Mechanismen zur Authentifizierung an ein kryptografisches Modul.

27.2 2. Kontrollimplementierung

27.2.1 2.1 Authentifikator-Verwaltung

Authentifikatortypen: - Passwörter - Kryptografische Schlüssel - Biometrische Daten - Token

Verwaltungsverfahren: [TODO: Beschreiben Sie Verwaltungsverfahren]

27.2.2 2.2 Passwortrichtlinien

Anforderungen: - Mindestlänge - Komplexität - Ablauf - Wiederverwendungsbeschränkungen

[TODO: Definieren Sie Passwortrichtlinien]

27.2.3 2.3 Kryptografische Authentifizierung

Kryptografische Mechanismen: [TODO: Beschreiben Sie kryptografische Authentifizierungsmechanismen]

27.3 3. Kontrollerweiterungen

- **IA-5(1):** Passwortbasierte Authentifizierung
- **IA-5(2):** PKI-basierte Authentifizierung
- **IA-5(3):** Authentifikatoren im Besitz der Organisation
- **IA-5(4):** Automatisierte Tools
- **IA-5(6):** Schutz von Authentifikatoren
- **IA-5(7):** Keine eingebetteten unverschlüsselten statischen Authentifikatoren

[TODO: Markieren Sie zutreffende Erweiterungen]

27.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

27.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 28

Incident Response Policy

Dokument-ID: NIST-0430
Control Family: Incident Response (IR)
Control: IR-1, IR-4, IR-5, IR-6
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Letzte Aktualisierung: {{ meta.document.last_updated }}

28.1 1. Control Description

IR-1 Policy and Procedures
IR-4 Incident Handling
IR-5 Incident Monitoring
IR-6 Incident Reporting

The organization implements incident response capabilities.

28.2 2. Control Implementation

28.2.1 2.1 Incident Response Process

Incident Response Phases: 1. **Preparation:** Training, tools, procedures 2. **Detection and Analysis:** Identify and assess incidents 3. **Containment, Eradication, and Recovery:** Limit damage and restore 4. **Post-Incident Activity:** Lessons learned

28.2.2 2.2 Incident Categories

Category	Severity	Response Time	Escalation
Critical	High	Immediate	ISSO, ISSM, AO
Major	Medium	1 hour	ISSO, ISSM

Category	Severity	Response Time	Escalation
Minor	Low	4 hours	ISSO

28.2.3 2.3 Incident Response Team

Team Members: - Incident Response Manager: [TODO: Name] - ISSO: {{ meta.roles.isso.name }} - System Administrator: [TODO: Name] - Legal: [TODO: Name] - Public Relations: [TODO: Name]

28.2.4 2.4 Incident Reporting

Internal Reporting: - ISSO: Immediate - ISSM: Within 1 hour - AO: Within 4 hours

External Reporting: - US-CERT: Within 1 hour for major incidents - Law Enforcement: As required - Affected Parties: As required

28.2.5 2.5 Incident Documentation

Required Information: - Incident date/time - Detection method - Incident description - Systems affected - Actions taken - Lessons learned

28.3 3. Implementation Status

Status: [TODO: Implemented / Partially Implemented / Planned]
Incident Response Plan: [TODO: Document reference]
Last Incident: [TODO: Date or None]

Dokumenthistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated | default('[TODO]') }}	{{ meta.defaults.author }}	Initiale Erstellung

ewpage

Chapter 29

Vorfallbehandlung und Unterstützung

Dokument-ID: NIST-0440
Kontrollfamilie: Incident Response (IR)
Kontrollen: IR-4, IR-7
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

29.1 1. Kontrollbeschreibung

IR-4 Vorfallbehandlung

Die Organisation implementiert Vorfallbehandlungsfähigkeiten für Sicherheitsvorfälle.

IR-7 Incident Response-Unterstützung

Die Organisation bietet eine Incident Response-Unterstützungsressource.

29.2 2. Kontrollimplementierung

29.2.1 2.1 Vorfallbehandlungsprozess

Phasen: 1. Vorbereitung 2. Erkennung und Analyse 3. Eindämmung, Beseitigung und Wiederherstellung 4. Post-Incident-Aktivitäten

[TODO: Beschreiben Sie Vorfallbehandlungsverfahren]

29.2.2 2.2 Incident Response-Team

Teammitglieder: [TODO: Listen Sie Teammitglieder und Rollen auf]

29.2.3 2.3 Unterstützungsressourcen

Verfügbare Ressourcen: [TODO: Beschreiben Sie Unterstützungsressourcen]

29.3 3. Kontrollerweiterungen

- **IR-4(1):** Automatisierte Vorfallbehandlungsprozesse
- **IR-4(2):** Dynamische Neukonfiguration
- **IR-4(3):** Kontinuität der Operationen
- **IR-4(4):** Informationskorrelation
- **IR-7(1):** Automatisierung für Verfügbarkeit von Informationen/Unterstützung
- **IR-7(2):** Koordination mit externen Anbietern

[TODO: Markieren Sie zutreffende Erweiterungen]

29.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

29.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 30

Vorfallüberwachung und Berichterstattung

Dokument-ID: NIST-0450
Kontrollfamilie: Incident Response (IR)
Kontrollen: IR-5, IR-6
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

30.1 1. Kontrollbeschreibung

IR-5 Vorfallüberwachung

Die Organisation verfolgt und dokumentiert Informationssystem-Sicherheitsvorfälle.

IR-6 Vorfallberichterstattung

Die Organisation verlangt, dass Personal Sicherheitsvorfälle meldet.

30.2 2. Kontrollimplementierung

30.2.1 2.1 Vorfallüberwachung

Überwachungsmechanismen: [TODO: Beschreiben Sie Überwachungsmechanismen]

Verfolgung und Dokumentation: [TODO: Beschreiben Sie Verfahren]

30.2.2 2.2 Berichterstattungsprozess

Berichterstattungskanäle: [TODO: Definieren Sie Berichterstattungskanäle]

Berichterstattungszeitrahmen: [TODO: Definieren Sie Zeitrahmen]

30.2.3 2.3 Externe Berichterstattung

Externe Stellen: [TODO: Listen Sie externe Berichterstattungsstellen auf]

30.3 3. Kontrollerweiterungen

- **IR-5(1):** Automatisierte Verfolgung/Datenerfassung/Analyse
- **IR-6(1):** Automatisierte Berichterstattung
- **IR-6(2):** Schwachstellenberichterstattung
- **IR-6(3):** Koordination mit Supply Chain

[TODO: Markieren Sie zutreffende Erweiterungen]

30.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

30.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 31

System Maintenance

Dokument-ID: NIST-0500
Control Family: Maintenance (MA)
Control: MA-1, MA-2, MA-4, MA-5
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Letzte Aktualisierung: {{ meta.document.last_updated }}

31.1 1. Control Description

MA-1 Policy and Procedures
MA-2 Controlled Maintenance
MA-4 Nonlocal Maintenance
MA-5 Maintenance Personnel

The organization performs system maintenance in a controlled manner.

31.2 2. Control Implementation

31.2.1 2.1 Maintenance Policy

Maintenance Types: - Preventive maintenance - Corrective maintenance - Emergency maintenance

Maintenance Schedule: [TODO: Schedule]

31.2.2 2.2 Maintenance Procedures

Pre-Maintenance: - Maintenance request approval - Security impact assessment - Backup verification

During Maintenance: - Supervised maintenance activities - Change documentation - Security monitoring

Post-Maintenance: - System verification - Security testing - Documentation update

31.2.3 2.3 Remote Maintenance

Remote Access Controls: - MFA required - Session logging - Encrypted connections - Time-limited access

31.3 3. Implementation Status

Status: [TODO: Implemented / Partially Implemented / Planned]

Dokumenthistorie:

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

ewpage

Chapter 32

Medienschutz-Richtlinie

Dokument-ID: NIST-0510
Kontrollfamilie: Medienschutz (MP)
Kontrolle: MP-1
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

32.1 1. Kontrollbeschreibung

MP-1 Medienschutz-Richtlinie und -Verfahren

Die Organisation entwickelt, dokumentiert und verbreitet Medienschutz-Richtlinien und -Verfahren.

32.2 2. Kontrollimplementierung

32.2.1 2.1 Medienschutz-Richtlinie

Richtlinienumfang: [TODO: Definieren Sie Richtlinienumfang]

Richtlinieninhalte: - Medientypen und Klassifizierung - Medienzugriffskontrolle - Medienkennzeichnung - Medienspeicherung - Medientransport - Medienbereinigung - Medienentsorgung

[TODO: Detaillieren Sie Richtlinieninhalte]

32.2.2 2.2 Verfahren

Verfahrensdokumentation: [TODO: Beschreiben Sie Verfahren]

32.2.3 2.3 Überprüfung und Aktualisierung

Überprüfungshäufigkeit: [TODO: z.B. Jährlich]
Aktualisierungsauslöser: [TODO: Definieren Sie Auslöser]

32.3 3. Kontrollerweiterungen

Keine Erweiterungen für MP-1.

32.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

32.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 33

Medienzugriff und Bereinigung

Dokument-ID: NIST-0520
Kontrollfamilie: Medienschutz (MP)
Kontrollen: MP-2, MP-3, MP-4, MP-5, MP-6, MP-7
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

33.1 1. Kontrollbeschreibung

Dieses Dokument umfasst Medienschutzkontrollen für Zugriff, Kennzeichnung, Speicherung, Transport, Bereinigung und Verwendung.

33.2 2. Kontrollimplementierung

33.2.1 2.1 Medienzugriff (MP-2)

Zugriffsbeschränkungen: [TODO: Definieren Sie Zugriffsbeschränkungen]

33.2.2 2.2 Medienkennzeichnung (MP-3)

Kennzeichnungsanforderungen: [TODO: Definieren Sie Kennzeichnungsanforderungen]

33.2.3 2.3 Medienspeicherung (MP-4)

Speicheranforderungen: [TODO: Definieren Sie Speicheranforderungen]

33.2.4 2.4 Medientransport (MP-5)

Transportverfahren: [TODO: Definieren Sie Transportverfahren]

33.2.5 2.5 Medienbereinigung (MP-6)

Bereinigungsmethoden: - Löschen - Überschreiben - Physische Zerstörung

[TODO: Definieren Sie Bereinigungsmethoden]

33.2.6 2.6 Medienverwendung (MP-7)

Verwendungsbeschränkungen: [TODO: Definieren Sie Verwendungsbeschränkungen]

33.3 3. Kontrollerweiterungen

- **MP-2(1):** Automatisierte Zugriffsbeschränkungen
- **MP-3(1):** Automatisierte Kennzeichnung
- **MP-4(1):** Kryptografischer Schutz
- **MP-5(4):** Kryptografischer Schutz
- **MP-6(1):** Überprüfung der Bereinigung
- **MP-6(2):** Gerätebereinigung
- **MP-6(3):** Nicht zerstörbare Medien
- **MP-7(1):** Verbot ohne Eigentümer
- **MP-7(2):** Verbot der Verwendung ohne Sicherheit

[TODO: Markieren Sie zutreffende Erweiterungen]

33.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

33.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 34

Physischer und Umgebungsschutz-Richtlinie

Dokument-ID: NIST-0530
Kontrollfamilie: Physischer und Umgebungsschutz (PE)
Kontrolle: PE-1
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

34.1 1. Kontrollbeschreibung

PE-1 Physischer und Umgebungsschutz-Richtlinie und -Verfahren

Die Organisation entwickelt, dokumentiert und verbreitet Richtlinien und Verfahren für physischen und Umgebungsschutz.

34.2 2. Kontrollimplementierung

34.2.1 2.1 Richtlinie

Richtlinienumfang: [TODO: Definieren Sie Richtlinienumfang]

Richtlinieninhalte: - Physische Zugriffskontrolle - Besucherverwaltung - Umgebungskontrollen - Notfallbeleuchtung - Brandschutz - Wasserschadenschutz

[TODO: Detaillieren Sie Richtlinieninhalte]

34.2.2 2.2 Verfahren

Verfahrensdokumentation: [TODO: Beschreiben Sie Verfahren]

34.2.3 2.3 Überprüfung und Aktualisierung

Überprüfungshäufigkeit: [TODO: z.B. Jährlich]
Aktualisierungsauslöser: [TODO: Definieren Sie Auslöser]

34.3 3. Kontrollerweiterungen

Keine Erweiterungen für PE-1.

34.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

34.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 35

Physische Zugriffskontrolle

Dokument-ID: NIST-0540
Kontrollfamilie: Physischer und Umgebungsschutz (PE)
Kontrollen: PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

35.1 1. Kontrollbeschreibung

Dieses Dokument umfasst physische Zugriffskontrollmaßnahmen.

35.2 2. Kontrollimplementierung

35.2.1 2.1 Physische Zugriffsautorisierungen (PE-2)

Autorisierungsverfahren: [TODO: Definieren Sie Autorisierungsverfahren]

35.2.2 2.2 Physische Zugriffskontrolle (PE-3)

Kontrollmechanismen: [TODO: Beschreiben Sie Kontrollmechanismen]

35.2.3 2.3 Zugriffskontrolle für Übertragung (PE-4)

Übertragungsschutz: [TODO: Definieren Sie Schutzmaßnahmen]

35.2.4 2.4 Zugriffskontrolle für Ausgabegeräte (PE-5)

Ausgabegeräteschutz: [TODO: Definieren Sie Schutzmaßnahmen]

35.2.5 2.5 Überwachung des physischen Zugriffs (PE-6)

Überwachungsmechanismen: [TODO: Beschreiben Sie Überwachungsmechanismen]

35.2.6 2.6 Besucherzugangsaufzeichnungen (PE-8)

Aufzeichnungsverfahren: [TODO: Definieren Sie Aufzeichnungsverfahren]

35.3 3. Kontrollerweiterungen

- **PE-2(1):** Zugriff durch Position/Rolle
- **PE-2(2):** Zwei Formen der Identifizierung
- **PE-3(1):** Informationssystem-Zugriff
- **PE-3(2):** Einrichtungs-/Informationssystem-Grenzen
- **PE-3(3):** Kontinuierliche Bewachung/Alarme/Überwachung
- **PE-6(1):** Intrusion-Alarme/Überwachungsgeräte
- **PE-6(4):** Überwachung physischer Zugriffe

[TODO: Markieren Sie zutreffende Erweiterungen]

35.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

35.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 36

Umgebungskontrollen

Dokument-ID: NIST-0550
Kontrollfamilie: Physischer und Umgebungsschutz (PE)
Kontrollen: PE-12, PE-13, PE-14, PE-15
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

36.1 1. Kontrollbeschreibung

Dieses Dokument umfasst Umgebungsschutzkontrollen.

36.2 2. Kontrollimplementierung

36.2.1 2.1 Notbeleuchtung (PE-12)

Notbeleuchtungsanforderungen: [TODO: Definieren Sie Anforderungen]

36.2.2 2.2 Brandschutz (PE-13)

Brandschutzmaßnahmen: [TODO: Beschreiben Sie Maßnahmen]

36.2.3 2.3 Umgebungskontrollen (PE-14)

Temperatur- und Feuchtigkeitskontrolle: [TODO: Definieren Sie Kontrollen]

36.2.4 2.4 Wasserschadenschutz (PE-15)

Schutzmaßnahmen: [TODO: Beschreiben Sie Schutzmaßnahmen]

36.3 3. Kontrollerweiterungen

- **PE-12(1):** Wesentliche Missionen/Geschäftsfunktionen
- **PE-13(1):** Erkennung/Unterdrückung/Eindämmung
- **PE-13(2):** Unterdrückungssysteme - Automatische Aktivierung
- **PE-13(3):** Automatische Benachrichtigungen
- **PE-14(1):** Automatische Kontrollen
- **PE-14(2):** Überwachung mit Alarmen

[TODO: Markieren Sie zutreffende Erweiterungen]

36.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

36.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 37

Security Planning Policy

Dokument-ID: NIST-0600
Control Family: Planning (PL)
Control: PL-1, PL-2
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Letzte Aktualisierung: {{ meta.document.last_updated }}

37.1 1. Control Description

PL-1 Policy and Procedures
PL-2 System Security Plan

The organization develops and maintains a System Security Plan (SSP).

37.2 2. Control Implementation

37.2.1 2.1 System Security Plan

SSP Components: - System identification - System categorization - Security control selection - Control implementation - Roles and responsibilities - Interconnections

SSP Maintenance: - Annual review - Update upon significant changes - AO approval required

37.3 3. Implementation Status

Status: [TODO: Implemented / Partially Implemented / Planned]
SSP Document: See NIST-0021

Dokumenthistorie:

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

ewpage

Chapter 38

Risikobewertungs-Richtlinie

Dokument-ID: NIST-0610
Kontrollfamilie: Risikobewertung (RA)
Kontrolle: RA-1
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

38.1 1. Kontrollbeschreibung

RA-1 Risikobewertungs-Richtlinie und -Verfahren

Die Organisation entwickelt, dokumentiert und verbreitet Risikobewertungs-Richtlinien und -Verfahren.

38.2 2. Kontrollimplementierung

38.2.1 2.1 Risikobewertungs-Richtlinie

Richtlinienumfang: [TODO: Definieren Sie Richtlinienumfang]

Richtlinieninhalte: - Risikobewertungsmethodik - Risikobewertungshäufigkeit - Risikoakzeptanzkriterien - Risikominderungsstrategien

[TODO: Detaillieren Sie Richtlinieninhalte]

38.2.2 2.2 Verfahren

Verfahrensdokumentation: [TODO: Beschreiben Sie Verfahren]

38.2.3 2.3 Überprüfung und Aktualisierung

Überprüfungshäufigkeit: [TODO: z.B. Jährlich]
Aktualisierungsauslöser: [TODO: Definieren Sie Auslöser]

38.3 3. Kontrollerweiterungen

Keine Erweiterungen für RA-1.

38.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

38.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 39

Risikobewertung und Schwachstellenmanagement

Dokument-ID: NIST-0620
Kontrollfamilie: Risikobewertung (RA)
Kontrollen: RA-3, RA-5, RA-7
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

39.1 1. Kontrollbeschreibung

Dieses Dokument umfasst Risikobewertung und Schwachstellenmanagement.

39.2 2. Kontrollimplementierung

39.2.1 2.1 Risikobewertung (RA-3)

Bewertungsmethodik: [TODO: Beschreiben Sie Methodik]

Bewertungshäufigkeit: [TODO: Definieren Sie Häufigkeit]

39.2.2 2.2 Schwachstellenüberwachung und -scanning (RA-5)

Scanning-Verfahren: [TODO: Beschreiben Sie Verfahren]

Schwachstellenbehebung: [TODO: Definieren Sie Behebungsverfahren]

39.2.3 2.3 Risikoantwort (RA-7)

Risikoantwortstrategien: - Risikovermeidung - Risikominderung - Risikoübertragung - Risikoakzeptanz

[TODO: Beschreiben Sie Strategien]

39.3 3. Kontrollerweiterungen

- **RA-3(1):** Supply Chain-Risikobewertung
- **RA-3(2):** Verwendung von All-Source-Intelligence
- **RA-3(3):** Dynamische Bedrohungsbewusstsein
- **RA-5(1):** Update-Tool-Fähigkeit
- **RA-5(2):** Update durch Häufigkeit/vor neuen Scans/wenn identifiziert
- **RA-5(3):** Breite/Tiefe der Abdeckung
- **RA-5(4):** Entdeckbare Informationen
- **RA-5(5):** Privilegierter Zugriff
- **RA-5(6):** Automatisierte Trendanalysen
- **RA-5(8):** Überprüfung historischer Audit-Logs

[TODO: Markieren Sie zutreffende Erweiterungen]

39.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

39.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 40

System- und Dienstleistungsbeschaffungs-Richtlinie

Dokument-ID: NIST-0630
Kontrollfamilie: System- und Dienstleistungsbeschaffung (SA)
Kontrollen: SA-1, SA-2, SA-3, SA-4, SA-8, SA-10, SA-15, SA-17
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

40.1 1. Kontrollbeschreibung

Dieses Dokument umfasst System- und Dienstleistungsbeschaffungskontrollen.

40.2 2. Kontrollimplementierung

40.2.1 2.1 Richtlinie und Verfahren (SA-1)

Richtlinienumfang: [TODO: Definieren Sie Richtlinienumfang]

40.2.2 2.2 Ressourcenzuweisung (SA-2)

Ressourcenplanung: [TODO: Beschreiben Sie Ressourcenplanung]

40.2.3 2.3 System-Entwicklungslebenszyklus (SA-3)

SDLC-Phasen: [TODO: Definieren Sie SDLC-Phasen]

40.2.4 2.4 Beschaffungsprozess (SA-4)

Beschaffungsanforderungen: [TODO: Definieren Sie Anforderungen]

40.2.5 2.5 Sicherheits- und Datenschutz-Engineering-Prinzipien (SA-8)

Engineering-Prinzipien: [TODO: Beschreiben Sie Prinzipien]

40.2.6 2.6 Entwickler-Konfigurationsmanagement (SA-10)

Konfigurationsmanagement: [TODO: Beschreiben Sie Verfahren]

40.2.7 2.7 Entwicklungsprozess, Standards und Tools (SA-15)

Entwicklungsstandards: [TODO: Definieren Sie Standards]

40.2.8 2.8 Entwickler-Sicherheits- und Datenschutzarchitektur (SA-17)

Architekturanforderungen: [TODO: Definieren Sie Anforderungen]

40.3 3. Kontrollerweiterungen

- **SA-3(1):** Verwaltung von Sicherheits- und Datenschutzfunktionen
- **SA-3(2):** Sicherheits- und Datenschutzarchitektur
- **SA-3(3):** Sicherheits- und Datenschutz-Engineering-Prinzipien
- **SA-4(1):** Funktionale Eigenschaften der Sicherheits- und Datenschutzkontrollen
- **SA-4(2):** Design-/Implementierungsinformationen für Sicherheits- und Datenschutzkontrollen
- **SA-4(9):** Funktionen/Ports/Protokolle/Dienste im Einsatz
- **SA-4(10):** Verwendung von genehmigten PIV-Produkten
- **SA-8(1):** Klare Abstraktion
- **SA-10(1):** Software-/Firmware-Integritätsüberprüfung
- **SA-15(1):** Qualitätsmetriken
- **SA-15(3):** Kritikalitätsanalyse
- **SA-15(7):** Automatisierte Schwachstellenanalyse
- **SA-17(1):** Formale Richtlinienmodell-Überprüfung
- **SA-17(2):** Sicherheitsrelevante Komponenten

[TODO: Markieren Sie zutreffende Erweiterungen]

40.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

40.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 41

Entwickler-Tests und Schulung

Dokument-ID: NIST-0640
Kontrollfamilie: System- und Dienstleistungsbeschaffung (SA)
Kontrollen: SA-11, SA-16
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

41.1 1. Kontrollbeschreibung

SA-11 Entwickler-Tests und -Bewertung

Die Organisation verlangt, dass der Entwickler Tests und Bewertungen durchführt.

SA-16 Vom Entwickler bereitgestellte Schulung

Die Organisation verlangt, dass der Entwickler Schulungen bereitstellt.

41.2 2. Kontrollimplementierung

41.2.1 2.1 Entwickler-Tests (SA-11)

Testanforderungen: [TODO: Definieren Sie Testanforderungen]

Testtypen: - Unit-Tests - Integrationstests - Systemtests - Sicherheitstests

[TODO: Beschreiben Sie Testtypen]

41.2.2 2.2 Entwickler-Schulung (SA-16)

Schulungsanforderungen: [TODO: Definieren Sie Schulungsanforderungen]

41.3 3. Kontrollerweiterungen

- **SA-11(1):** Statische Code-Analyse
- **SA-11(2):** Bedrohungs- und Schwachstellenanalysen
- **SA-11(3):** Unabhängige Überprüfung von Bewertungsplänen/-beweisen
- **SA-11(4):** Manuelle Code-Reviews
- **SA-11(5):** Penetrationstests
- **SA-11(8):** Dynamische Code-Analyse

[TODO: Markieren Sie zutreffende Erweiterungen]

41.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

41.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 42

Supply-Chain-Risikomanagement

Dokument-ID: NIST-0650
Kontrollfamilie: Supply-Chain-Risikomanagement (SR)
Kontrollen: SR-1, SR-2, SR-3, SR-5, SR-6, SR-8, SR-10, SR-11
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

42.1 1. Kontrollbeschreibung

Dieses Dokument umfasst Supply-Chain-Risikomanagementkontrollen.

42.2 2. Kontrollimplementierung

42.2.1 2.1 Richtlinie und Verfahren (SR-1)

Richtlinienumfang: [TODO: Definieren Sie Richtlinienumfang]

42.2.2 2.2 Supply-Chain-Risikomanagementplan (SR-2)

Plankomponenten: [TODO: Beschreiben Sie Plankomponenten]

42.2.3 2.3 Supply-Chain-Kontrollen und -Prozesse (SR-3)

Kontrollmaßnahmen: [TODO: Definieren Sie Kontrollmaßnahmen]

42.2.4 2.4 Beschaffungsstrategien, Tools und Methoden (SR-5)

Beschaffungsstrategien: [TODO: Beschreiben Sie Strategien]

42.2.5 2.5 Lieferantenbewertungen und -überprüfungen (SR-6)

Bewertungsverfahren: [TODO: Definieren Sie Verfahren]

42.2.6 2.6 Benachrichtigungsvereinbarungen (SR-8)

Benachrichtigungsanforderungen: [TODO: Definieren Sie Anforderungen]

42.2.7 2.7 Inspektion von Systemen oder Komponenten (SR-10)

Inspektionsverfahren: [TODO: Beschreiben Sie Verfahren]

42.2.8 2.8 Komponentenauthentizität (SR-11)

Authentizitätsprüfung: [TODO: Definieren Sie Prüfverfahren]

42.3 3. Kontrollerweiterungen

- **SR-2(1):** Etablierung von SCRM-Team
- **SR-3(1):** Vielfalt der Lieferanten
- **SR-3(2):** Begrenzung von Schäden
- **SR-5(1):** Angemessene Sicherheit
- **SR-5(2):** Vertrauenswürdige Lieferanten
- **SR-6(1):** Tests und Analysen
- **SR-10(1):** Mehrere Phasen des SDLC
- **SR-11(1):** Anti-Fälschungsschulung
- **SR-11(2):** Konfigurationskontrolle für Komponentenauthentizität
- **SR-11(3):** Anti-Fälschungsscans

[TODO: Markieren Sie zutreffende Erweiterungen]

42.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

42.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 43

System and Communications Protection

Dokument-ID: NIST-0700
Control Family: System and Communications Protection (SC)
Control: SC-1, SC-7, SC-8, SC-13
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Letzte Aktualisierung: {{ meta.document.last_updated }}

43.1 1. Control Description

SC-1 Policy and Procedures
SC-7 Boundary Protection
SC-8 Transmission Confidentiality and Integrity
SC-13 Cryptographic Protection

The organization protects system and communications.

43.2 2. Control Implementation

43.2.1 2.1 Boundary Protection

Network Boundaries: - Firewalls - DMZ - Network segmentation - Intrusion detection/prevention

43.2.2 2.2 Cryptographic Protection

Encryption Standards: - Data at rest: [TODO: AES-256] - Data in transit: [TODO: TLS 1.2+] - Key management: [TODO: Process]

43.2.3 2.3 Transmission Protection

Protected Channels: - VPN for remote access - TLS for web traffic - SSH for administrative access

43.3 3. Implementation Status

Status: [TODO: Implemented / Partially Implemented / Planned]

Dokumenthistorie:

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

ewpage

Chapter 44

Netzwerksicherheit und Grenzschutz

Dokument-ID: NIST-0710
Kontrollfamilie: System- und Kommunikationsschutz (SC)
Kontrollen: SC-5, SC-7, SC-20, SC-21, SC-22
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

44.1 1. Kontrollbeschreibung

Dieses Dokument umfasst Netzwerksicherheits- und Grenzschutzkontrollen.

44.2 2. Kontrollimplementierung

44.2.1 2.1 Denial-of-Service-Schutz (SC-5)

Schutzmaßnahmen: [TODO: Beschreiben Sie Schutzmaßnahmen]

44.2.2 2.2 Grenzschutz (SC-7)

Grenzschutzgeräte: - Firewalls - Intrusion Detection/Prevention Systems - Web Application Firewalls - Network Access Control

[TODO: Beschreiben Sie Grenzschutzimplementierung]

44.2.3 2.3 Sichere Namens-/Adressauflösungsdienste (SC-20, SC-21, SC-22)

DNS-Sicherheit: [TODO: Beschreiben Sie DNS-Sicherheitsmaßnahmen]

44.3 3. Kontrollerweiterungen

- **SC-5(1):** Verfügbarkeit von Ressourcen
- **SC-5(2):** Überschusskapazität/Bandbreite/Redundanz
- **SC-5(3):** Erkennung/Überwachung
- **SC-7(3):** Zugriffspunkte
- **SC-7(4):** Externe Telekommunikationsdienste
- **SC-7(5):** Verweigerung standardmäßig/Erlauben nach Ausnahme
- **SC-7(7):** Split-Tunneling für Remote-Geräte verhindern
- **SC-7(8):** Route-Verkehr zu authentifizierten Proxy-Servern
- **SC-7(10):** Verhindern unbefugter Exfiltration
- **SC-7(11):** Einschränkung eingehender Kommunikation
- **SC-7(12):** Host-basierte Schutzmaßnahmen
- **SC-7(18):** Fehler sicher
- **SC-7(20):** Dynamische Isolation/Segregation
- **SC-7(21):** Isolation von Informationssystemkomponenten
- **SC-20(1):** Kindersicherheit
- **SC-20(2):** Datenherkunft und Integritätsschutz
- **SC-21(1):** Datenherkunft und Integritätsschutz
- **SC-22(1):** Autorisierung von Namensauflösungsdiensten

[TODO: Markieren Sie zutreffende Erweiterungen]

44.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

44.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

Version	Datum	Autor	Änderungen
0.1	{{ meta.document.last_updated | default('') }}	{{ meta.defaults.author }}	Ersterstellung

ewpage

Chapter 45

Kryptografischer Schutz

Dokument-ID: NIST-0720
Kontrollfamilie: System- und Kommunikationsschutz (SC)
Kontrollen: SC-8, SC-12, SC-13, SC-17, SC-28
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

45.1 1. Kontrollbeschreibung

Dieses Dokument umfasst kryptografische Schutzkontrollen.

45.2 2. Kontrollimplementierung

45.2.1 2.1 Übertragungsvertraulichkeit und -integrität (SC-8)

Übertragungsschutz: [TODO: Beschreiben Sie Übertragungsschutzmaßnahmen]

45.2.2 2.2 Kryptografische Schlüsseletablierung und -verwaltung (SC-12)

Schlüsselverwaltung: [TODO: Beschreiben Sie Schlüsselverwaltungsverfahren]

45.2.3 2.3 Kryptografischer Schutz (SC-13)

Kryptografische Mechanismen: [TODO: Beschreiben Sie verwendete kryptografische Mechanismen]

45.2.4 2.4 Public-Key-Infrastruktur-Zertifikate (SC-17)

PKI-Implementierung: [TODO: Beschreiben Sie PKI-Implementierung]

45.2.5 2.5 Schutz von Informationen im Ruhezustand (SC-28)

Verschlüsselung im Ruhezustand: [TODO: Beschreiben Sie Verschlüsselungsmaßnahmen]

45.3 3. Kontrollerweiterungen

- **SC-8(1):** Kryptografischer Schutz
- **SC-8(2):** Vorhandene Sicherheitsattribute
- **SC-12(1):** Verfügbarkeit
- **SC-12(2):** Symmetrische Schlüssel
- **SC-12(3):** Asymmetrische Schlüssel
- **SC-12(6):** Physische Kontrolle von kryptografischen Schlüsseln
- **SC-13(1):** FIPS-validierte Kryptografie
- **SC-17(1):** Zertifikatsstatus-Informationen
- **SC-17(2):** Zertifikatsstatus-Validierung
- **SC-28(1):** Kryptografischer Schutz
- **SC-28(2):** Offline-Speicherung

[TODO: Markieren Sie zutreffende Erweiterungen]

45.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

45.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 46

System- und Informationsintegritäts-Richtlinie

Dokument-ID: NIST-0730
Kontrollfamilie: System- und Informationsintegrität (SI)
Kontrolle: SI-1, SI-6, SI-7, SI-10, SI-11, SI-12, SI-16
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

46.1 1. Kontrollbeschreibung

Dieses Dokument umfasst System- und Informationsintegritätskontrollen.

46.2 2. Kontrollimplementierung

46.2.1 2.1 Richtlinie und Verfahren (SI-1)

Richtlinienumfang: [TODO: Definieren Sie Richtlinienumfang]

46.2.2 2.2 Sicherheits- und Datenschutzfunktionsüberprüfung (SI-6)

Überprüfungsverfahren: [TODO: Beschreiben Sie Überprüfungsverfahren]

46.2.3 2.3 Software-, Firmware- und Informationsintegrität (SI-7)

Integritätsschutzmaßnahmen: [TODO: Beschreiben Sie Schutzmaßnahmen]

46.2.4 2.4 Informationseingabevalidierung (SI-10)

Validierungsverfahren: [TODO: Beschreiben Sie Validierungsverfahren]

46.2.5 2.5 Fehlerbehandlung (SI-11)

Fehlerbehandlungsverfahren: [TODO: Beschreiben Sie Verfahren]

46.2.6 2.6 Informationsmanagement und -aufbewahrung (SI-12)

Aufbewahrungsrichtlinien: [TODO: Definieren Sie Aufbewahrungsrichtlinien]

46.2.7 2.7 Speicherschutz (SI-16)

Speicherschutzmaßnahmen: [TODO: Beschreiben Sie Schutzmaßnahmen]

46.3 3. Kontrollerweiterungen

- **SI-6(1):** Benachrichtigung bei anomalem Verhalten
- **SI-6(2):** Automatisierung zur Unterstützung der Reaktion auf Anomalien
- **SI-6(3):** Automatisierte Reaktion auf Integritätsverletzungen
- **SI-7(1):** Integritätsprüfungen
- **SI-7(2):** Automatisierte Benachrichtigungen bei Integritätsverletzungen
- **SI-7(5):** Automatisierte Reaktion auf Integritätsverletzungen
- **SI-7(6):** Kryptografischer Schutz
- **SI-7(7):** Integration der Erkennung und Reaktion
- **SI-7(10):** Schutz vor unbefugten Änderungen an Software und Informationen
- **SI-7(15):** Code-Authentifizierung
- **SI-7(16):** Zeit-Limit für Prozessausführung ohne Überwachung
- **SI-10(1):** Manuelle Überschreibung
- **SI-10(2):** Überprüfung von Informationseingaben
- **SI-10(3):** Vorhersagbares Verhalten
- **SI-11(1):** Warnung und Fehlerbehandlung
- **SI-16(1):** Hardware-erzwungene Trennung

[TODO: Markieren Sie zutreffende Erweiterungen]

46.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

46.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 47

Fehlerbehebung

Dokument-ID: NIST-0740
Kontrollfamilie: System- und Informationsintegrität (SI)
Kontrollen: SI-2, SI-5
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

47.1 1. Kontrollbeschreibung

SI-2 Fehlerbehebung

Die Organisation identifiziert, meldet und korrigiert Informationssystemfehler.

SI-5 Sicherheitswarnungen, -hinweise und -anweisungen

Die Organisation empfängt Sicherheitswarnungen, -hinweise und -anweisungen und ergreift Maßnahmen.

47.2 2. Kontrollimplementierung

47.2.1 2.1 Fehlerbehebungsprozess (SI-2)

Fehleridentifikation: [TODO: Beschreiben Sie Identifikationsverfahren]

Patch-Management: [TODO: Beschreiben Sie Patch-Management-Verfahren]

Fehlerbehebungszeitrahmen: [TODO: Definieren Sie Zeitrahmen]

47.2.2 2.2 Sicherheitswarnungen (SI-5)

Warnungsquellen: [TODO: Listen Sie Warnungsquellen auf]

Reaktionsverfahren: [TODO: Beschreiben Sie Reaktionsverfahren]

47.3 3. Kontrollerweiterungen

- **SI-2(1):** Zentrale Verwaltung
- **SI-2(2):** Automatisierte Fehlerbehebungsstatus
- **SI-2(3):** Zeit zur Behebung/Benchmark für Korrekturmaßnahmen
- **SI-2(4):** Automatisierte Patch-Management-Tools
- **SI-2(5):** Automatische Software-/Firmware-Updates
- **SI-2(6):** Entfernung früherer Versionen von Software/Firmware
- **SI-5(1):** Automatisierte Warnungen und Hinweise

[TODO: Markieren Sie zutreffende Erweiterungen]

47.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

47.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 48

Schadcode-Schutz und Systemüberwachung

Dokument-ID: NIST-0750
Kontrollfamilie: System- und Informationsintegrität (SI)
Kontrollen: SI-3, SI-4, SI-8
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

48.1 1. Kontrollbeschreibung

Dieses Dokument umfasst Schadcode-Schutz und Systemüberwachungskontrollen.

48.2 2. Kontrollimplementierung

48.2.1 2.1 Schadcode-Schutz (SI-3)

Schutzmaßnahmen: - Antivirus-Software - Anti-Malware-Software - Endpoint Detection and Response (EDR) - Verhaltensanalyse

[TODO: Beschreiben Sie Schutzmaßnahmen]

48.2.2 2.2 Systemüberwachung (SI-4)

Überwachungsmechanismen: - Intrusion Detection Systems (IDS) - Intrusion Prevention Systems (IPS) - Security Information and Event Management (SIEM) - Network Traffic Analysis

[TODO: Beschreiben Sie Überwachungsmechanismen]

48.2.3 2.3 Spam-Schutz (SI-8)

Spam-Schutzmaßnahmen: [TODO: Beschreiben Sie Spam-Schutzmaßnahmen]

48.3 3. Kontrollerweiterungen

- **SI-3(1):** Zentrale Verwaltung
- **SI-3(2):** Automatische Updates
- **SI-3(4):** Updates nur von autorisierten Quellen
- **SI-3(6):** Tests/Überprüfung
- **SI-3(7):** Nicht signierte Malware-Erkennung
- **SI-3(8):** Erkennung und Eradikation
- **SI-3(10):** Schadcode-Analyse
- **SI-4(1):** Systemweite Intrusion Detection
- **SI-4(2):** Automatisierte Tools für Echtzeitanalyse
- **SI-4(4):** Eingehende und ausgehende Kommunikationsverkehr
- **SI-4(5):** Systemgenerierte Warnungen
- **SI-4(7):** Automatisierte Reaktion auf verdächtige Ereignisse
- **SI-4(10):** Sichtbarkeit nicht autorisierter Netzwerkaktivitäten
- **SI-4(11):** Analyse von ausgehender Kommunikation auf ungewöhnliche/nicht autorisierte Aktivitäten
- **SI-4(12):** Automatisierte Warnungen
- **SI-4(16):** Korrelation von Überwachungsinformationen
- **SI-4(18):** Analyse von Verkehr/Ereignismustern
- **SI-4(20):** Privilegierte Benutzer
- **SI-4(22):** Host-basierte Geräte
- **SI-4(23):** Host-basierte Geräte mit automatisierten Mechanismen
- **SI-8(1):** Zentrale Verwaltung
- **SI-8(2):** Automatische Updates
- **SI-8(3):** Kontinuierliches Lernen

[TODO: Markieren Sie zutreffende Erweiterungen]

48.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

48.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen, Testen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 49

Control Traceability Matrix

Dokument-ID: NIST-0800
Organisation: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Review / Freigegeben
Letzte Aktualisierung: {{ meta.document.last_updated }}

49.1 1. Zweck

Dieses Dokument bietet eine Rückverfolgbarkeitsmatrix für alle NIST 800-53 Sicherheitskontrollen des Systems {{ meta.nist.system_name }}.

49.2 2. Control Traceability Matrix

Control ID	Control Name	Baseline	Implementation Status	Document Reference	Assessment Status
AC-1	Access Control Policy	Low	Implemented	NIST-0100	Satisfied
AC-2	Account Management	Low	Implemented	NIST-0110	Satisfied
AT-1	Awareness and Training Policy	Low	Implemented	NIST-0200	Satisfied
AU-1	Audit and Accountability Policy	Low	Implemented	NIST-0220	Satisfied

Control ID	Control Name	Baseline	Implementation Status	Document Reference	Assessment Status
CM-1	Configuration Management Policy	Low	Implemented	NIST-0300	Satisfied
CP-1	Contingency Planning Policy	Low	Implemented	NIST-0330	Satisfied
IA-1	Identification and Authentication Policy	Low	Implemented	NIST-0400	Satisfied
IR-1	Incident Response Policy	Low	Implemented	NIST-0430	Satisfied
MA-1	Maintenance Policy	Low	Implemented	NIST-0500	Satisfied
PL-1	Planning Policy	Low	Implemented	NIST-0600	Satisfied
SC-1	System Protection Policy	Low	Implemented	NIST-0700	Satisfied
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

49.3 3. Control Summary

Total Controls: [TODO: Number]
Implemented: [TODO: Number / Percentage]
Partially Implemented: [TODO: Number / Percentage]
Planned: [TODO: Number / Percentage]
Not Applicable: [TODO: Number / Percentage]

49.4 4. Control Families Coverage

Control Family	Total Controls	Implemented	Percentage
Access Control (AC)	[TODO]	[TODO]	[TODO]%
Awareness and Training (AT)	[TODO]	[TODO]	[TODO]%
Audit and Accountability (AU)	[TODO]	[TODO]	[TODO]%
Configuration Management (CM)	[TODO]	[TODO]	[TODO]%
Contingency Planning (CP)	[TODO]	[TODO]	[TODO]%
Identification and Authentication (IA)	[TODO]	[TODO]	[TODO]%
Incident Response (IR)	[TODO]	[TODO]	[TODO]%
Maintenance (MA)	[TODO]	[TODO]	[TODO]%
Planning (PL)	[TODO]	[TODO]	[TODO]%
System Protection (SC)	[TODO]	[TODO]	[TODO]%

Dokumenthistorie:

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

ewpage

Chapter 50

Kontrollbewertungsverfahren

Dokument-ID: NIST-0810
Kontrollfamilie: Bewertung, Autorisierung und Überwachung (CA)
Kontrolle: CA-2
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

50.1 1. Kontrollbeschreibung

CA-2 Kontrollbewertungen

Die Organisation entwickelt einen Kontrollbewertungsplan und bewertet die Sicherheits- und Datenschutzkontrollen.

50.2 2. Kontrollimplementierung

50.2.1 2.1 Bewertungsplan

Plankomponenten: - Bewertungsumfang - Bewertungsmethoden - Bewertungszeitplan - Bewertungsteam - Bewertungsverfahren

[TODO: Entwickeln Sie Bewertungsplan]

50.2.2 2.2 Bewertungsmethoden

Methoden: - Prüfen (Examine): Dokumentenprüfung - Befragen (Interview): Interviews mit Personal - Testen (Test): Funktionale Tests

[TODO: Definieren Sie Bewertungsmethoden]

50.2.3 2.3 Bewertungsdurchführung

Bewertungsverfahren: [TODO: Beschreiben Sie Bewertungsverfahren]

50.2.4 2.4 Bewertungsberichterstattung

Berichtskomponenten: - Bewertungsergebnisse - Feststellungen - Empfehlungen - Korrekturmaßnahmen

[TODO: Definieren Sie Berichtsanforderungen]

50.3 3. Kontrollerweiterungen

- **CA-2(1):** Unabhängige Bewerter
- **CA-2(2):** Spezialisierte Bewertungen
- **CA-2(3):** Externe Organisationen
- **CA-7(1):** Unabhängige Bewertung
- **CA-7(3):** Trendanalysen

[TODO: Markieren Sie zutreffende Erweiterungen]

50.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

50.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 51

Maßnahmenplan und Meilensteine

Dokument-ID: NIST-0820
Kontrollfamilie: Bewertung, Autorisierung und Überwachung (CA)
Kontrollen: CA-5, PM-4
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

51.1 1. Kontrollbeschreibung

CA-5 Plan of Action and Milestones (POA&M)

Die Organisation entwickelt einen Plan of Action and Milestones für das Informationssystem.

PM-4 Plan of Action and Milestones Process

Die Organisation implementiert einen Prozess für Plan of Action and Milestones.

51.2 2. Kontrollimplementierung

51.2.1 2.1 POA&M-Entwicklung

POA&M-Komponenten: - Identifizierte Schwachstellen/Mängel - Geplante Korrekturmaßnahmen - Verantwortliche Personen - Meilensteine - Ressourcen - Abschlussdaten - Status

[TODO: Entwickeln Sie POA&M-Vorlage]

51.2.2 2.2 POA&M-Verwaltung

Verwaltungsverfahren: - Regelmäßige Überprüfungen - Statusaktualisierungen - Eskalationsverfahren - Abschlussverfahren

[TODO: Definieren Sie Verwaltungsverfahren]

51.2.3 2.3 POA&M-Berichterstattung

Berichterstattungsanforderungen: [TODO: Definieren Sie Berichterstattungsanforderungen]

51.3 3. Kontrollerweiterungen

- **CA-5(1):** Automatisierung zur Unterstützung von POA&M-Management

[TODO: Markieren Sie zutreffende Erweiterungen]

51.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

51.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 52

Datenschutzkontrollen

Dokument-ID: NIST-0830
Kontrollfamilie: Datenschutzkontrollen (PT, AP, AR, DI, DM, IP, SE, TR, UL)
Kontrollen: PT-1, AP-1, AR-1, DI-1, DM-1, IP-1, SE-1, TR-1, UL-1
Organisation: AdminSend GmbH
Verantwortlich: IT Operations Manager
Version: 1.0.0
Status: Entwurf / In Prüfung / Genehmigt
Letzte Aktualisierung: {{ meta.document.last_updated }}

52.1 1. Kontrollbeschreibung

Dieses Dokument umfasst Datenschutzkontrollen aus verschiedenen Kontrollfamilien.

52.2 2. Kontrollimplementierung

52.2.1 2.1 Datenschutzrichtlinie und -verfahren (PT-1)

Richtlinienumfang: [TODO: Definieren Sie Datenschutzrichtlinienumfang]

52.2.2 2.2 Befugnis zur Erhebung (AP-1)

Erhebungsbefugnis: [TODO: Dokumentieren Sie Erhebungsbefugnis]

52.2.3 2.3 Governance und Datenschutzprogramm (AR-1)

Programmstruktur: [TODO: Beschreiben Sie Datenschutzprogrammstruktur]

52.2.4 2.4 Datenqualität (DI-1)

Qualitätssicherung: [TODO: Definieren Sie Datenqualitätsmaßnahmen]

52.2.5 2.5 Minimierung personenbezogener Daten (DM-1)

Minimierungsprinzipien: [TODO: Beschreiben Sie Minimierungsprinzipien]

52.2.6 2.6 Einwilligung (IP-1)

Einwilligungsverfahren: [TODO: Definieren Sie Einwilligungsverfahren]

52.2.7 2.7 Inventar personenbezogener Daten (SE-1)

Inventarverfahren: [TODO: Beschreiben Sie Inventarverfahren]

52.2.8 2.8 Datenschutzhinweis (TR-1)

Hinweisanforderungen: [TODO: Definieren Sie Datenschutzhinweisanforderungen]

52.2.9 2.9 Interne Verwendung (UL-1)

Verwendungsbeschränkungen: [TODO: Definieren Sie interne Verwendungsbeschränkungen]

52.3 3. Kontrollerweiterungen

- **PT-1(1):** Datenschutz-Folgenabschätzung
- **AP-1(1):** Befugnis zur Verarbeitung
- **AR-1(1):** Datenschutzbeauftragter
- **DI-1(1):** Datenqualitätsbewertung
- **DI-1(2):** Datenqualitätskorrektur
- **DM-1(1):** Datenminimierungspraktiken
- **IP-1(1):** Mechanismen zur Einwilligung
- **SE-1(1):** Datenflussdiagramme
- **TR-1(1):** Echtzeit-Benachrichtigung
- **UL-1(1):** Interne Zugriffskontrollen

[TODO: Markieren Sie zutreffende Erweiterungen]

52.4 4. Implementierungsstatus

Status: [TODO: Implementiert / Teilweise implementiert / Geplant / Nicht zutreffend]
Implementierungsdatum: [TODO: Datum]
Verantwortlich: [TODO: Name/Rolle]

52.5 5. Bewertung

Bewertungsmethode: Prüfen, Befragen
Bewertungsstatus: [TODO: Erfüllt / Nicht erfüllt / Nicht zutreffend]
Feststellungen: [TODO: Beschreibung]

Dokumentenhistorie:

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

ewpage

Chapter 53

Glossar und Abkürzungen

Dokument-ID: NIST-0850
Organisation: AdminSend GmbH
Version: 1.0.0
Letzte Aktualisierung: {{ meta.document.last_updated }}

53.1 1. Abkürzungen

Abkürzung	Bedeutung
AC	Access Control
AO	Authorizing Official
AT	Awareness and Training
ATO	Authorization to Operate
AU	Audit and Accountability
CA	Assessment, Authorization, and Monitoring
CDE	Cardholder Data Environment
CM	Configuration Management
CP	Contingency Planning
FIPS	Federal Information Processing Standards
IA	Identification and Authentication
IR	Incident Response
ISCM	Information Security Continuous Monitoring
ISSO	Information System Security Officer
ISSM	Information System Security Manager
MA	Maintenance
MFA	Multi-Factor Authentication
MP	Media Protection
NIST	National Institute of Standards and Technology
PE	Physical and Environmental Protection
PL	Planning
POA&M	Plan of Action and Milestones

Abkürzung	Bedeutung
RA	Risk Assessment
RMF	Risk Management Framework
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SA	System and Services Acquisition
SAR	Security Assessment Report
SC	System and Communications Protection
SCA	Security Control Assessor
SI	System and Information Integrity
SIEM	Security Information and Event Management
SP	Special Publication
SR	Supply Chain Risk Management
SSP	System Security Plan

53.2 2. Glossar

Authorizing Official (AO): A senior official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk.

Authorization to Operate (ATO): The official management decision to authorize operation of an information system.

Baseline Configuration: A documented set of specifications for an information system that has been formally reviewed and agreed upon.

Confidentiality: Preserving authorized restrictions on information access and disclosure.

Contingency Plan: Management policy and procedures designed to maintain or restore business operations.

Control: A safeguard or countermeasure prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

FIPS 199: Federal standard for categorizing information and information systems according to an assessment of the potential impact.

High-Water Mark: The process of selecting the highest impact level from among the security objectives.

Impact Level: The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure, modification, or destruction of information.

Information System Security Officer (ISSO): Individual responsible for the security posture of an information system.

Integrity: Guarding against improper information modification or destruction.

Multi-Factor Authentication (MFA): Authentication using two or more different factors to achieve authentication.

Plan of Action and Milestones (POA&M): A document that identifies tasks needing to be accomplished to correct weaknesses.

Risk Management Framework (RMF): A structured approach for integrating security and risk management activities into the system development life cycle.

Security Assessment Report (SAR): A report documenting the results of a security control assessment.

Security Control: A safeguard or countermeasure prescribed for an information system.

System Security Plan (SSP): A formal document that provides an overview of the security requirements for an information system.

Dokumenthistorie:

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

ewpage