Contents

Chapter 1

Informationssicherheitsleitlinie (Top-Management)

Dokument-ID: 0010
Dokumenttyp: Leitlinie/Policy
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

1.1 1. Zweck und Zielsetzung

Die Informationssicherheitsleitlinie von **AdminSend GmbH** definiert die strategischen Ziele und Grundsätze für den Schutz von Informationen und IT-Systemen.

1.1.1 1.1 Ziel der Informationssicherheit

AdminSend GmbH verpflichtet sich, die Informationssicherheit als integralen Bestandteil der Unternehmensführung zu etablieren. Ziel ist der angemessene Schutz aller Informationswerte vor Bedrohungen und Risiken.

[TODO: Spezifische Sicherheitsziele der Organisation ergänzen]

1.1.2 1.2 Schutzwerte

Die Informationssicherheit von **AdminSend GmbH** basiert auf folgenden Schutzzielen:

- **Vertraulichkeit:** Schutz vor unbefugter Offenlegung von Informationen
- **Integrität:** Schutz vor unbefugter Veränderung von Informationen
- **Verfügbarkeit:** Sicherstellung der Verfügbarkeit von Informationen und Systemen
- **Authentizität:** Sicherstellung der Echtheit und Glaubwürdigkeit von Informationen

- **Nachvollziehbarkeit:** Sicherstellung der Rückverfolgbarkeit von Aktionen

1.2 2. Geltungsbereich

1.2.1 2.1 Organisation und Standorte

Diese Leitlinie gilt für:

- **Organisation:** AdminSend GmbH
- **Standorte:** {{ meta.organization.locations }}
- **Geschäftsführung:** Max Mustermann
- **Informationssicherheitsbeauftragter (ISB):** Thomas Weber

1.2.2 2.2 Informationsverbünde im Scope

[TODO: Definieren Sie die im Scope befindlichen Informationsverbünde]

Beispiele: - IT-Infrastruktur und Netzwerke - Geschäftsanwendungen und Datenbanken - Cloud-Services und externe Dienstleister - Mobile Endgeräte und Remote-Arbeitsplätze

1.2.3 2.3 Ausnahmen

[TODO: Dokumentieren Sie explizite Ausnahmen vom Geltungsbereich]

1.3 3. Grundsätze

1.3.1 3.1 Risikobasierter Ansatz

AdminSend GmbH verfolgt einen risikobasierten Ansatz zur Informationssicherheit gemäß BSI Standard 200-3. Sicherheitsmaßnahmen werden auf Basis einer systematischen Risikoanalyse und -bewertung implementiert.

1.3.2 3.2 Verantwortlichkeiten und Ressourcen

Die Geschäftsführung stellt sicher, dass: - Klare Verantwortlichkeiten für Informationssicherheit definiert sind - Ausreichende Ressourcen (Personal, Budget, Zeit) bereitgestellt werden - Informationssicherheit in allen Geschäftsprozessen berücksichtigt wird

1.3.3 3.3 Kontinuierliche Verbesserung

Das Informationssicherheits-Managementsystem (ISMS) wird kontinuierlich überwacht, bewertet und verbessert. Regelmäßige Reviews und Audits stellen die Wirksamkeit sicher.

1.3.4 3.4 Verpflichtung zur Einhaltung

AdminSend GmbH verpflichtet sich zur Einhaltung: - Gesetzlicher und regulatorischer Anforderungen (DSGVO, IT-Sicherheitsgesetz, etc.) - Vertraglicher Verpflichtungen gegenüber Kunden und Partnern - Interner Richtlinien und Standards - BSI IT-Grundschutz-Anforderungen

1.4 4. Verantwortlichkeiten

1.4.1 4.1 Top-Management / Geschäftsführung

Verantwortlich: Max Mustermann (max.mustermann@adminsend.de)

Die Geschäftsführung trägt die Gesamtverantwortung für Informationssicherheit und: - Genehmigt die Informationssicherheitsleitlinie - Stellt Ressourcen bereit - Fördert die Sicherheitskultur - Überwacht die ISMS-Leistung

1.4.2 4.2 Informationssicherheitsbeauftragter (ISB)

Verantwortlich: Thomas Weber (thomas.weber@adminsend.de)

Der ISB ist verantwortlich für: - Koordination des ISMS - Beratung der Geschäftsführung - Überwachung der Sicherheitsmaßnahmen - Durchführung von Risikoanalysen - Incident Management Koordination

1.4.3 4.3 IT-Leitung

Verantwortlich: Anna Schmidt (anna.schmidt@adminsend.de)

Die IT-Leitung ist verantwortlich für: - Umsetzung technischer Sicherheitsmaßnahmen - Betrieb sicherer IT-Systeme - Patch- und Vulnerability Management - Technische Incident Response

1.4.4 4.4 Informationsverbund-Verantwortliche

[TODO: Definieren Sie Verantwortliche für spezifische Informationsverbünde]

1.4.5 4.5 Alle Mitarbeitenden

Alle Mitarbeitenden sind verpflichtet: - Sicherheitsrichtlinien einzuhalten - Sicherheitsvorfälle zu melden - An Schulungen teilzunehmen - Verantwortungsvoll mit Informationen umzugehen

1.5 5. Kommunikation und Durchsetzung

1.5.1 5.1 Kommunikation der Leitlinie

Diese Leitlinie wird kommuniziert durch: - Veröffentlichung im Intranet - Schulungen und Awareness-Programme - Onboarding neuer Mitarbeitender - Regelmäßige Erinnerungen und Updates

1.5.2 5.2 Konsequenzen bei Verstößen

Verstöße gegen diese Leitlinie können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

1.6 6. Review und Aktualisierung

Diese Leitlinie wird mindestens jährlich oder bei wesentlichen Änderungen überprüft und aktualisiert.

Nächster Review: {{ meta.document.next_review }}

1.7 7. Freigabe

Rolle	Name	Datum	Freigabe
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI Standard 200-1: Managementsysteme für Informationssicherheit (ISMS) - BSI Standard 200-2: IT-Grundschutz-Methodik - BSI Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz - BSI IT-Grundschutz-Kompendium

ewpage

Chapter 2

ISMS-Organisation, Rollen und Verantwortlichkeiten

Dokument-ID: 0020
Dokumenttyp: Grundlagendokument
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

2.1 1. ISMS-Organisation

2.1.1 1.1 ISMS-Owner/Sponsor

Verantwortlich: Max Mustermann (max.mustermann@adminsend.de)

Der ISMS-Owner trägt die Gesamtverantwortung für das Informationssicherheits-Managementsystem und stellt sicher, dass: - Ausreichende Ressourcen bereitgestellt werden - Die Informationssicherheitsleitlinie genehmigt wird - Strategische Entscheidungen zur Informationssicherheit getroffen werden - Das ISMS in die Geschäftsprozesse integriert wird

2.1.2 1.2 Informationssicherheitsbeauftragter (ISB)

Verantwortlich: Thomas Weber (thomas.weber@adminsend.de)

Der ISB ist die zentrale Koordinationsstelle für alle Informationssicherheitsaktivitäten: - Koordination und Steuerung des ISMS - Beratung der Geschäftsführung und Fachabteilungen - Durchführung von Risikoanalysen und Sicherheitsbewertungen - Überwachung der Umsetzung von Sicherheitsmaßnahmen - Berichterstattung an die Geschäftsführung - Koordination von Sicherheitsvorfällen - Durchführung von Awareness-Maßnahmen

2.1.3 1.3 ISMS-Team / Informationssicherheitsgremium

Das ISMS-Team unterstützt den ISB bei der Umsetzung des ISMS:

Rolle	Name	Verantwortungsbereich
ISB (Leitung)	Thomas Weber	Gesamtkoordination ISMS
IT-Leitung	Anna Schmidt	Technische Sicherheitsmaßnahmen
Datenschutzbeauftragter	[TODO]	Datenschutz-Schnittstelle
BCM-Verantwortlicher	[TODO]	Business Continuity
Risk Manager	[TODO]	Risikomanagement
HR-Vertreter	[TODO]	Personal- und Awareness-Themen
Legal/Compliance	[TODO]	Rechtliche Anforderungen

Sitzungsrhythmus: [TODO: z.B. monatlich, quartalsweise]

2.1.4 1.4 Schnittstellen zu anderen Bereichen

2.1.4.1 1.4.1 IT Service Management (ITSM)

Ansprechpartner: Anna Schmidt

Schnittstellen: - Change Management: Sicherheitsbewertung von Changes - Incident Management: Sicherheitsvorfälle - Problem Management: Sicherheitsschwachstellen - Configuration Management: Asset-Inventar

2.1.4.2 1.4.2 Datenschutz

Ansprechpartner: [TODO: Datenschutzbeauftragter]

Schnittstellen: - Verzeichnis von Verarbeitungstätigkeiten (VVT) - Datenschutz-Folgenabschätzung (DSFA) - Technische und organisatorische Maßnahmen (TOM) - Meldung von Datenschutzverletzungen

2.1.4.3 1.4.3 Business Continuity Management (BCM)

Ansprechpartner: [TODO: BCM-Verantwortlicher]

Schnittstellen: - Business Impact Analysis (BIA) - IT-Disaster Recovery Pläne - Notfallübungen und Tests - Krisenmanagement

2.1.4.4 1.4.4 Risikomanagement

Ansprechpartner: [TODO: Risk Manager]

Schnittstellen: - Unternehmensweites Risikomanagement - Risikoregister und -bewertung - Risikoreporting - Risikoakzeptanz-Entscheidungen

2.1.4.5 1.4.5 Internal Audit

Ansprechpartner: [TODO: Internal Audit]

Schnittstellen: - ISMS-Audits - Compliance-Prüfungen - Nachverfolgung von Audit-Findings - Berichterstattung an Management

2.2 2. Rollen und Verantwortlichkeiten

2.2.1 2.1 Informationsverbund-Verantwortliche/r

Rolle: Verantwortlich für einen spezifischen Informationsverbund (z.B. Geschäftsanwendung, IT-System)

Aufgaben: - Definition des Geltungsbereichs des Informationsverbunds - Durchführung der Strukturanalyse - Schutzbedarfsfeststellung - Modellierung und Bausteinzuordnung - Koordination der Maßnahmenumsetzung - Überwachung der Sicherheit des Informationsverbunds

[TODO: Benennen Sie spezifische Informationsverbund-Verantwortliche]

2.2.2 2.2 Asset Owner / System Owner

Rolle: Verantwortlich für spezifische Assets oder IT-Systeme

Aufgaben: - Klassifizierung und Bewertung von Assets - Definition von Sicherheitsanforderungen - Genehmigung von Zugriffsrechten - Überwachung der Asset-Nutzung - Entscheidung über Außerbetriebnahme

[TODO: Definieren Sie Asset Owner für kritische Systeme]

2.2.3 2.3 Maßnahme-/Control-Owner

Rolle: Verantwortlich für die Umsetzung spezifischer Sicherheitsmaßnahmen

Aufgaben: - Implementierung zugewiesener Sicherheitsmaßnahmen - Dokumentation der Umsetzung - Nachweis der Wirksamkeit - Kontinuierliche Überwachung und Verbesserung

[TODO: Zuordnung von Maßnahmen-Verantwortlichen]

2.2.4 2.4 Administratoren / Betreiber

Rolle: Technische Umsetzung und Betrieb von IT-Systemen

Aufgaben: - Konfiguration und Härtung von Systemen - Patch- und Update-Management - Monitoring und Logging - Backup und Recovery - Incident Response (technisch)

Verantwortlich: Anna Schmidt (IT-Leitung)

2.2.5 2.5 Alle Mitarbeitenden

Rolle: Nutzer von IT-Systemen und Informationen

Aufgaben: - Einhaltung von Sicherheitsrichtlinien - Meldung von Sicherheitsvorfällen - Teilnahme an Schulungen - Verantwortungsvoller Umgang mit Informationen - Schutz von Zugangsdaten

2.3 3. RACI-Matrix für BSI IT-Grundschutz-Prozesse

Aktivität	Geschäfts-führung	ISB	IT-Leitung	Informations-verbund-Verantwortliche	Fach-abteilungen	Internal Audit
Strukturanalyse	I	A	C	R	C	I
Schutzbedarfsfeststellung	A	C	C	R	C	I
Modellierung (Bausteinzuordnung)	I	A	C	R	C	I
Basis-Sicherheitscheck	I	A	C	R	C	I
Risikoanalyse (BSI 200-3)	A	R	C	C	C	I
Maßnahmenplanung	A	R	C	C	C	I
Maßnahmenumsetzung	I	C	R	R	R	I
Wirksamkeitsprüfung	I	A	C	R	C	I
ISMS-Audit	I	C	C	C	C	R/A
Management Review	A	R	C	I	I	C
Incident Management	I	A	R	C	C	I
Awareness-Schulungen	I	A	C	C	R	I
Dokumentation	I	A	R	R	C	I

2.4 4. Eskalationswege

2.4.1 4.1 Operative Eskalation

1. **Level 1:** Informationsverbund-Verantwortliche / System Owner
2. **Level 2:** ISB / IT-Leitung
3. **Level 3:** Geschäftsführung

2.4.2 4.2 Sicherheitsvorfälle

1. **Meldung:** Alle Mitarbeitenden → ISB / IT-Leitung
2. **Bewertung:** ISB / IT-Leitung
3. **Eskalation (bei Major Incidents):** Geschäftsführung
4. **Externe Meldung (falls erforderlich):** BSI, Datenschutzbehörde, Strafverfolgung

2.5 5. Kommunikation und Berichtswesen

2.5.1 5.1 Regelmäßige Berichte

Bericht	Frequenz	Ersteller	Empfänger
ISMS-Status-Report	Monatlich	ISB	Geschäftsführung, ISMS-Team
Sicherheitsvorfälle	Monatlich	ISB	Geschäftsführung
Risiko-Dashboard	Quartalsweise	ISB	Geschäftsführung
Management Review	Jährlich	ISB	Geschäftsführung
Audit-Ergebnisse	Nach Audit	Internal Audit	Geschäftsführung, ISB

2.5.2 5.2 Ad-hoc Kommunikation

- **Sicherheitsvorfälle:** Sofortige Meldung an ISB
- **Kritische Schwachstellen:** Sofortige Meldung an ISB und IT-Leitung
- **Compliance-Verstöße:** Meldung an ISB und Legal/Compliance

2.6 6. Ressourcen und Budget

[TODO: Definieren Sie Budget und Ressourcen für ISMS-Aktivitäten]

- **ISMS-Budget:** [TODO]
- **Personalressourcen:** [TODO]
- **Externe Unterstützung:** [TODO]
- **Tools und Systeme:** [TODO]

2.7 7. Review und Aktualisierung

Diese Organisationsstruktur wird mindestens jährlich oder bei wesentlichen Änderungen überprüft und aktualisiert.

Nächster Review: {{ meta.document.next_review }}

Referenzen: - BSI Standard 200-1: Managementsysteme für Informationssicherheit (ISMS) - BSI Standard 200-2: IT-Grundschutz-Methodik - BSI IT-Grundschutz-Kompendium

ewpage

Chapter 3

Dokumentenlenkung und Dokumentenregister

Dokument-ID: 0030
Dokumenttyp: Prozess/Grundlage
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

3.1 1. Zweck und Geltungsbereich

Dieses Dokument beschreibt die Dokumentenlenkung für das Informationssicherheits-Managementsystem (ISMS) von **AdminSend GmbH**. Es definiert Prozesse für Erstellung, Review, Freigabe, Verteilung, Änderung und Archivierung von ISMS-Dokumenten.

3.1.1 1.1 Geltungsbereich

Diese Dokumentenlenkung gilt für alle ISMS-relevanten Dokumente: - Leitlinien und Policies - Richtlinien und Prozessbeschreibungen - Sicherheitskonzepte und Risikoanalysen - Arbeitsanweisungen und Checklisten - Protokolle und Nachweise

3.2 2. Ablage und Zugriff

3.2.1 2.1 Offizieller Ablageort

Primärer Ablageort: [TODO: z.B. SharePoint, Confluence, DMS]

Verantwortlich: IT Operations Manager

Alle ISMS-Dokumente werden zentral abgelegt in: - **Pfad:** [TODO: z.B. /ISMS/Dokumentation/] - **Backup:** [TODO: Backup-Strategie] - **Versionierung:** Automatische Versionierung aktiviert

3.2.2 2.2 Zugriffskontrolle (RBAC)

Zugriff auf ISMS-Dokumente erfolgt rollenbasiert:

Rolle	Lesen	Schreiben	Freigeben	Löschen
Geschäftsführung				
ISB				
ISMS-Team				
Informationsverbund-Verantwortliche		(eigene Dokumente)		
Alle Mitarbeitenden	(öffentliche Dokumente)			

3.2.3 2.3 Klassifizierung und Schutzbedarf

Klassifizierung	Beschreibung	Zugriff	Beispiele
Öffentlich	Keine Vertraulichkeit	Alle Mitarbeitenden	Awareness-Material
Intern	Nur für interne Nutzung	Alle Mitarbeitenden	Policies, Richtlinien
Vertraulich	Eingeschränkter Zugriff	ISMS-Team, Berechtigte	Risikoanalysen, Sicherheitskonzepte
Streng vertraulich	Höchste Vertraulichkeit	Geschäftsführung, ISB	Incident-Berichte, Audit-Findings

3.2.4 2.4 Notfallzugriff

Im Notfall (z.B. Ausfall des ISB) haben folgende Personen Zugriff auf alle ISMS-Dokumente: - **Geschäftsführung:** Max Mustermann - **IT-Leitung:** Anna Schmidt - **Stellvertretender ISB:** [TODO]

3.3 3. Dokumentenlebenszyklus

3.3.1 3.1 Erstellung

Prozess: 1. **Initiierung:** Bedarf wird identifiziert (ISB, ISMS-Team, Fachabteilung) 2. **Erstellung:** Autor erstellt Dokument basierend auf Template 3. **Qualitätssicherung:** Peer-Review durch ISMS-Team 4. **Freigabe:** Freigabe durch zuständige Rolle (siehe Freigabematrix)

Verantwortlich: Dokumentautor, ISB (Koordination)

3.3.2 3.2 Review und Freigabe

3.3.2.1 3.2.1 Freigabematrix

Dokumenttyp	Ersteller	Reviewer	Genehmiger
Leitlinien/Policies	ISB	ISMS-Team	Geschäftsführung
Richtlinien	ISB, Fachabteilung	ISMS-Team	ISB
Sicherheitskonzepte	Informationsverbund-Verantwortliche	ISB	ISB
Arbeitsanweisungen	Fachabteilung	ISB	IT-Leitung
Risikoanalysen	ISB	ISMS-Team	Geschäftsführung

3.3.2.2 3.2.2 Review-Intervalle

Dokumenttyp	Review-Intervall	Verantwortlich
Leitlinien/Policies	Jährlich	ISB
Richtlinien	Jährlich	ISB
Sicherheitskonzepte	Jährlich oder bei Änderungen	Informationsverbund-Verantwortliche
Arbeitsanweisungen	Jährlich	Fachabteilung
Risikoanalysen	Jährlich oder bei wesentlichen Änderungen	ISB

Zusätzliche Review-Trigger: - Wesentliche Änderungen in der IT-Infrastruktur - Neue gesetzliche Anforderungen - Sicherheitsvorfälle - Audit-Findings - Organisatorische Änderungen

3.3.3 3.3 Versionierung

Versionierungsschema: - **Major Version (X.0):** Wesentliche inhaltliche Änderungen, neue Freigabe erforderlich - **Minor Version (X.Y):** Kleinere Anpassungen, redaktionelle Änderungen

Beispiel: - Version 1.0: Initiale Freigabe - Version 1.1: Kleinere Anpassungen - Version 2.0: Wesentliche Überarbeitung

3.3.4 3.4 Verteilung und Kommunikation

Verteilungsprozess: 1. Freigabe des Dokuments 2. Veröffentlichung im zentralen Ablageort 3. Benachrichtigung betroffener Stakeholder (E-Mail, Intranet) 4. Schulung/Awareness (falls erforderlich) 5. Bestätigung der Kenntnisnahme (bei kritischen Dokumenten)

Verantwortlich: ISB

3.3.5 3.5 Änderungsmanagement

Prozess für Änderungen: 1. **Änderungsantrag:** Initiator stellt Änderungsantrag an ISB 2. **Bewertung:** ISB bewertet Änderungsbedarf und Auswirkungen 3. **Genehmigung:** Genehmigung durch zuständige Rolle 4. **Umsetzung:** Autor aktualisiert Dokument 5. **Review:** Review durch ISMS-Team 6. **Freigabe:** Freigabe gemäß Freigabematrix 7. **Verteilung:** Kommunikation der Änderungen

3.3.6 3.6 Archivierung und Löschung

Archivierung: - Alte Versionen werden für [TODO: z.B. 5 Jahre] archiviert - Archivierte Dokumente sind schreibgeschützt - Zugriff nur für ISB und Audit

Löschung: - Dokumente werden nach Ablauf der Aufbewahrungsfrist gelöscht - Löschung erfolgt gemäß Datenschutz- und Compliance-Anforderungen - Löschprotokoll wird geführt

Verantwortlich: ISB

3.4 4. Dokumentenregister

Dokument	ID	Owner	Status	Version	Letzte Aktualisierung	Nächster Review
Informationssicherheitsleitlinie	0010	Thomas Weber	{{ meta.document.status }}	1.0.0	{{ meta.document.last_updated }}	{{ meta.document.next_revie
ISMS-Organisation, Rollen und RACI	0020	Thomas Weber	{{ meta.document.status }}	1.0.0	{{ meta.document.last_updated }}	{{ meta.document.next_revie
Dokumentenlenkung	0030	Thomas Weber	{{ meta.document.status }}	1.0.0	{{ meta.document.last_updated }}	{{ meta.document.next_revie
[TODO: Weitere Dokumente ergänzen]						

3.5 5. Änderungsprotokoll

Version	Datum	Änderung	Autor	Genehmiger	Status
0.1	{{ meta.document.last_updated }}	Erster Entwurf	IT Operations Manager	-	Entwurf
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

3.6 6. Qualitätssicherung

3.6.1 6.1 Dokumentenqualität

Alle ISMS-Dokumente müssen folgende Qualitätskriterien erfüllen: - **Vollständigkeit:** Alle erforderlichen Inhalte vorhanden - **Korrektheit:** Inhaltlich korrekt und aktuell - **Verständlichkeit:** Klar und verständlich formuliert - **Konsistenz:** Konsistent mit anderen ISMS-Dokumenten - **Nachvollziehbarkeit:** Änderungen nachvollziehbar dokumentiert

3.6.2 6.2 Dokumenten-Templates

Für alle Dokumenttypen existieren Templates mit: - Standardisiertem Header (Metadaten) - Strukturvorgaben - Platzhaltern für variable Inhalte - Hinweisen für Autoren

Ablageort Templates: [TODO: z.B. /ISMS/Templates/]

3.7 7. Schulung und Awareness

Alle Dokumentautoren und ISMS-Team-Mitglieder werden geschult in: - Dokumentenlenkungsprozess - Verwendung von Templates - Versionierung und Änderungsmanagement - Klassifizierung und Schutzbedarf

Verantwortlich: ISB

3.8 8. Überwachung und Verbesserung

Der Dokumentenlenkungsprozess wird regelmäßig überwacht: - **Metriken:** Anzahl Dokumente, Review-Compliance, Änderungsrate - **Review:** Jährliche Überprüfung des Prozesses - **Verbesserung:** Kontinuierliche Optimierung basierend auf Feedback

Nächster Review: {{ meta.document.next_review }}

Referenzen: - BSI Standard 200-1: Managementsysteme für Informationssicherheit (ISMS) - BSI Standard 200-2: IT-Grundschutz-Methodik

ewpage

Chapter 4

Geltungsbereich und Informationsverbund (Abgrenzung)

Dokument-ID: 0040
Dokumenttyp: Grundlagendokument
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

4.1 1. Zweck und Zielsetzung

Dieses Dokument definiert den Geltungsbereich des Informationssicherheits-Managementsystems (ISMS) von **AdminSend GmbH** und grenzt den Informationsverbund ab. Die klare Definition des Scopes ist Grundlage für alle weiteren IT-Grundschutz-Aktivitäten (Strukturanalyse, Schutzbedarfsfeststellung, Modellierung).

4.2 2. Scope-Definition

4.2.1 2.1 Organisationseinheiten und Standorte

Organisation: AdminSend GmbH

Standorte im Scope:

Standort	Adresse	Typ	Mitarbeitende	Im Scope
{{ meta.organization.primary_location }}	[TODO]	Hauptstandort	[TODO]	

Standort	Adresse	Typ	Mitarbeitende	Im Scope
[TODO: Weitere Standorte]	[TODO]	[TODO]	[TODO]	/

Organisationseinheiten im Scope: - Geschäftsführung - IT-Abteilung - [TODO: Weitere Abteilungen]

4.2.2 2.2 Geschäftsprozesse und Services

Kritische Geschäftsprozesse im Scope:

Prozess	Beschreibung	Kritikalität	Owner	Im Scope
[TODO: Prozess 1]	[TODO]	Hoch/Mittel/Niedrig	[TODO]	
[TODO: Prozess 2]	[TODO]	Hoch/Mittel/Niedrig	[TODO]	

IT-Services im Scope:

Service	Beschreibung	Nutzer	Service Owner	Im Scope
[TODO: Service 1]	[TODO]	[TODO]	Anna Schmidt	
[TODO: Service 2]	[TODO]	[TODO]	Anna Schmidt	

4.2.3 2.3 IT-Infrastruktur

IT-Systeme im Scope:

4.2.3.1 2.3.1 On-Premise IT

Kategorie	Systeme	Anzahl	Im Scope
Server	{{ netbox.device.servers }}	[TODO]	
Netzwerk	{{ netbox.device.network }}	[TODO]	
Storage	{{ netbox.device.storage }}	[TODO]	
Clients	Workstations, Laptops	[TODO]	
Mobile Devices	Smartphones, Tablets	[TODO]	

4.2.3.2 2.3.2 Cloud-Services

Cloud-Service	Provider	Typ (IaaS/PaaS/SaaS)	Im Scope
[TODO: Cloud Service 1]	[TODO]	[TODO]	
[TODO: Cloud Service 2]	[TODO]	[TODO]	

4.2.3.3 2.3.3 OT/IoT (falls zutreffend)

OT/IoT-System	Beschreibung	Standort	Im Scope
[TODO: OT System 1]	[TODO]	[TODO]	/

4.2.4 2.4 Anwendungen und Daten

Geschäftsanwendungen im Scope:

Anwendung	Typ	Kritikalität	Datenklassifizierung	Im Scope
[TODO: Anwendung 1]	[TODO]	Hoch/Mittel/Niedrig	Vertraulich/Intern	
[TODO: Anwendung 2]	[TODO]	Hoch/Mittel/Niedrig	Vertraulich/Intern	

Datenarten im Scope: - Personenbezogene Daten (DSGVO-relevant) - Geschäftsgeheimnisse - Kundendaten - Finanzdaten - [TODO: Weitere Datenarten]

4.3 3. Abgrenzung des Informationsverbunds

4.3.1 3.1 In Scope

Folgende Elemente sind im Scope des ISMS:

1. **Infrastruktur:**
   - Alle Server und Netzwerkkomponenten an Standort {{ meta.organization.primary_location }}
   - [TODO: Weitere Infrastruktur]
2. **Anwendungen:**
   - Alle geschäftskritischen Anwendungen
   - [TODO: Spezifische Anwendungen]
3. **Daten:**
   - Alle personenbezogenen Daten
   - Alle Geschäftsdaten mit Klassifizierung “Vertraulich” oder höher
   - [TODO: Weitere Daten]
4. **Personen:**
   - Alle Mitarbeitenden von AdminSend GmbH
   - Externe Dienstleister mit Zugriff auf Scope-Systeme
   - [TODO: Weitere Personengruppen]
5. **Prozesse:**
   - Alle IT-Betriebsprozesse
   - Alle geschäftskritischen Prozesse
   - [TODO: Weitere Prozesse]

4.3.2 3.2 Out of Scope

Folgende Elemente sind NICHT im Scope des ISMS:

Element	Begründung	Risikobewertung	Schnittstellen zum Scope
[TODO: Out-of-Scope Element 1]	[TODO: Begründung]	[TODO: Risiko]	[TODO: Schnittstellen]
[TODO: Out-of-Scope Element 2]	[TODO: Begründung]	[TODO: Risiko]	[TODO: Schnittstellen]

Wichtig: Auch Out-of-Scope-Elemente müssen hinsichtlich ihrer Risiken für den Scope bewertet werden, insbesondere wenn Schnittstellen bestehen.

4.3.3 3.3 Begründung der Abgrenzung

[TODO: Erläutern Sie die Gründe für die gewählte Scope-Abgrenzung]

Beispiele für Begründungen: - Fokus auf kritische Geschäftsprozesse - Ressourcenbeschränkungen (schrittweise Erweiterung geplant) - Externe Verantwortung (z.B. ausgelagerte Prozesse) - Geringe Kritikalität

4.4 4. Schnittstellen und Abhängigkeiten

4.4.1 4.1 Externe Dienstleister und Provider

Dienstleister	Service	Kritikalität	Vertragliche Regelungen	Sicherheitsanforderungen
[TODO: Provider 1]	[TODO]	Hoch/Mittel/Niedrig	[TODO: Vertrag vorhanden]	[TODO: SLA, Zertifizierungen]
[TODO: Provider 2]	[TODO]	Hoch/Mittel/Niedrig	[TODO: Vertrag vorhanden]	[TODO: SLA, Zertifizierungen]

4.4.2 4.2 Kritische Schnittstellen

Schnittstellen zwischen Scope und Out-of-Scope:

Schnittstelle	Von (Scope)	Nach (Out-of-Scope)	Datenfluss	Sicherheitsmaßnahmen
[TODO: Schnittstelle 1]	[TODO]	[TODO]	[TODO]	[TODO: Verschlüsselung, Firewall, etc.]
[TODO: Schnittstelle 2]	[TODO]	[TODO]	[TODO]	[TODO]

Schnittstellen zu externen Partnern:

Informationsverbund-Diagramm

Figure 4.1: Informationsverbund-Diagramm

Partner	Zweck	Datenarten	Sicherheitsmaßnahmen
[TODO: Partner 1]	[TODO]	[TODO]	[TODO]
[TODO: Partner 2]	[TODO]	[TODO]	[TODO]

4.4.3 4.3 Abhängigkeiten

Kritische Abhängigkeiten des Scopes:

Abhängigkeit	Typ	Auswirkung bei Ausfall	Mitigationsmaßnahmen
Internetanbindung	Externe Infrastruktur	[TODO]	[TODO: Redundanz, Backup-Leitung]
Stromversorgung	Externe Infrastruktur	[TODO]	[TODO: USV, Notstrom]
[TODO: Weitere Abhängigkeiten]	[TODO]	[TODO]	[TODO]

4.5 5. Informationsverbund-Diagramm

Diagramm-Legende: - **Grüne Linie:** Scope-Grenze (im ISMS) - **Rote Linie:** Out-of-Scope-Grenze - **Blaue Pfeile:** Datenflüsse - **Gelbe Symbole:** Kritische Schnittstellen

[TODO: Erstellen Sie ein Diagramm des Informationsverbunds]

4.6 6. Scope-Änderungen

4.6.1 6.1 Änderungsprozess

Änderungen am Scope erfordern: 1. **Antrag:** Formaler Änderungsantrag an ISB 2. **Bewertung:** Bewertung der Auswirkungen (Risiken, Ressourcen, Compliance) 3. **Genehmigung:** Genehmigung durch Geschäftsführung 4. **Umsetzung:** Aktualisierung aller betroffenen Dokumente 5. **Kommunikation:** Information aller Stakeholder

Verantwortlich: Thomas Weber (ISB)

4.6.2 6.2 Scope-Review

Der Scope wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Trigger:** Neue Geschäftsprozesse, IT-Systeme, Standorte, regulatorische Anforderungen - **Verantwortlich:** ISB

Nächster Review: {{ meta.document.next_review }}

4.7 7. Dokumentation und Nachweise

Folgende Dokumente und Nachweise werden für den Scope geführt: - Dieses Scope-Dokument - Informationsverbund-Diagramm - Asset-Inventar (siehe Anhang 0710) - Datenfluss-Diagramme (siehe Anhang 0720) - Verträge mit externen Dienstleistern - Scope-Änderungsprotokolle

4.8 8. Freigabe

Rolle	Name	Datum	Freigabe
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI Standard 200-1: Managementsysteme für Informationssicherheit (ISMS) - BSI Standard 200-2: IT-Grundschutz-Methodik (Kapitel 4: Festlegung des Geltungsbereichs) - BSI IT-Grundschutz-Kompendium

ewpage

Chapter 5

Strukturanalyse (Template)

Dokument-ID: 0050
Dokumenttyp: Methodik-Artefakt
Referenzrahmen: BSI IT-Grundschutz (BSI Standard 200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

5.1 1. Ziel und Zweck

Die Strukturanalyse erfasst systematisch die Struktur des Informationsverbunds von **AdminSend GmbH**. Sie bildet die Grundlage für: - Schutzbedarfsfeststellung (Dokument 0060) - Modellierung und Bausteinzuordnung (Dokument 0070) - Basis-Sicherheitscheck (Dokument 0080) - Risikoanalyse (Dokument 0090)

Verantwortlich: Thomas Weber (ISB)

5.2 2. Vorgehen und Methodik

5.2.1 2.1 Datenquellen

Folgende Datenquellen werden für die Strukturanalyse genutzt:

Datenquelle	Typ	Verantwortlich	Aktualität
CMDB/Asset-Inventar	System	Anna Schmidt	[TODO]
Netzwerkdokumentation	Dokument	Anna Schmidt	[TODO]
Architekturdiagramme	Dokument	Anna Schmidt	[TODO]
Verträge mit Dienstleistern	Dokument	[TODO]	[TODO]
Interviews mit Stakeholdern	Primärquelle	Thomas Weber	[TODO]

5.2.2 2.2 Granularität

Die Strukturanalyse erfolgt auf folgenden Granularitätsebenen:

- **Geschäftsprozesse:** Prozessebene (nicht Aktivitätsebene)
- **Anwendungen:** Anwendungssystemebene (nicht Modulebene)
- **IT-Systeme:** Logische Systeme (Server, Datenbanken, Storage)
- **Netzwerke:** Netzwerksegmente und Zonen
- **Räume:** Standorte und kritische Räume (Rechenzentrum, Serverraum)

5.2.3 2.3 Durchführung

Zeitplan: - **Start:** [TODO] - **Datenerhebung:** [TODO: z.B. 2 Wochen] - **Validierung:** [TODO: z.B. 1 Woche] - **Abschluss:** [TODO]

Beteiligte: - ISB: Thomas Weber - IT-Leitung: Anna Schmidt - Informationsverbund-Verantwortliche: [TODO] - Fachabteilungen: [TODO]

5.3 3. Struktur-Register

5.3.1 3.1 Geschäftsprozesse und Services

ID	Prozess/Service	Owner	Beschreibung	Kritikalität	Abhängigkeiten	Anwendungen
P-001	[TODO: Prozess 1]	[TODO]	[TODO]	Hoch/Mittel/Niedrig	[TODO]	[TODO: A-001, A-002]
P-002	[TODO: Prozess 2]	[TODO]	[TODO]	Hoch/Mittel/Niedrig	[TODO]	[TODO]
P-003	[TODO: Prozess 3]	[TODO]	[TODO]	Hoch/Mittel/Niedrig	[TODO]	[TODO]

Anzahl Prozesse gesamt: [TODO]

5.3.2 3.2 Anwendungen

ID	Anwendung	Owner	Zweck	Nutzergruppen	Schnittstellen	Hosting	Kritikalität
A-001	[TODO: App 1]	[TODO]	[TODO]	[TODO]	[TODO]	On-Prem/Cloud/SaaS	Hoch/Mittel/Niedrig
A-002	[TODO: App 2]	[TODO]	[TODO]	[TODO]	[TODO]	On-Prem/Cloud/SaaS	Hoch/Mittel/Niedrig
A-003	[TODO: App 3]	[TODO]	[TODO]	[TODO]	[TODO]	On-Prem/Cloud/SaaS	Hoch/Mittel/Niedrig

Anzahl Anwendungen gesamt: [TODO]

Hosting-Verteilung: - On-Premise: [TODO] - Cloud (IaaS/PaaS): [TODO] - SaaS: [TODO]

5.3.3 3.3 IT-Systeme und Komponenten

ID	System/Komponente	Typ	Owner	Standort/Region	Betrieb	IP-Adresse	Bemerkungen
S-001	{{ netbox.device.server_001 }}	Server	Anna Schmidt	{{ meta.organization.primary_location }}	Intern	{{ netbox.ipaddress.server_001 }}	[TODO]
S-002	[TODO: System 2]	Datenbank	Anna Schmidt	[TODO]	Intern/Extern	[TODO]	[TODO]
S-003	[TODO: System 3]	Storage	Anna Schmidt	[TODO]	Intern/Extern	[TODO]	[TODO]
S-004	[TODO: System 4]	Firewall	Anna Schmidt	[TODO]	Intern	[TODO]	[TODO]

Anzahl IT-Systeme gesamt: [TODO]

Systemtypen: - Server: [TODO] - Datenbanken: [TODO] - Storage: [TODO] - Netzwerkkomponenten: [TODO] - Sicherheitskomponenten: [TODO] - Clients: [TODO]

5.3.4 3.4 Netzwerke und Kommunikation

ID	Netz/Zone	Zweck	Segmentierung	Internetzugang	VLAN-ID	Betreiber	Sicherheitszone
N-001	Management-Netz	Administration	Ja	Nein	{{ netbox.vlan.management }}	Anna Schmidt	Hochsicher
N-002	Produktiv-Netz	Geschäftsanwendungen	Ja	Ja (gefiltert)	[TODO]	Anna Schmidt	Sicher
N-003	DMZ	Externe Services	Ja	Ja	[TODO]	Anna Schmidt	Mittel
N-004	Gast-WLAN	Gäste	Ja	Ja (isoliert)	[TODO]	Anna Schmidt	Niedrig

Anzahl Netzwerksegmente gesamt: [TODO]

Sicherheitszonen: - Hochsicher (Management, kritische Systeme): [TODO] - Sicher (Produktivsysteme): [TODO] - Mittel (DMZ, externe Schnittstellen): [TODO] - Niedrig (Gast-Netz): [TODO]

5.3.5 3.5 Räume und Standorte

ID	Standort/Raum	Typ	Schutzmaßnahmen	Zutritt	Betreiber	Kritikalität
R-001	{{ meta.organization.primary_location }}	Hauptstandort	[TODO]	Zugangskontrolle	AdminSend GmbH	Hoch

ID	Standort/Raum	Typ	Schutzmaßnahmen	Zutritt	Betreiber	Kritikalität
R-002	Rechenzentrum	Serverraum	Klimatisierung, Brandschutz, Zutrittskontrolle	Autorisiert	AdminSend GmbH	Hoch
R-003	[TODO: Raum 3]	[TODO]	[TODO]	[TODO]	[TODO]	Mittel/Niedrig

Anzahl Standorte gesamt: [TODO]
Anzahl kritische Räume gesamt: [TODO]

5.3.6 3.6 Externe Dienstleister und Cloud-Provider

ID	Dienstleister	Service	Kritikalität	Vertrag	Zertifizierungen	Standort	Bemerkungen
D-001	[TODO: Provider 1]	[TODO: Service]	Hoch/Mittel/Niedrig	[TODO: Vertragsnr.]	[TODO: ISO 27001, etc.]	[TODO]	[TODO]
D-002	[TODO: Provider 2]	[TODO: Service]	Hoch/Mittel/Niedrig	[TODO]	[TODO]	[TODO]	[TODO]

Anzahl Dienstleister gesamt: [TODO]

5.3.7 3.7 Personen und Rollen

Rolle	Name	Verantwortungsbereich	Kontakt	Stellvertreter
Geschäftsführung	Max Mustermann	Gesamtverantwortung	max.mustermann@adminsend.de	[TODO]
ISB	Thomas Weber	ISMS-Koordination	thomas.weber@adminsend.de	[TODO]
IT-Leitung	Anna Schmidt	IT-Betrieb	anna.schmidt@adminsend.de	[TODO]
[TODO: Weitere Rollen]	[TODO]	[TODO]	[TODO]	[TODO]

5.4 4. Abhängigkeiten und Schnittstellen

5.4.1 4.1 Interne Abhängigkeiten

Von (Quelle)	Nach (Ziel)	Typ	Kritikalität	Bemerkungen
[TODO: System A]	[TODO: System B]	Datenfluss	Hoch/Mittel/Niedrig	[TODO]

Netzwerkdiagramm

Figure 5.1: Netzwerkdiagramm

Anwendungsarchitektur

Figure 5.2: Anwendungsarchitektur

Von (Quelle)	Nach (Ziel)	Typ	Kritikalität	Bemerkungen
[TODO: Anwendung X]	[TODO: Datenbank Y]	Datenzugriff	Hoch/Mittel/Niedrig	[TODO]

5.4.2 4.2 Externe Schnittstellen

Schnittstelle	Partner/Provider	Richtung	Datenarten	Protokoll	Sicherheitsmaßnahmen
[TODO: Schnittstelle 1]	[TODO]	Eingehend/Ausgehend/Bidirektional	[TODO]	[TODO]	[TODO: VPN, TLS, etc.]
[TODO: Schnittstelle 2]	[TODO]	Eingehend/Ausgehend/Bidirektional	[TODO]	[TODO]	[TODO]

5.5 5. Diagramme und Visualisierungen

5.5.1 5.1 Netzwerkdiagramm

[TODO: Erstellen Sie ein Netzwerkdiagramm mit allen Segmenten und Zonen]

5.5.2 5.2 Anwendungsarchitektur

[TODO: Erstellen Sie ein Diagramm der Anwendungslandschaft]

5.5.3 5.3 Datenflussdiagramm

[TODO: Erstellen Sie ein Datenflussdiagramm für kritische Prozesse]

5.6 6. Validierung und Qualitätssicherung

5.6.1 6.1 Validierungsprozess

Die Strukturanalyse wird validiert durch: 1. **Review durch IT-Leitung:** Anna Schmidt 2. **Review durch Informationsverbund-Verantwortliche:** [TODO] 3. **Abgleich mit CMDB/Inventar:** [TODO: Datum] 4. **Freigabe durch ISB:** Thomas Weber

Datenflussdiagramm

Figure 5.3: Datenflussdiagramm

5.6.2 6.2 Vollständigkeitsprüfung

Kategorie	Anzahl erfasst	Vollständigkeit	Bemerkungen
Geschäftsprozesse	[TODO]	[TODO: %]	[TODO]
Anwendungen	[TODO]	[TODO: %]	[TODO]
IT-Systeme	[TODO]	[TODO: %]	[TODO]
Netzwerke	[TODO]	[TODO: %]	[TODO]
Räume	[TODO]	[TODO: %]	[TODO]
Dienstleister	[TODO]	[TODO: %]	[TODO]

5.7 7. Aktualisierung und Pflege

Die Strukturanalyse wird aktualisiert bei: - Neuen IT-Systemen oder Anwendungen - Änderungen in der Netzwerkarchitektur - Neuen Dienstleistern oder Cloud-Services - Organisatorischen Änderungen - Mindestens jährlich im Rahmen des ISMS-Reviews

Verantwortlich: Thomas Weber (ISB)
Nächster Review: {{ meta.document.next_review }}

5.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI Standard 200-2: IT-Grundschutz-Methodik (Kapitel 5: Strukturanalyse) - BSI IT-Grundschutz-Kompendium

ewpage

Chapter 6

Schutzbedarfsfeststellung (Template)

Dokument-ID: 0060
Dokumenttyp: Methodik-Artefakt
Referenzrahmen: BSI IT-Grundschutz (BSI Standard 200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

6.1 1. Ziel und Zweck

Die Schutzbedarfsfeststellung bestimmt systematisch den Schutzbedarf für Geschäftsprozesse, Informationen, Anwendungen und IT-Systeme von **AdminSend GmbH**. Sie bildet die Grundlage für: - Auswahl angemessener Sicherheitsmaßnahmen - Priorisierung von Sicherheitsinvestitionen - Risikoanalyse (Dokument 0090) - Compliance-Nachweis

Verantwortlich: Thomas Weber (ISB)

6.2 2. Schutzbedarfskategorien und Kriterien

6.2.1 2.1 Schutzziele

Die Schutzbedarfsfeststellung erfolgt für folgende Schutzziele:

6.2.1.1 2.1.1 Vertraulichkeit (Confidentiality)

Schutz vor unbefugter Offenlegung von Informationen.

Kategorie	Beschreibung	Schadensbeispiele
Normal	Begrenzte negative Auswirkungen	Geringfügige Beeinträchtigung, interne Peinlichkeit
Hoch	Beträchtliche negative Auswirkungen	Verstoß gegen Gesetze, erheblicher finanzieller Schaden, Reputationsschaden
Sehr hoch	Existenzbedrohende Auswirkungen	Existenzgefährdung, katastrophaler Reputationsschaden, strafrechtliche Konsequenzen

6.2.1.2 2.1.2 Integrität (Integrity)

Schutz vor unbefugter Veränderung von Informationen.

Kategorie	Beschreibung	Schadensbeispiele
Normal	Begrenzte negative Auswirkungen	Korrigierbare Fehler, geringe Auswirkungen auf Geschäftsprozesse
Hoch	Beträchtliche negative Auswirkungen	Erhebliche Geschäftsprozess-Störungen, finanzielle Verluste, Compliance-Verstöße
Sehr hoch	Existenzbedrohende Auswirkungen	Kritische Geschäftsprozess-Ausfälle, existenzbedrohende finanzielle Schäden

6.2.1.3 2.1.3 Verfügbarkeit (Availability)

Sicherstellung der Verfügbarkeit von Informationen und Systemen.

Kategorie	Beschreibung	Tolerierbare Ausfallzeit	Schadensbeispiele
Normal	Begrenzte negative Auswirkungen	$>$ 24 Stunden	Geringe Produktivitätsverluste, Unannehmlichkeiten
Hoch	Beträchtliche negative Auswirkungen	4-24 Stunden	Erhebliche Produktivitätsverluste, Kundenbeschwerden, finanzielle Verluste
Sehr hoch	Existenzbedrohende Auswirkungen	$<$ 4 Stunden	Kritische Geschäftsprozess-Ausfälle, massive finanzielle Verluste, Existenzgefährdung

6.2.1.4 2.1.4 Authentizität (Optional)

Sicherstellung der Echtheit und Glaubwürdigkeit von Informationen.

Kategorie	Beschreibung	Schadensbeispiele
Normal	Begrenzte negative Auswirkungen	Geringe Zweifel an Echtheit, korrigierbar
Hoch	Beträchtliche negative Auswirkungen	Erhebliche rechtliche oder finanzielle Konsequenzen
Sehr hoch	Existenzbedrohende Auswirkungen	Existenzbedrohende rechtliche oder finanzielle Konsequenzen

6.2.1.5 2.1.5 Nachvollziehbarkeit (Optional)

Sicherstellung der Rückverfolgbarkeit von Aktionen.

Kategorie	Beschreibung	Schadensbeispiele
Normal	Begrenzte negative Auswirkungen	Erschwerte Fehlersuche, geringe Compliance-Risiken
Hoch	Beträchtliche negative Auswirkungen	Compliance-Verstöße, erschwerte Incident-Aufklärung
Sehr hoch	Existenzbedrohende Auswirkungen	Schwerwiegende Compliance-Verstöße, unmögliche Incident-Aufklärung

6.2.2 2.2 Bewertungsmaßstab

Bewertungskriterien: - Gesetzliche und regulatorische Anforderungen (DSGVO, IT-Sicherheitsgesetz, etc.) - Vertragliche Verpflichtungen - Geschäftskritikalität - Finanzielle Auswirkungen - Reputationsrisiken - Personenbezogene Daten - Geschäftsgeheimnisse

6.3 3. Schutzbedarfsfeststellung

6.3.1 3.1 Geschäftsprozesse

Prozess-ID	Prozess	Owner	C	I	A	Begründung	Schutzbedarf gesamt
P-001	[TODO: Prozess 1]	[TODO]	Normal/Hoch/Sehr hoch	Normal/Hoch/Sehr hoch	Normal/Hoch/Sehr hoch	[TODO: Begründung]	[TODO: Maximum-Prinzip]
P-002	[TODO: Prozess 2]	[TODO]	Normal/Hoch/Sehr hoch	Normal/Hoch/Sehr hoch	Normal/Hoch/Sehr hoch	[TODO]	[TODO]
P-003	[TODO: Prozess 3]	[TODO]	Normal/Hoch/Sehr hoch	Normal/Hoch/Sehr hoch	Normal/Hoch/Sehr hoch	[TODO]	[TODO]

Anzahl Prozesse gesamt: [TODO]
Verteilung: - Normal: [TODO] - Hoch: [TODO] - Sehr hoch: [TODO]

6.3.2 3.2 Informationen und Daten

Info-ID	Information/Daten	Prozessart	C	I	A	Begründung	Schutzbedarf gesamt
I-001	Personenbezogene Daten (DSGVO)	[TODO]	Hoch	Hoch	Normal	DSGVO-Anforderungen	Hoch
I-002	Geschäftsgeheimnisse	[TODO]	Sehr hoch	Hoch	Normal	Wettbewerbsvorteil	Sehr hoch
I-003	Finanzdaten	[TODO]	Hoch	Sehr hoch	Hoch	Gesetzliche Anforderungen	Sehr hoch
I-004	[TODO: Weitere Daten]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Anzahl Informationsarten gesamt: [TODO]

6.3.3 3.3 Anwendungen

Anwendungs-ID	Anwendung	Prozess	C	I	A	Begründung	Schutzbedarf gesamt
A-001	[TODO: Anwendung 1]	P-001	[TODO]	[TODO]	[TODO]	Vererbung von Prozess P-001	[TODO]
A-002	[TODO: Anwendung 2]	P-002	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
A-003	[TODO: Anwendung 3]	P-003	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Anzahl Anwendungen gesamt: [TODO]

6.3.4 3.4 IT-Systeme und Komponenten

System-ID	System/Komponente	Anwendung	C	I	A	Begründung	Schutzbedarf gesamt
S-001	{{ netbox.device.server_001 }}	A-001	[TODO]	[TODO]	[TODO]	Vererbung von Anwendung A-001	[TODO]
S-002	[TODO: System 2]	A-002	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
S-003	[TODO: System 3]	A-003	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Anzahl IT-Systeme gesamt: [TODO]

6.3.5 3.5 Netzwerke

Netz-ID	Netzwerk/Zone	Systeme	C	I	A	Begründung	Schutzbedarf gesamt
N-001	Management-Netz	S-001, S-002	Sehr hoch	Sehr hoch	Hoch	Kritische Administrationszugriffe	Sehr hoch
N-002	Produktiv-Netz	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
N-003	DMZ	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Anzahl Netzwerke gesamt: [TODO]

6.3.6 3.6 Räume und Standorte

Raum-ID	Raum/Standort	Systeme	C	I	A	Begründung	Schutzbedarf gesamt
R-001	Rechenzentrum	Alle kritischen Server	Sehr hoch	Sehr hoch	Sehr hoch	Hosting kritischer Systeme	Sehr hoch
R-002	{{ meta.organization.primary_location }}	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Anzahl Räume gesamt: [TODO]

6.4 4. Schutzbedarfsvererbung und Abhängigkeiten

6.4.1 4.1 Vererbungsprinzip

Der Schutzbedarf wird nach dem **Maximum-Prinzip** vererbt:

```
Geschäftsprozess
    ↓ (vererbt Schutzbedarf)
Informationen
    ↓ (vererbt Schutzbedarf)
Anwendungen
    ↓ (vererbt Schutzbedarf)
IT-Systeme
    ↓ (vererbt Schutzbedarf)
Netzwerke, Räume
```

Beispiel: - Prozess P-001 hat Schutzbedarf "Sehr hoch" für Vertraulichkeit - Anwendung A-001 unterstützt Prozess P-001 - → Anwendung A-001 erbt Schutzbedarf "Sehr hoch" für Vertraulichkeit - Server S-001 hostet Anwendung A-001 - → Server S-001 erbt Schutzbedarf "Sehr hoch" für Vertraulichkeit

6.4.2 4.2 Vererbungstabelle

Von (Quelle)	Nach (Ziel)	Vererbter Schutzbedarf	Begründung
P-001	A-001	C: Sehr hoch, I: Hoch, A: Hoch	Anwendung unterstützt kritischen Prozess
A-001	S-001	C: Sehr hoch, I: Hoch, A: Hoch	Server hostet kritische Anwendung
[TODO]	[TODO]	[TODO]	[TODO]

6.4.3 4.3 Ausnahmen und Begründungen

Ausnahmen vom Maximum-Prinzip:

Objekt	Erwarteter Schutzbedarf	Tatsächlicher Schutzbedarf	Begründung	Genehmigt von
[TODO: Objekt]	[TODO]	[TODO]	[TODO: Begründung für Abweichung]	Thomas Weber

Wichtig: Ausnahmen müssen dokumentiert und genehmigt werden.

6.4.4 4.4 Kumulative Effekte

Wenn ein System mehrere Anwendungen mit unterschiedlichem Schutzbedarf hostet, gilt das **Maximum-Prinzip**:

System	Anwendung 1	Anwendung 2	Anwendung 3	Resultierender Schutzbedarf
S-001	C: Hoch	C: Sehr hoch	C: Normal	C: Sehr hoch (Maximum)
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

6.5 5. Validierung und Qualitätssicherung

6.5.1 5.1 Validierungsprozess

Die Schutzbedarfsfeststellung wird validiert durch:

1. **Review durch Prozess-Owner:** Bestätigung der Geschäftskritikalität
2. **Review durch IT-Leitung:** Anna Schmidt - Technische Machbarkeit
3. **Review durch Legal/Compliance:** Gesetzliche Anforderungen
4. **Review durch Datenschutz:** DSGVO-Konformität
5. **Freigabe durch ISB:** Thomas Weber

6.5.2 5.2 Konsistenzprüfung

Prüfkriterium	Status	Bemerkungen
Alle Prozesse bewertet	[TODO: /]	[TODO]
Alle Anwendungen bewertet	[TODO: /]	[TODO]
Alle IT-Systeme bewertet	[TODO: /]	[TODO]
Vererbung konsistent	[TODO: /]	[TODO]
Ausnahmen dokumentiert	[TODO: /]	[TODO]
Begründungen vollständig	[TODO: /]	[TODO]

6.6 6. Auswirkungen auf Sicherheitsmaßnahmen

6.6.1 6.1 Maßnahmen nach Schutzbedarf

Schutzbedarf	Beispielhafte Maßnahmen
Normal	Standard-Sicherheitsmaßnahmen, Basis-Härtung, Standard-Backup
Hoch	Erweiterte Sicherheitsmaßnahmen, Verschlüsselung, MFA, erweiterte Überwachung, redundante Systeme
Sehr hoch	Maximale Sicherheitsmaßnahmen, Ende-zu-Ende-Verschlüsselung, Hardware-Token, 24/7-Überwachung, Hochverfügbarkeit, Disaster Recovery

6.6.2 6.2 Priorisierung von Maßnahmen

Sicherheitsmaßnahmen werden priorisiert nach: 1. **Sehr hoher Schutzbedarf:** Höchste Priorität 2. **Hoher Schutzbedarf:** Hohe Priorität 3. **Normaler Schutzbedarf:** Normale Priorität

6.7 7. Dokumentation und Nachweise

Folgende Dokumente und Nachweise werden geführt: - Dieses Schutzbedarfsfeststellungs-Dokument - Bewertungsworkshop-Protokolle - Freigaben der Prozess-Owner - Ausnahme-Genehmigungen - Änderungsprotokolle

6.8 8. Aktualisierung und Pflege

Die Schutzbedarfsfeststellung wird aktualisiert bei: - Neuen Geschäftsprozessen oder Anwendungen - Wesentlichen Änderungen an bestehenden Prozessen - Neuen gesetzlichen Anforderungen - Sicherheitsvorfällen - Mindestens jährlich im Rahmen des ISMS-Reviews

Verantwortlich: Thomas Weber (ISB)
Nächster Review: {{ meta.document.next_review }}

6.9 9. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI Standard 200-2: IT-Grundschutz-Methodik (Kapitel 6: Schutzbedarfsfeststellung) - BSI IT-Grundschutz-Kompendium

ewpage

Chapter 7

Modellierung: Bausteinzuordnung (Template)

Dokument-ID: 0070
Dokumenttyp: Methodik-Artefakt
Referenzrahmen: BSI IT-Grundschutz (BSI Standard 200-2, IT-Grundschutz-Kompendium)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

7.1 1. Ziel und Zweck

Die Modellierung ordnet den Objekten des Informationsverbunds von **AdminSend GmbH** geeignete IT-Grundschutz-Bausteine zu. Sie bildet die Grundlage für: - Basis-Sicherheitscheck (Dokument 0080) - Identifikation umzusetzender Anforderungen - Systematische Sicherheitsmaßnahmen-Planung

Verantwortlich: Thomas Weber (ISB)

Wichtig: Dieses Dokument referenziert nur Bausteine. Die vollständigen Bausteintexte befinden sich im BSI IT-Grundschutz-Kompendium und werden nicht kopiert.

7.2 2. IT-Grundschutz-Bausteine: Übersicht

7.2.1 2.1 Bausteinstruktur

Das BSI IT-Grundschutz-Kompendium gliedert Bausteine in folgende Schichten:

Schicht	Kürzel	Beschreibung	Beispiele
ISMS	ISMS	Sicherheitsmanagement	ISMS.1 Sicherheits-management
Organisation und Personal	ORP	Organisatorische Prozesse	ORP.1 Organisation, ORP.3 Sensibilisierung und Schulung
Konzeption und Vorgehensweisen	CON	Konzepte und Methoden	CON.1 Kryptokonzept, CON.3 Daten-sicherungskonzept
Betrieb	OPS	IT-Betriebsprozesse	OPS.1.1.2 Ordnungsgemäße IT-Administration
Detektion und Reaktion	DER	Incident Management	DER.1 Detektion von sicherheitsrelevanten Ereignissen
Systeme	SYS	IT-Systeme	SYS.1.1 Allgemeiner Server, SYS.2.1 Allgemeiner Client
Anwendungen	APP	Anwendungssoftware	APP.1.1 Office-Produkte, APP.3.1 Webanwendungen
IT-Systeme	NET	Netzwerke und Kommunikation	NET.1.1 Netzarchitektur und -design, NET.3.1 Router und Switches
Industrielle IT	IND	OT/ICS-Systeme	IND.1 Betriebs- und Steuerungstechnik

7.2.2 2.2 Zuordnungslogik

Prinzipien: 1. **Vollständigkeit:** Alle relevanten Objekte erhalten Bausteinzuordnungen 2. **Angemessenheit:** Bausteine passen zum Objekttyp und Schutzbedarf 3. **Keine Redundanz:** Jeder Baustein wird nur einmal pro Objekt zugeordnet 4. **Granularität:** Zuordnung auf sinnvoller Abstraktionsebene

Vorgehen: 1. Objekte aus Strukturanalyse (Dokument 0050) übernehmen 2. Passende Bausteine aus IT-Grundschutz-Kompendium identifizieren 3. Zuordnung dokumentieren 4. Validierung durch IT-Leitung und ISB

7.3 3. Bausteinzuordnung

7.3.1 3.1 ISMS und Organisation (ISMS, ORP)

Objekt-ID	Objekt	Objektklasse	Zugeordnete Bausteine	Begründung	Owner
ORG-001	AdminSend GmbH	Organisation	ISMS.1 Sicherheits-management	Gesamtorganisation	Thomas Weber
ORG-001	AdminSend GmbH	Organisation	ORP.1 Organisation	Organisationsstruktur	Thomas Weber
ORG-001	AdminSend GmbH	Organisation	ORP.2 Personal	Personalmanagement	[TODO: HR]
ORG-001	AdminSend GmbH	Organisation	ORP.3 Sensi-bilisierung und Schulung	Awareness-Programm	Thomas Weber
ORG-001	AdminSend GmbH	Organisation	ORP.4 Identitäts- und Berechti-gungsmanage-ment	IAM-Prozesse	Anna Schmidt
ORG-001	AdminSend GmbH	Organisation	ORP.5 Compliance Management (An-forderungs-management)	Compliance	[TODO]

7.3.2 3.2 Konzeption und Vorgehensweisen (CON)

Objekt-ID	Objekt	Objektklasse	Zugeordnete Bausteine	Begründung	Owner
CON-001	Kryptokonzept	Konzept	CON.1 Kryp-tokonzept	Verschlüsselungsstrategie	Thomas Weber
CON-002	Datensicherungskonzept	Konzept	CON.3 Daten-sicherungskonzept	Backup-Strategie	Anna Schmidt
CON-003	Löschkonzept	Konzept	CON.6 Löschen und Vernichten	Datenlöschung	Thomas Weber
CON-004	Patch- und Änderungs-management	Konzept	CON.7 Information-ssicherheit auf Ausland-sreisen	[TODO: falls zutreffend]	[TODO]
CON-005	Softwareentwicklung	Konzept	CON.8 Software-Entwicklung	[TODO: falls zutreffend]	[TODO]

7.3.3 3.3 Betrieb (OPS)

Objekt-ID	Objekt	Objektklasse	Zugeordnete Bausteine	Begründung	Owner
OPS-001	IT-Betrieb	Betriebsprozess	OPS.1.1.2 Ordnungsgemäße IT-Administration	IT-Administration	Anna Schmidt
OPS-002	Patch Management	Betriebsprozess	OPS.1.1.3 Patch- und Änderungsmanagement	Patch-Prozess	Anna Schmidt
OPS-003	Schutz vor Schadprogrammen	Betriebsprozess	OPS.1.1.4 Schutz vor Schadprogrammen	Malware-Schutz	Anna Schmidt
OPS-004	Datensicherung	Betriebsprozess	OPS.1.1.5 Protokollierung	Logging	Anna Schmidt
OPS-005	Software-Tests	Betriebsprozess	OPS.1.1.6 Software-Tests und -Freigaben	[TODO: falls zutreffend]	[TODO]
OPS-006	Outsourcing	Betriebsprozess	OPS.2.1 Outsourcing für Kunden	[TODO: falls zutreffend]	[TODO]
OPS-007	Cloud-Nutzung	Betriebsprozess	OPS.2.2 Cloud-Nutzung	Cloud-Services	Anna Schmidt

7.3.4 3.4 Detektion und Reaktion (DER)

Objekt-ID	Objekt	Objektklasse	Zugeordnete Bausteine	Begründung	Owner
DER-001	Detektion	Prozess	DER.1 Detektion von sicherheitsrelevanten Ereignissen	SIEM, Monitoring	Anna Schmidt
DER-002	Incident Management	Prozess	DER.2.1 Behandlung von Sicherheitsvorfällen	Incident Response	Thomas Weber
DER-003	Forensik	Prozess	DER.2.2 Vorsorge für die IT-Forensik	[TODO: falls zutreffend]	[TODO]

Objekt-ID	Objekt	Objektklasse	Zugeordnete Bausteine	Begründung	Owner
DER-004	Audits	Prozess	DER.3.1 Audits und Revisionen	Internal Audit	[TODO]

7.3.5 3.5 Anwendungen (APP)

Objekt-ID	Objekt	Objektklasse	Zugeordnete Bausteine	Begründung	Owner
A-001	[TODO: Anwendung 1]	Anwendung	APP.1.1 Office-Produkte	[TODO: falls Office-Anwendung]	[TODO]
A-002	[TODO: Anwendung 2]	Anwendung	APP.3.1 Webanwendungen	[TODO: falls Webanwendung]	[TODO]
A-003	[TODO: Anwendung 3]	Anwendung	APP.3.2 Webserver	[TODO: falls Webserver]	Anna Schmidt
A-004	[TODO: Anwendung 4]	Anwendung	APP.3.3 Fileserver	[TODO: falls Fileserver]	Anna Schmidt
A-005	[TODO: Anwendung 5]	Anwendung	APP.3.6 DNS-Server	[TODO: falls DNS]	Anna Schmidt
A-006	[TODO: Anwendung 6]	Anwendung	APP.4.3 Relationale Datenbanksysteme	[TODO: falls Datenbank]	Anna Schmidt
A-007	[TODO: Anwendung 7]	Anwendung	APP.5.1 Allgemeine Groupware	[TODO: falls Groupware]	[TODO]
A-008	[TODO: Anwendung 8]	Anwendung	APP.5.2 Microsoft Exchange und Outlook	[TODO: falls Exchange]	Anna Schmidt

7.3.6 3.6 IT-Systeme (SYS)

Objekt-ID	Objekt	Objektklasse	Zugeordnete Bausteine	Begründung	Owner
S-001	{{ net-box.device.server_001 }}	Server	SYS.1.1 Allgemeiner Server	Allgemeiner Server	Anna Schmidt
S-002	[TODO: Linux-Server]	Server	SYS.1.3 Server unter Linux und Unix	Linux-Server	Anna Schmidt

Objekt-ID	Objekt	Objektklasse	Zugeordnete Bausteine	Begründung	Owner
S-003	[TODO: Windows-Server]	Server	SYS.1.2.3 Windows Server	Windows-Server	Anna Schmidt
S-004	[TODO: Virtualisierung]	Virtualisierung	SYS.1.5 Virtualisierung	VMware/Hyper-V	Anna Schmidt
S-005	[TODO: Container]	Container	SYS.1.6 Containerisierung	Docker/Kubernetes	Anna Schmidt
S-006	[TODO: Storage]	Storage	SYS.1.8 Speicherlösungen	SAN/NAS	Anna Schmidt
S-007	[TODO: Client]	Client	SYS.2.1 Allgemeiner Client	Workstations	Anna Schmidt
S-008	[TODO: Windows-Client]	Client	SYS.2.2.3 Clients unter Windows	Windows-Clients	Anna Schmidt
S-009	[TODO: macOS-Client]	Client	SYS.2.4 Clients unter macOS	macOS-Clients	Anna Schmidt
S-010	[TODO: Mobile Device]	Mobile	SYS.3.2.1 Allgemeine Smartphones und Tablets	Mobile Devices	Anna Schmidt
S-011	[TODO: IoT]	IoT	SYS.4.4 Allgemeines IoT-Gerät	[TODO: falls IoT]	[TODO]

7.3.7 3.7 Netzwerke und Kommunikation (NET)

Objekt-ID	Objekt	Objektklasse	Zugeordnete Bausteine	Begründung	Owner
N-001	Netzwerkarchitektur	Netzwerk	NET.1.1 Netzarchitektur und -design	Gesamtnetzwerk	Anna Schmidt
N-002	Netzwerkmanagement	Netzwerk	NET.1.2 Netzmanagement	Netzwerk-Monitoring	Anna Schmidt
N-003	[TODO: Router/Switches]	Netzwerkkomponente	NET.3.1 Router und Switches	Netzwerkgeräte	Anna Schmidt
N-004	[TODO: Firewall]	Sicherheitskomponente	NET.3.2 Firewall	Perimeter-Schutz	Anna Schmidt
N-005	[TODO: VPN]	Sicherheitskomponente	NET.3.3 VPN	Remote-Zugriff	Anna Schmidt

Objekt-ID	Objekt	Objektklasse	Zugeordnete Bausteine	Begründung	Owner
N-006	[TODO: WLAN]	Netzwerk	NET.2.1 WLAN-Betrieb	Wireless-Netzwerk	Anna Schmidt
N-007	[TODO: E-Mail]	Kommunikation	NET.4.1 TLS-Verschlüsselung	[TODO: falls zutreffend]	Anna Schmidt

7.3.8 3.8 Industrielle IT (IND) - Optional

Objekt-ID	Objekt	Objektklasse	Zugeordnete Bausteine	Begründung	Owner
IND-001	[TODO: OT-System]	OT/ICS	IND.1 Betriebs- und Steuerungstechnik	[TODO: falls OT im Scope]	[TODO]
IND-002	[TODO: ICS-Komponente]	OT/ICS	IND.2.1 Allgemeine ICS-Komponente	[TODO: falls ICS im Scope]	[TODO]

7.3.9 3.9 Räume und Infrastruktur (INF)

Objekt-ID	Objekt	Objektklasse	Zugeordnete Bausteine	Begründung	Owner
R-001	Rechenzentrum	Raum	INF.2 Rechenzentrum sowie Serverraum	Kritischer Serverraum	[TODO: Facility]
R-002	{{ meta.organization.primary_location }}	Gebäude	INF.1 Allgemeines Gebäude	Hauptstandort	[TODO: Facility]
R-003	[TODO: Büroraum]	Raum	INF.8 Häuslicher Arbeitsplatz	[TODO: falls Home Office]	[TODO]

7.4 4. Zusammenfassung und Statistik

7.4.1 4.1 Zuordnungsstatistik

Bausteinschicht	Anzahl zugeordneter Bausteine	Anzahl betroffener Objekte
ISMS	[TODO]	[TODO]
ORP (Organisation und Personal)	[TODO]	[TODO]

Bausteinschicht	Anzahl zugeordneter Bausteine	Anzahl betroffener Objekte
CON (Konzeption)	[TODO]	[TODO]
OPS (Betrieb)	[TODO]	[TODO]
DER (Detektion und Reaktion)	[TODO]	[TODO]
APP (Anwendungen)	[TODO]	[TODO]
SYS (Systeme)	[TODO]	[TODO]
NET (Netzwerke)	[TODO]	[TODO]
IND (Industrielle IT)	[TODO]	[TODO]
INF (Infrastruktur)	[TODO]	[TODO]
Gesamt	**[TODO]**	**[TODO]**

7.4.2 4.2 Vollständigkeitsprüfung

Objekttyp	Anzahl Objekte	Anzahl mit Bausteinzuordnung	Vollständigkeit
Prozesse	[TODO]	[TODO]	[TODO: %]
Anwendungen	[TODO]	[TODO]	[TODO: %]
IT-Systeme	[TODO]	[TODO]	[TODO: %]
Netzwerke	[TODO]	[TODO]	[TODO: %]
Räume	[TODO]	[TODO]	[TODO: %]

7.4.3 4.3 Offene Punkte

ID	Objekt	Problem	Verantwortlich	Frist
[TODO]	[TODO]	[TODO: Kein passender Baustein gefunden]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO: Unklare Zuordnung]	[TODO]	[TODO]

7.5 5. Validierung und Qualitätssicherung

7.5.1 5.1 Validierungsprozess

Die Bausteinzuordnung wird validiert durch: 1. **Review durch IT-Leitung:** Anna Schmidt - Technische Korrektheit 2. **Review durch Informationsverbund-Verantwortliche:** Vollständigkeit 3. **Abgleich mit IT-Grundschutz-Kompendium:** Aktualität der Bausteine 4. **Freigabe durch ISB:** Thomas Weber

7.5.2 5.2 Qualitätskriterien

Kriterium	Status	Bemerkungen
Alle Objekte haben Bausteinzuordnungen	[TODO: /]	[TODO]
Bausteine sind aktuell (IT-Grundschutz-Kompendium Edition [TODO])	[TODO: /]	[TODO]
Zuordnungen sind nachvollziehbar begründet	[TODO: /]	[TODO]
Keine Redundanzen	[TODO: /]	[TODO]
Owner sind benannt	[TODO: /]	[TODO]

7.6 6. Nächste Schritte

Nach Abschluss der Modellierung folgen: 1. **Basis-Sicherheitscheck (Dokument 0080):** Abgleich Soll-Ist für alle zugeordneten Bausteine 2. **Risikoanalyse (Dokument 0090):** Für Objekte mit erhöhtem Schutzbedarf oder nicht modellierbaren Risiken 3. **Maßnahmenplanung (Dokument 0100):** Umsetzungsplanung identifizierter Anforderungen

7.7 7. Aktualisierung und Pflege

Die Bausteinzuordnung wird aktualisiert bei: - Neuen IT-Systemen oder Anwendungen - Änderungen in der IT-Architektur - Neuer Edition des IT-Grundschutz-Kompendiums - Mindestens jährlich im Rahmen des ISMS-Reviews

Verantwortlich: Thomas Weber (ISB)
Nächster Review: {{ meta.document.next_review }}

7.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI Standard 200-2: IT-Grundschutz-Methodik (Kapitel 7: Modellierung) - BSI IT-Grundschutz-Kompendium (aktuelle Edition) - BSI IT-Grundschutz-Kompendium: https://www.bsi.bund.de/grundschutz-kompendium

ewpage

Chapter 8

Basis-Sicherheitscheck / Gap-Analyse (Template)

Dokument-ID: 0080
Dokumenttyp: Methodik-Artefakt
Referenzrahmen: BSI IT-Grundschutz (BSI Standard 200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

8.1 1. Ziel und Zweck

Der Basis-Sicherheitscheck bewertet systematisch, inwieweit die für den Informationsverbund von **AdminSend GmbH** modellierten IT-Grundschutz-Anforderungen umgesetzt sind. Er bildet die Grundlage für: - Identifikation von Sicherheitslücken (Gaps) - Priorisierung von Maßnahmen - Maßnahmenplanung (Dokument 0100) - Compliance-Nachweis

Verantwortlich: Thomas Weber (ISB)

8.2 2. Vorgehen und Methodik

8.2.1 2.1 Datenquellen

Folgende Quellen werden für den Basis-Sicherheitscheck genutzt:

Datenquelle	Typ	Verantwortlich	Verwendung
Interviews mit Stakeholdern	Primärquelle	Thomas Weber	Prozess- und Organisationsanforderungen

Datenquelle	Typ	Verantwortlich	Verwendung
Konfigurationsnachweise	Technisch	Anna Schmidt	Technische Anforderungen
Policies und Richtlinien	Dokument	Thomas Weber	Organisatorische Anforderungen
Tickets und Change-Records	System	Anna Schmidt	Umsetzungsnachweise
Logs und Monitoring-Daten	System	Anna Schmidt	Betriebsanforderungen
Audit-Berichte	Dokument	[TODO: Internal Audit]	Externe Validierung

8.2.2 2.2 Bewertungslogik

Erfüllungsgrade:

Status	Kürzel	Beschreibung	Kriterien
Erfüllt	E	Anforderung vollständig umgesetzt	Alle Aspekte der Anforderung sind implementiert und nachgewiesen
Teilweise erfüllt	T	Anforderung teilweise umgesetzt	Wesentliche Aspekte umgesetzt, aber Lücken vorhanden
Nicht erfüllt	N	Anforderung nicht umgesetzt	Anforderung nicht oder nur minimal umgesetzt
Nicht anwendbar	N/A	Anforderung nicht relevant	Anforderung trifft auf Organisation nicht zu
Nicht bewertet	-	Noch nicht geprüft	Bewertung steht noch aus

8.2.3 2.3 Stichprobenumfang

Prüftiefe: - **Kritische Anforderungen (Schutzbedarf "Sehr hoch"):** 100% Prüfung - **Wichtige Anforderungen (Schutzbedarf "Hoch"):** Stichprobe 50% - **Standard-Anforderungen (Schutzbedarf "Normal"):** Stichprobe 25%

Prüfmethoden: - Dokumentenprüfung - Konfigurationsprüfung - Interviews - Technische Tests (Stichproben)

8.2.4 2.4 Durchführung

Zeitplan: - **Start:** [TODO] - **Datenerhebung:** [TODO: z.B. 4 Wochen] - **Bewertung:** [TODO: z.B. 2 Wochen] - **Validierung:** [TODO: z.B. 1 Woche] - **Abschluss:** [TODO]

Beteiligte: - ISB: Thomas Weber - IT-Leitung: Anna Schmidt - Informationsverbund-Verantwortliche: [TODO] - Fachabteilungen: [TODO]

8.3 3. Basis-Sicherheitscheck: Ergebnisse

8.3.1 3.1 ISMS und Organisation (ISMS, ORP)

Baustein	Anforderung (Kurz)	Objekt	Status	Nachweis/Evidenz	Finding	Maßnahme	Owner	Zieltermin
ISMS.1	Sicherheitsleitlinie erstellt	Admin GmbH	E	Dokument 0010	-	-	Thomas Weber	-
ISMS.1	ISMS-Organisation definiert	Admin GmbH	E	Dokument 0020	-	-	Thomas Weber	-
ISMS.1	Ressourcen bereitgestellt	Admin GmbH	T	Budget-Nachweis	Budget unzureichend	Budget erhöhen	Max Mustermann	[TODO]
ORP.1	Rollen und Verantwortlichkeiten definiert	Admin GmbH	E	Dokument 0020	-	-	Thomas Weber	-
ORP.2	Einarbeitung neuer Mitarbeitender	Admin GmbH	T	HR-Prozess	Keine Security-Schulung im Onboarding	Security-Schulung integrieren	[TODO: HR]	[TODO]
ORP.3	Awareness-Programm	Admin GmbH	N	-	Kein Awareness-Programm vorhanden	Awareness-Programm aufbauen	Thomas Weber	[TODO]
ORP.4	IAM-Prozess	Admin GmbH	T	IAM-Richtlinie	Rezertifizierung fehlt	Rezertifizierung implementieren	Anna Schmidt	[TODO]

8.3.2 3.2 Konzeption und Vorgehensweisen (CON)

Baustein	Anforderung (Kurz)	Objekt	Status	Nachweis/Evidenz	Finding	Maßnahme	Owner	Zieltermin
CON.1	Kryptokonzept erstellt	Kryptokonzept	N	-	Kein Kryptokonzept vorhanden	Kryptokonzept erstellen	Thomas Weber	[TODO]
CON.3	Datensicherungskonzept erstellt	Backup-Konzept	E	Backup-Dokumentation	-	-	Anna Schmidt	-

Baustein	Anforderung (Kurz)	Objekt	Status	Nachweis/Evidenz	Finding	Maßnahme	Owner	Zieltermin
CON.3	Backup-Tests durchgeführt	Backup-Prozess	T	Test-Protokolle	Tests nicht regelmäßig	Quartalsweise Backup-Tests etablieren	Anna Schmidt	[TODO]
CON.6	Löschkonzept erstellt	Löschkonzept	N	-	Kein Löschkonzept vorhanden	Löschkonzept erstellen	Thomas Weber	[TODO]

8.3.3 3.3 Betrieb (OPS)

Baustein	Anforderung (Kurz)	Objekt	Status	Nachweis/Evidenz	Finding	Maßnahme	Owner	Zieltermin
OPS.1.1.2	Administrationskonzept	IT-Administration	T	Admin-Richtlinie	Privileged Access Management fehlt	PAM-Lösung implementieren	Anna Schmidt	[TODO]
OPS.1.1.3	Patch-Prozess etabliert	Patch Management	E	Patch-Dokumentation	-	-	Anna Schmidt	-
OPS.1.1.3	Patch-SLAs definiert	Patch Management	T	SLA-Dokument	Kritische Patches > 30 Tage	SLA auf 7 Tage reduzieren	Anna Schmidt	[TODO]
OPS.1.1.4	Malware-Schutz implementiert	Alle Systeme	E	Antivirus-Lösung	-	-	Anna Schmidt	-
OPS.1.1.5	Logging aktiviert	Alle Systeme	T	Log-Konfiguration	Zentrale Log-Sammlung fehlt	SIEM implementieren	Anna Schmidt	[TODO]
OPS.2.2	Cloud-Sicherheitskonzept	Cloud-Services	N	-	Kein Cloud-Sicherheitskonzept	Cloud-Sicherheitskonzept erstellen	Thomas Weber	[TODO]

8.3.4 3.4 Detektion und Reaktion (DER)

Baustein	Anforderung (Kurz)	Objekt	Status	Nachweis/Evidenz	Finding	Maßnahme	Owner	Zieltermin
DER.1	Detektion etabliert	Monitoring	T	Monitoring-Tools	SIEM fehlt	SIEM implementieren	Anna Schmidt	[TODO]
DER.2.1	Incident-Response-Prozess	Incident Management	T	IR-Richtlinie	Keine Incident-Response-Übungen	Jährliche IR-Übung etablieren	Thomas Weber	[TODO]
DER.2.2	Forensik-Vorbereitung	Forensik	N	-	Keine Forensik-Vorbereitung	Forensik-Konzept erstellen	Thomas Weber	[TODO]

8.3.5 3.5 Anwendungen (APP)

Baustein	Anforderung (Kurz)	Objekt	Status	Nachweis/Evidenz	Finding	Maßnahme	Owner	Zieltermin
APP.3.1	Sichere Webanwendungsentwicklung	[TODO: Webanwendung]	T	SDLC-Prozess	SAST/DAST fehlt	Security-Testing integrieren	[TODO]	[TODO]
APP.3.2	Webserver-Härtung	[TODO: Webserver]	E	Härtungs-Checkliste	-	-	Anna Schmidt	-
APP.4.3	Datenbank-Härtung	[TODO: Datenbank]	T	DB-Konfiguration	Verschlüsselung at rest fehlt	TDE aktivieren	Anna Schmidt	[TODO]

8.3.6 3.6 IT-Systeme (SYS)

Baustein	Anforderung (Kurz)	Objekt	Status	Nachweis/Evidenz	Finding	Maßnahme	Owner	Zieltermin
SYS.1.1	Server-Härtung	{{ netbox.device.server_001 }}	E	Härtungs-Baseline	-	-	Anna Schmidt	-
SYS.1.3	Linux-Härtung	[TODO: Linux-Server]	T	CIS Benchmark	Nicht alle CIS-Controls umgesetzt	Vollständige CIS-Umsetzung	Anna Schmidt	[TODO]

Baustein	Anforderung (Kurz)	Objekt	Status	Nachweis/Evidenz	Finding	Maßnahme	Owner	Zieltermin
SYS.1.5	Virtualisierungs-Sicherheit	[TODO: VMware]	T	VMware-Konfiguration	Netzwerksegmentierung unzureichend	Mikrosegmentierung implementieren	Anna Schmidt	[TODO]
SYS.2.1	Client-Härtung	Workstations	T	GPO-Konfiguration	BitLocker nicht flächendeckend	BitLocker auf allen Clients aktivieren	Anna Schmidt	[TODO]
SYS.3.2.1	Mobile Device Management	Mobile Devices	N	-	Kein MDM vorhanden	MDM-Lösung implementieren	Anna Schmidt	[TODO]

8.3.7 3.7 Netzwerke und Kommunikation (NET)

Baustein	Anforderung (Kurz)	Objekt	Status	Nachweis/Evidenz	Finding	Maßnahme	Owner	Zieltermin
NET.1.1	Netzwerksegmentierung	Netzwerkarchitektur	T	Netzwerkdiagramm	Segmentierung unzureichend	Mikrosegmentierung implementieren	Anna Schmidt	[TODO]
NET.1.2	Netzwerk-Monitoring	Netzwerkmanagement	E	Monitoring-Tools	-	-	Anna Schmidt	-
NET.3.1	Router/Switch-Härtung	Netzwerkgeräte	T	Konfigurationsnachweis	SNMP v3 nicht überall	SNMP v3 flächendeckend	Anna Schmidt	[TODO]
NET.3.2	Firewall-Regelwerk	Firewall	E	Firewall-Rules	-	-	Anna Schmidt	-
NET.3.3	VPN-Sicherheit	VPN	T	VPN-Konfiguration	MFA für VPN fehlt	MFA für VPN implementieren	Anna Schmidt	[TODO]
NET.2.1	WLAN-Sicherheit	WLAN	E	WLAN-Konfiguration	-	-	Anna Schmidt	-

8.3.8 3.8 Infrastruktur (INF)

Baustein	Anforderung (Kurz)	Objekt	Status	Nachweis/Evidenz	Finding	Maßnahme	Owner	Zieltermin
INF.1	Gebäudesicherheit	{{ meta.organization.primary_location }}	T	Sicherheitskonzept	Besuchermanagement unzureichend	Besuchermanagement-System	[TODO: Facility-Management]	[TODO]
INF.2	Rechenzentrum Sicherheit	Rechenzentrum	Erfüllt	RZ-Dokumentation	-	-	[TODO: Facility]	-

8.4 4. Zusammenfassung und Statistik

8.4.1 4.1 Erfüllungsstatistik

Bausteinschicht	Gesamt	Erfüllt (E)	Teilweise (T)	Nicht erfüllt (N)	N/A	Erfüllungsgrad
ISMS	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
ORP	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
CON	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
OPS	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
DER	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
APP	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
SYS	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
NET	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
INF	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO: %]
Gesamt	**[TODO]**	**[TODO]**	**[TODO]**	**[TODO]**	**[TODO]**	**[TODO: %]**

Gesamterfüllungsgrad: [TODO: %]

8.4.2 4.2 Kritische Lücken (Priorität 1)

ID	Anforderung	Objekt	Risiko	Maßnahme	Owner	Zieltermin
GAP-001	[TODO: Kritische Lücke 1]	[TODO]	Sehr hoch	[TODO]	[TODO]	[TODO]
GAP-002	[TODO: Kritische Lücke 2]	[TODO]	Sehr hoch	[TODO]	[TODO]	[TODO]

8.4.3 4.3 Quick Wins (Priorität 2)

ID	Anforderung	Objekt	Aufwand	Nutzen	Maßnahme	Owner	Zieltermin
QW-001	[TODO: Quick Win 1]	[TODO]	Niedrig	Hoch	[TODO]	[TODO]	[TODO]
QW-002	[TODO: Quick Win 2]	[TODO]	Niedrig	Hoch	[TODO]	[TODO]	[TODO]

8.4.4 4.4 Mittelfristige Maßnahmen (Priorität 3)

ID	Anforderung	Objekt	Aufwand	Maßnahme	Owner	Zieltermin
MF-001	[TODO: Mittelfristige Maßnahme 1]	[TODO]	Mittel	[TODO]	[TODO]	[TODO]
MF-002	[TODO: Mittelfristige Maßnahme 2]	[TODO]	Mittel	[TODO]	[TODO]	[TODO]

8.5 5. Management Summary

8.5.1 5.1 Gesamtbewertung

Erfüllungsgrad: [TODO: %]

Bewertung: - [TODO: Zusammenfassende Bewertung des Sicherheitsniveaus] - [TODO: Haupterkenntnisse] - [TODO: Kritische Handlungsfelder]

8.5.2 5.2 Top 5 Findings

1. **[TODO: Finding 1]:** [TODO: Beschreibung und Auswirkung]
2. **[TODO: Finding 2]:** [TODO: Beschreibung und Auswirkung]
3. **[TODO: Finding 3]:** [TODO: Beschreibung und Auswirkung]
4. **[TODO: Finding 4]:** [TODO: Beschreibung und Auswirkung]
5. **[TODO: Finding 5]:** [TODO: Beschreibung und Auswirkung]

8.5.3 5.3 Ressourcenbedarf

Geschätzter Aufwand für Maßnahmenumsetzung: - **Personentage:** [TODO] - **Budget:** [TODO] - **Externe Unterstützung:** [TODO] - **Zeitrahmen:** [TODO]

8.5.4 5.4 Abhängigkeiten

Maßnahme	Abhängigkeit	Auswirkung	Mitigation
[TODO: Maßnahme 1]	[TODO: Abhängigkeit]	[TODO]	[TODO]
[TODO: Maßnahme 2]	[TODO: Abhängigkeit]	[TODO]	[TODO]

8.6 6. Nächste Schritte

1. **Maßnahmenplanung (Dokument 0100):** Detaillierte Planung der identifizierten Maßnahmen
2. **Risikoanalyse (Dokument 0090):** Für Objekte mit erhöhtem Schutzbedarf oder nicht modellierbaren Risiken
3. **Management-Präsentation:** Vorstellung der Ergebnisse an Geschäftsführung
4. **Maßnahmenumsetzung:** Start der Umsetzung priorisierter Maßnahmen

8.7 7. Aktualisierung und Pflege

Der Basis-Sicherheitscheck wird wiederholt: - Nach Abschluss wesentlicher Maßnahmen - Bei wesentlichen Änderungen in der IT-Infrastruktur - Mindestens jährlich im Rahmen des ISMS-Reviews

Verantwortlich: Thomas Weber (ISB)
Nächster Check: {{ meta.document.next_review }}

8.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI Standard 200-2: IT-Grundschutz-Methodik (Kapitel 8: Basis-Sicherheitscheck) - BSI IT-Grundschutz-Kompendium

ewpage

Chapter 9

Risikoanalyse (BSI Standard 200-3) – Template

Dokument-ID: 0090
Dokumenttyp: Methodik-Artefakt
Referenzrahmen: BSI IT-Grundschutz (BSI Standard 200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

9.1 1. Ziel und Auslöser

Die Risikoanalyse nach BSI Standard 200-3 identifiziert und bewertet Risiken für **AdminSend GmbH**, die nicht durch IT-Grundschutz-Bausteine abgedeckt sind.

Verantwortlich: Thomas Weber (ISB)

Auslöser für Risikoanalyse: - Hoher oder sehr hoher Schutzbedarf (siehe Dokument 0060) - Besondere Bedrohungslage (z.B. gezielte Angriffe) - Abweichungen von IT-Grundschutz-Anforderungen - Neue Technologien ohne passende Bausteine - Externe Anforderungen (Kunden, Regulierung)

[TODO: Spezifische Auslöser für diese Risikoanalyse dokumentieren]

9.2 2. Risikoobjekte und Scope

Betroffene Objekte:

Objekt-ID	Objekt	Typ	Schutzbedarf	Begründung für Risikoanalyse
[TODO]	[TODO]	Prozess/Anwendung/System	[TODO]	[TODO]
[TODO]	[TODO]	Prozess/Anwendung/System	[TODO]	[TODO]

Schnittstellen und Provider: - [TODO: Externe Schnittstellen und Dienstleister dokumentieren]

9.3 3. Bedrohungen, Schwachstellen und Szenarien

9.3.1 3.1 Bedrohungskatalog

Bedrohungs-ID	Bedrohung	Kategorie	Beschreibung
T-001	Gezielte Cyberangriffe	Extern	APT-Angriffe auf kritische Systeme
T-002	Ransomware	Extern	Verschlüsselung kritischer Daten
T-003	Insider-Bedrohung	Intern	Missbrauch privilegierter Zugriffe
T-004	DDoS-Angriffe	Extern	Verfügbarkeitsbeeinträchtigung
T-005	Supply Chain Attacks	Extern	Kompromittierung über Lieferanten
[TODO]	[TODO]	[TODO]	[TODO]

9.3.2 3.2 Schwachstellenkatalog

Schwachstellen-ID	Schwachstelle	Objekt	Beschreibung
V-001	Unzureichende Segmentierung	Netzwerk	Fehlende Mikrosegmentierung
V-002	Fehlende MFA	VPN-Zugang	Nur Passwort-Authentifizierung
V-003	Veraltete Software	[TODO: System]	End-of-Life Software im Einsatz
[TODO]	[TODO]	[TODO]	[TODO]

9.3.3 3.3 Risikoszenarien

Szenario-ID	Szenario	Bedrohung	Schwachstelle	Betroffenes Objekt
S-001	Ransomware-Angriff auf Produktionssysteme	T-002	V-001, V-002	[TODO: Produktionssystem]

Szenario-ID	Szenario	Bedrohung	Schwachstelle	Betroffenes Objekt
S-002	Datendiebstahl durch Insider	T-003	V-002	[TODO: Datenbank]
S-003	DDoS auf öffentliche Services	T-004	[TODO]	[TODO: Webserver]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

9.4 4. Risikobewertung

9.4.1 4.1 Bewertungsskala

Eintrittswahrscheinlichkeit:

Stufe	Beschreibung	Häufigkeit
1 - Sehr gering	Unwahrscheinlich	< 1x in 10 Jahren
2 - Gering	Selten	1x in 5-10 Jahren
3 - Mittel	Gelegentlich	1x in 1-5 Jahren
4 - Hoch	Wahrscheinlich	1x pro Jahr
5 - Sehr hoch	Sehr wahrscheinlich	Mehrmals pro Jahr

Auswirkung (Schadenshöhe):

Stufe	Beschreibung	Finanzielle Auswirkung	Geschäftsauswirkung
1 - Sehr gering	Vernachlässigbar	< 10.000 €	Keine wesentliche Beeinträchtigung
2 - Gering	Begrenzt	10.000 - 50.000 €	Geringe Beeinträchtigung
3 - Mittel	Beträchtlich	50.000 - 250.000 €	Merkliche Beeinträchtigung
4 - Hoch	Schwerwiegend	250.000 - 1.000.000 €	Erhebliche Beeinträchtigung
5 - Sehr hoch	Katastrophal	> 1.000.000 €	Existenzbedrohend

Risikomatrix:

Eintrittswahrscheinlichkeit	Auswirkung 1	Auswirkung 2	Auswirkung 3	Auswirkung 4	Auswirkung 5
5 - Sehr hoch	Mittel	Hoch	Hoch	Sehr hoch	Sehr hoch
4 - Hoch	Mittel	Mittel	Hoch	Hoch	Sehr hoch
3 - Mittel	Niedrig	Mittel	Mittel	Hoch	Hoch
2 - Gering	Niedrig	Niedrig	Mittel	Mittel	Hoch

Eintrittswahrscheinlichkeit	Auswirkung 1	Auswirkung 2	Auswirkung 3	Auswirkung 4	Auswirkung 5
1 - Sehr gering	Niedrig	Niedrig	Niedrig	Mittel	Mittel

9.4.2 4.2 Risikoakzeptanzkriterien

Risikostufe	Behandlung	Genehmigung erforderlich
Sehr hoch	Muss behandelt werden	Geschäftsführung
Hoch	Sollte behandelt werden	ISB
Mittel	Kann behandelt werden	ISB
Niedrig	Kann akzeptiert werden	Informationsverbund-Verantwortlicher

9.5 5. Risikoregister

Risiko-ID	Objekt	Szenario	Bedrohung	Schwachstelle	Bestehende Maßnahme	Eintrittswahrscheinlichkeit	Auswirkung	Risiko (inhärent)	Behandlung	Zusätzliche Maßnahme	Owner	Termin	Risiko (nachher)
R-001	[TODO]	S-001	T-002	V-001, V-002	Antivirus, Backup	4	5	Sehr hoch	Mindern	Mikrosegmentierung, MFA	Anna Schmidt	[TODO]	Mittel
R-002	[TODO]	S-002	T-003	V-002	Logging, IAM	3	4	Hoch	Mindern	PAM, DLP	Anna Schmidt	[TODO]	Niedrig
R-003	[TODO]	S-003	T-004	[TODO]	Firewall	3	3	Mittel	Mindern	DDoS-Protection	Anna Schmidt	[TODO]	Niedrig
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Risikobehandlungsoptionen: - **Mindern:** Zusätzliche Maßnahmen implementieren - **Vermeiden:** Risikoquelle eliminieren - **Übertragen:** Risiko auf Dritte übertragen (Versicherung, Outsourcing) - **Akzeptieren:** Risiko bewusst akzeptieren (mit Genehmigung)

9.6 6. Risikobewertung: Zusammenfassung

Risikoverteilung (vor Behandlung): - Sehr hoch: [TODO] - Hoch: [TODO] - Mittel: [TODO] - Niedrig: [TODO]

Risikoverteilung (nach Behandlung): - Sehr hoch: [TODO] - Hoch: [TODO] - Mittel: [TODO] - Niedrig: [TODO]

Top 5 Risiken: 1. [TODO: Risiko 1] 2. [TODO: Risiko 2] 3. [TODO: Risiko 3] 4. [TODO: Risiko 4] 5. [TODO: Risiko 5]

9.7 7. Freigabe und Risikoakzeptanz

9.7.1 7.1 Risikoeigner

Risiko-ID	Risiko	Risikoeigner	Akzeptanz	Datum
R-001	[TODO]	Max Mustermann	Akzeptiert nach Maßnahmenumsetzung	[TODO]
R-002	[TODO]	Thomas Weber	Akzeptiert nach Maßnahmenumsetzung	[TODO]

9.7.2 7.2 Management-Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

9.8 8. Aktualisierung und Pflege

Die Risikoanalyse wird aktualisiert bei: - Wesentlichen Änderungen in der Bedrohungslage - Neuen Schwachstellen oder Sicherheitsvorfällen - Änderungen am Informationsverbund - Mindestens jährlich im Rahmen des ISMS-Reviews

Verantwortlich: Thomas Weber (ISB)
Nächster Review: {{ meta.document.next_review }}

Referenzen: - BSI Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz - BSI IT-Grundschutz-Kompendium

ewpage

Chapter 10

Sicherheitskonzept und Maßnahmenplan

Dokument-ID: 0100
Dokumenttyp: Plan/Steuerungsdokument
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

10.1 1. Zielbild und Strategie

10.1.1 1.1 Sicherheitsziele

AdminSend GmbH verfolgt folgende strategische Sicherheitsziele:

1. **[TODO: Ziel 1]:** [TODO: Beschreibung]
2. **[TODO: Ziel 2]:** [TODO: Beschreibung]
3. **[TODO: Ziel 3]:** [TODO: Beschreibung]

10.1.2 1.2 Prioritäten

Priorisierung nach: - Kritikalität (Schutzbedarf) - Risikohöhe - Compliance-Anforderungen - Quick Wins (Aufwand vs. Nutzen) - Abhängigkeiten

10.1.3 1.3 Architekturelle Leitplanken

Sicherheitsarchitektur-Prinzipien: - Defense in Depth (mehrschichtige Sicherheit) - Zero Trust (Verify explicitly, Least privilege, Assume breach) - Secure by Design - Privacy by Design - [TODO: Weitere Prinzipien]

10.2 2. Maßnahmenkatalog

10.2.1 2.1 Maßnahmen aus Basis-Sicherheitscheck

Maßnahme-ID	Quelle	Beschreibung	Priorität	Owner	Aufwand (PT)	Budget	Zieltermin	Abhängigkeiten	Status
M-001	Basis-Check (GAP-001)	[TODO: Kritische Maßnahme 1]	P1 - Kritisch	Thomas Weber	[TODO]	[TODO]	[TODO]	-	Offen
M-002	Basis-Check (QW-001)	[TODO: Quick Win 1]	P2 - Hoch	Anna Schmidt	[TODO]	[TODO]	[TODO]	-	Offen
M-003	Basis-Check	[TODO: Maßnahme 3]	P3 - Mittel	[TODO]	[TODO]	[TODO]	[TODO]	M-001	Offen
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

10.2.2 2.2 Maßnahmen aus Risikoanalyse

Maßnahme-ID	Quelle	Beschreibung	Priorität	Owner	Aufwand (PT)	Budget	Zieltermin	Abhängigkeiten	Status
M-101	Risikoanalyse (R-001)	[TODO: Risikominderung 1]	P1 - Kritisch	Anna Schmidt	[TODO]	[TODO]	[TODO]	-	Offen
M-102	Risikoanalyse (R-002)	[TODO: Risikominderung 2]	P2 - Hoch	Anna Schmidt	[TODO]	[TODO]	[TODO]	-	Offen
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

10.2.3 2.3 Strategische Maßnahmen

Maßnahme-ID	Beschreibung	Priorität	Owner	Aufwand (PT)	Budget	Zieltermin	Status
M-201	SIEM-Implementierung	P1 - Kritisch	Anna Schmidt	[TODO]	[TODO]	[TODO]	Offen

Maßnahme-ID	Beschreibung	Priorität	Owner	Aufwand (PT)	Budget	Zieltermin	Status
M-202	Zero Trust Architecture	P2 - Hoch	Anna Schmidt	[TODO]	[TODO]	[TODO]	Offen
M-203	Security Awareness Programm	P2 - Hoch	Thomas Weber	[TODO]	[TODO]	[TODO]	Offen
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

10.3 3. Maßnahmen-Priorisierung

10.3.1 3.1 Priorität 1 - Kritisch (Sofort)

Maßnahme-ID	Beschreibung	Owner	Zieltermin	Abhängigkeiten
M-001	[TODO]	[TODO]	[TODO]	-
M-101	[TODO]	[TODO]	[TODO]	-
M-201	[TODO]	[TODO]	[TODO]	-

Anzahl: [TODO]
Gesamtaufwand: [TODO] PT
Gesamtbudget: [TODO] €

10.3.2 3.2 Priorität 2 - Hoch (Kurzfristig, 0-6 Monate)

Maßnahme-ID	Beschreibung	Owner	Zieltermin	Abhängigkeiten
M-002	[TODO]	[TODO]	[TODO]	-
M-102	[TODO]	[TODO]	[TODO]	M-001
M-202	[TODO]	[TODO]	[TODO]	M-201

Anzahl: [TODO]
Gesamtaufwand: [TODO] PT
Gesamtbudget: [TODO] €

10.3.3 3.3 Priorität 3 - Mittel (Mittelfristig, 6-12 Monate)

Maßnahme-ID	Beschreibung	Owner	Zieltermin	Abhängigkeiten
M-003	[TODO]	[TODO]	[TODO]	M-001
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Anzahl: [TODO]
Gesamtaufwand: [TODO] PT
Gesamtbudget: [TODO] €

10.3.4 3.4 Priorität 4 - Niedrig (Langfristig, > 12 Monate)

Maßnahme-ID	Beschreibung	Owner	Zieltermin	Abhängigkeiten
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Anzahl: [TODO]
Gesamtaufwand: [TODO] PT
Gesamtbudget: [TODO] €

10.4 4. Roadmap

10.4.1 4.1 Quartal 1 (Q1 {{ meta.document.year }})

Fokus: Kritische Sicherheitslücken schließen

Maßnahme-ID	Beschreibung	Owner	Status
M-001	[TODO]	[TODO]	Geplant
M-101	[TODO]	[TODO]	Geplant

10.4.2 4.2 Quartal 2 (Q2 {{ meta.document.year }})

Fokus: Quick Wins und Basis-Sicherheit

Maßnahme-ID	Beschreibung	Owner	Status
M-002	[TODO]	[TODO]	Geplant
M-201	[TODO]	[TODO]	Geplant

10.4.3 4.3 Quartal 3 (Q3 {{ meta.document.year }})

Fokus: Strategische Maßnahmen

Maßnahme-ID	Beschreibung	Owner	Status
M-202	[TODO]	[TODO]	Geplant
M-203	[TODO]	[TODO]	Geplant

10.4.4 4.4 Quartal 4 (Q4 {{ meta.document.year }})

Fokus: Konsolidierung und Optimierung

Maßnahme-ID	Beschreibung	Owner	Status
M-003	[TODO]	[TODO]	Geplant
[TODO]	[TODO]	[TODO]	Geplant

10.5 5. Ressourcenplanung

10.5.1 5.1 Personalressourcen

Rolle	Aufwand (PT)	Verfügbarkeit	Lücke
ISB	[TODO]	[TODO]	[TODO]
IT-Leitung	[TODO]	[TODO]	[TODO]
IT-Administratoren	[TODO]	[TODO]	[TODO]
Externe Berater	[TODO]	[TODO]	[TODO]
Gesamt	**[TODO]**	**[TODO]**	**[TODO]**

10.5.2 5.2 Budget

Kategorie	Budget	Verwendung
Software-Lizenzen	[TODO] €	SIEM, PAM, EDR, etc.
Hardware	[TODO] €	Firewalls, Server, etc.
Externe Dienstleistungen	[TODO] €	Beratung, Implementierung
Schulungen	[TODO] €	Awareness, technische Schulungen
Sonstiges	[TODO] €	[TODO]
Gesamt	**[TODO] €**	

10.5.3 5.3 Externe Unterstützung

Dienstleister	Leistung	Aufwand	Budget	Zeitraum
[TODO: Dienstleister 1]	[TODO]	[TODO] PT	[TODO] €	[TODO]
[TODO: Dienstleister 2]	[TODO]	[TODO] PT	[TODO] €	[TODO]

10.6 6. Abhängigkeiten und Risiken

10.6.1 6.1 Kritische Abhängigkeiten

Maßnahme	Abhängigkeit	Auswirkung	Mitigation
M-202 (Zero Trust)	M-201 (SIEM)	Verzögerung	Parallele Planung
[TODO]	[TODO]	[TODO]	[TODO]

10.6.2 6.2 Umsetzungsrisiken

Risiko	Wahrscheinlichkeit	Auswirkung	Mitigation	Owner
Ressourcenmangel	Hoch	Verzögerung	Externe Unterstützung	Thomas Weber
Budget-Kürzung	Mittel	Priorisierung	Fokus auf P1-Maßnahmen	Max Mustermann
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

10.7 7. Erfolgsmessung

10.7.1 7.1 Erfolgskriterien

Kriterium	Ziel	Messung
Maßnahmenumsetzung	100% P1-Maßnahmen bis [TODO]	Maßnahmenplan-Tracking
Erfüllungsgrad IT-Grundschutz	> 80% bis [TODO]	Basis-Sicherheitscheck
Risikoreduktion	Keine “Sehr hoch”-Risiken	Risikoregister
[TODO]	[TODO]	[TODO]

10.7.2 7.2 Meilensteine

Meilenstein	Datum	Kriterium	Status
M1: Kritische Lücken geschlossen	[TODO]	Alle P1-Maßnahmen umgesetzt	Geplant
M2: Basis-Sicherheit erreicht	[TODO]	80% Erfüllungsgrad	Geplant
M3: Strategische Maßnahmen umgesetzt	[TODO]	SIEM, Zero Trust produktiv	Geplant
M4: IT-Grundschutz-Zertifizierung	[TODO]	Zertifizierung erhalten	Geplant

10.8 8. Governance und Steuerung

Steuerungsgremium: ISMS-Team (siehe Dokument 0020)

Regeltermine: - **Wöchentlich:** Maßnahmen-Status-Update (ISB, IT-Leitung) - **Monatlich:** ISMS-Team-Meeting (Fortschritt, Eskalationen) - **Quartalsweise:** Management-Review (Geschäftsführung)

Reporting: Siehe Dokument 0110 (Umsetzungssteuerung und KPIs)

10.9 9. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI Standard 200-2: IT-Grundschutz-Methodik - Dokument 0080: Basis-Sicherheitscheck - Dokument 0090: Risikoanalyse

ewpage

Chapter 11

Umsetzungssteuerung, Reporting und KPIs

Dokument-ID: 0110
Dokumenttyp: Steuerungsdokument
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

11.1 1. Steuerungsmodell

11.1.1 1.1 Governance-Struktur

ISMS-Steuerung erfolgt auf drei Ebenen:

Ebene	Gremium	Frequenz	Teilnehmer	Fokus
Strategisch	Management Review	Jährlich	Geschäftsführung, ISB, IT-Leitung	Strategische Ausrichtung, Ressourcen
Taktisch	ISMS-Team-Meeting	Monatlich	ISB, IT-Leitung, Informationsverbund-Verantwortliche	Maßnahmenplanung, Risiken
Operativ	Maßnahmen-Status-Update	Wöchentlich	ISB, IT-Leitung, Maßnahmen-Owner	Umsetzungsfortschritt

11.1.2 1.2 Regeltermine

Wöchentlich - Maßnahmen-Status-Update: - **Termin:** [TODO: z.B. Montag 10:00] - **Dauer:** 30 Minuten - **Teilnehmer:** ISB, IT-Leitung, aktuelle Maßnahmen-Owner - **Agenda:** Status laufender Maßnahmen, Blocker, Eskalationen

Monatlich - ISMS-Team-Meeting: - **Termin:** [TODO: z.B. erster Donnerstag im Monat, 14:00] - **Dauer:** 2 Stunden - **Teilnehmer:** ISMS-Team (siehe Dokument 0020) - **Agenda:** - KPI-Review - Maßnahmenfortschritt - Neue Risiken und Vorfälle - Compliance-Updates - Entscheidungen und Eskalationen

Quartalsweise - Management-Review: - **Termin:** [TODO: z.B. letzter Freitag im Quartal] - **Dauer:** 1 Stunde - **Teilnehmer:** Geschäftsführung, ISB, IT-Leitung - **Agenda:** - ISMS-Performance (KPIs) - Maßnahmenumsetzung - Risiko-Dashboard - Budget und Ressourcen - Strategische Entscheidungen

Jährlich - Management Review (umfassend): - **Termin:** [TODO: z.B. Q4] - **Dauer:** Halber Tag - **Teilnehmer:** Geschäftsführung, ISB, IT-Leitung, ISMS-Team - **Agenda:** Siehe Dokument 0140 (Management Review Template)

11.1.3 1.3 Reporting-Kanäle

Bericht	Frequenz	Ersteller	Empfänger	Tool/Format
Maßnahmen-Status	Wöchentlich	ISB	IT-Leitung	[TODO: Ticketing-System]
ISMS-Status-Report	Monatlich	ISB	Geschäftsführung, ISMS-Team	[TODO: Dashboard/PDF]
Sicherheitsvorfälle	Monatlich	ISB	Geschäftsführung	[TODO: Incident-Tool]
Risiko-Dashboard	Quartalsweise	ISB	Geschäftsführung	[TODO: GRC-Tool]
Management Review	Jährlich	ISB	Geschäftsführung	Präsentation

11.2 2. Key Performance Indicators (KPIs)

11.2.1 2.1 Maßnahmenumsetzung

KPI	Definition	Ziel	Quelle	Frequenz	Owner
Maßnahmenplan-Erfüllung	% abgeschlossene Maßnahmen vs. geplant	100%	Maßnahmenplan (Dokument 0100)	Monatlich	Thomas Weber
P1-Maßnahmen-Erfüllung	% abgeschlossene P1-Maßnahmen	100% in [TODO] Monaten	Maßnahmenplan	Wöchentlich	Thomas Weber

KPI	Definition	Ziel	Quelle	Frequenz	Owner
Maßnahmen-Verzögerung	Durchschnittliche Verzögerung in Tagen	< 14 Tage	Maßnahmenplan	Monatlich	Thomas Weber
Budget-Einhaltung	% genutztes Budget vs. geplant	100% ± 10%	Finanzcontrolling	Monatlich	Max Mustermann

11.2.2 2.2 IT-Grundschutz-Compliance

KPI	Definition	Ziel	Quelle	Frequenz	Owner
Erfüllungsgrad IT-Grundschutz	% erfüllte Anforderungen	> 80%	Basis-Sicherheitscheck (Dokument 0080)	Quartalsweise	Thomas Weber
Kritische Lücken	Anzahl nicht erfüllter P1-Anforderungen	0	Basis-Sicherheitscheck	Monatlich	Thomas Weber
Baustein-Abdeckung	% modellierte Bausteine mit Soll-Ist-Vergleich	100%	Modellierung (Dokument 0070)	Quartalsweise	Thomas Weber

11.2.3 2.3 Risikomanagement

KPI	Definition	Ziel	Quelle	Frequenz	Owner
Risiko-Exposition	Anzahl "Sehr hoch"-Risiken	0	Risikoregister (Dokument 0090)	Monatlich	Thomas Weber
Risikoreduktion	% reduzierte Risiken vs. identifiziert	> 80%	Risikoregister	Quartalsweise	Thomas Weber
Risikoakzeptanz-Quote	% akzeptierte Risiken (ohne Maßnahmen)	< 10%	Risikoregister	Quartalsweise	Thomas Weber

11.2.4 2.4 Patch- und Vulnerability Management

KPI	Definition	Ziel	Quelle	Frequenz	Owner
Patch-Compliance	% Systeme mit aktuellen Patches	> 95%	Patch-Management-Tool	Monatlich	Anna Schmidt

KPI	Definition	Ziel	Quelle	Frequenz	Owner
Kritische Patches (SLA)	% kritische Patches innerhalb SLA (7 Tage)	100%	Patch-Management-Tool	Wöchentlich	Anna Schmidt
Vulnerability-Remediation	Durchschnittliche Zeit bis Behebung (Tage)	< 30 Tage (Hoch), < 90 Tage (Mittel)	Vulnerability Scanner	Monatlich	Anna Schmidt
Offene Schwachstellen	Anzahl offener Schwachstellen (Kritisch/Hoch)	< 10	Vulnerability Scanner	Wöchentlich	Anna Schmidt

11.2.5 2.5 Backup und Recovery

KPI	Definition	Ziel	Quelle	Frequenz	Owner
Backup-Erfolgsrate	% erfolgreiche Backups	> 99%	Backup-System	Täglich	Anna Schmidt
Backup-Testquote	% erfolgreiche Restore-Tests	100%	Test-Protokolle	Quartalsweise	Anna Schmidt
Recovery Time Actual (RTA)	Tatsächliche Wiederherstellungszeit	< RTO	Test-Protokolle	Quartalsweise	Anna Schmidt

11.2.6 2.6 Incident Management

KPI	Definition	Ziel	Quelle	Frequenz	Owner
Sicherheitsvorfälle	Anzahl Sicherheitsvorfälle	Trend abnehmend	Incident-Management-System	Monatlich	Thomas Weber
Mean Time to Detect (MTTD)	Durchschnittliche Erkennungszeit	< 24 Stunden	SIEM	Monatlich	Anna Schmidt
Mean Time to Respond (MTTR)	Durchschnittliche Reaktionszeit	< 4 Stunden (Kritisch)	Incident-Management-System	Monatlich	Thomas Weber
Incident-Closure-Rate	% geschlossene Incidents innerhalb SLA	> 95%	Incident-Management-System	Monatlich	Thomas Weber

11.2.7 2.7 Awareness und Schulung

KPI	Definition	Ziel	Quelle	Frequenz	Owner
Schulungsquote	% Mitarbeitende mit Awareness-Schulung	100%	HR-System	Quartalsweise	Thomas Weber
Phishing-Test-Erfolgsrate	% Mitarbeitende, die Phishing-Test bestehen	> 90%	Phishing-Simulation	Quartalsweise	Thomas Weber
Security-Champion-Quote	Anzahl Security Champions pro Abteilung	Min. 1 pro Abteilung	ISMS-Team	Jährlich	Thomas Weber

11.2.8 2.8 Access Management

KPI	Definition	Ziel	Quelle	Frequenz	Owner
Privileged Account Compliance	% privilegierte Accounts mit MFA	100%	IAM-System	Monatlich	Anna Schmidt
Access Review Compliance	% durchgeführte Zugriffsrezertifizierungen	100%	IAM-System	Quartalsweise	Anna Schmidt
Orphaned Accounts	Anzahl verwaister Accounts	0	IAM-System	Monatlich	Anna Schmidt

11.3 3. KPI-Dashboard

11.3.1 3.1 Ampel-Status

KPI-Kategorie	Aktueller Wert	Ziel	Status	Trend
Maßnahmenumsetzung	[TODO: %]	100%	/ /	/→/
IT-Grundschutz-Compliance	[TODO: %]	> 80%	/ /	/→/
Risikomanagement	[TODO]	0 “Sehr hoch”	/ /	/→/
Patch-Compliance	[TODO: %]	> 95%	/ /	/→/
Backup-Erfolgsrate	[TODO: %]	> 99%	/ /	/→/
Sicherheitsvorfälle	[TODO]	Trend	/ /	/→/
Awareness-Schulung	[TODO: %]	100%	/ /	/→/

Ampel-Logik: - **Grün:** Ziel erreicht oder übertroffen - **Gelb:** Ziel nicht erreicht, aber akzeptabel (< 10% Abweichung) - **Rot:** Ziel deutlich verfehlt (> 10% Abweichung), Eskalation erforderlich

11.3.2 3.2 Trend-Analyse

[TODO: Diagramme und Trend-Visualisierungen einfügen]

11.4 4. Eskalationsregeln

11.4.1 4.1 Eskalationsstufen

Stufe	Trigger	Eskalation an	Reaktionszeit	Maßnahmen
Stufe 1	KPI für 1 Monat	IT-Leitung	1 Woche	Ursachenanalyse, Korrekturmaßnahmen
Stufe 2	KPI oder für 2 Monate	ISB	3 Tage	Eskalationsmeeting, Ressourcen prüfen
Stufe 3	KPI für 1 Monat	Geschäftsführung	Sofort	Management-Entscheidung, Ressourcen freigeben

11.4.2 4.2 Eskalationsprozess

1. **Identifikation:** KPI-Abweichung wird erkannt
2. **Analyse:** Ursachenanalyse durch Owner
3. **Eskalation:** Eskalation gemäß Stufe
4. **Maßnahmen:** Korrekturmaßnahmen definieren und umsetzen
5. **Monitoring:** Engmaschiges Monitoring bis Zielerreichung
6. **Lessons Learned:** Dokumentation und Prozessverbesserung

11.5 5. Reporting-Templates

11.5.1 5.1 Monatlicher ISMS-Status-Report

Berichtsstruktur: 1. **Executive Summary:** Gesamtstatus (1 Seite) 2. **KPI-Dashboard:** Ampel-Status und Trends 3. **Maßnahmenfortschritt:** Top 10 Maßnahmen 4. **Sicherheitsvorfälle:** Zusammenfassung 5. **Risiken:** Top 5 Risiken 6. **Eskalationen:** Offene Eskalationen 7. **Nächste Schritte:** Geplante Aktivitäten

11.5.2 5.2 Quartalsweises Risiko-Dashboard

Berichtsstruktur: 1. **Risiko-Heatmap:** Visualisierung aller Risiken 2. **Top 10 Risiken:** Detailbeschreibung 3. **Risikoreduktion:** Fortschritt seit letztem Quartal 4. **Neue Risiken:** Identifizierte neue Risiken 5. **Risikoakzeptanz:** Akzeptierte Risiken mit Begründung

11.5.3 5.3 Jährliches Management Review

Berichtsstruktur: Siehe Dokument 0140 (Management Review Template)

11.6 6. Continuous Improvement

11.6.1 6.1 Verbesserungsprozess

PDCA-Zyklus: 1. **Plan:** Ziele und KPIs definieren 2. **Do:** Maßnahmen umsetzen 3. **Check:** KPIs messen und bewerten 4. **Act:** Verbesserungsmaßnahmen ableiten

11.6.2 6.2 Lessons Learned

Nach jedem größeren Vorfall oder Projekt: 1. **Retrospektive:** Was lief gut? Was nicht? 2. **Root Cause Analysis:** Ursachen identifizieren 3. **Verbesserungsmaßnahmen:** Konkrete Maßnahmen definieren 4. **Dokumentation:** Lessons Learned dokumentieren 5. **Kommunikation:** Erkenntnisse teilen

11.7 7. Tools und Systeme

Tool/System	Zweck	Owner	Status
[TODO: GRC-Tool]	Risikomanagement, Compliance	Thomas Weber	[TODO]
[TODO: Ticketing-System]	Maßnahmentracking	Anna Schmidt	[TODO]
[TODO: SIEM]	Security Monitoring	Anna Schmidt	[TODO]
[TODO: Vulnerability Scanner]	Schwachstellen-Management	Anna Schmidt	[TODO]
[TODO: Dashboard-Tool]	KPI-Visualisierung	Thomas Weber	[TODO]

11.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI Standard 200-1: Managementsysteme für Informationssicherheit (ISMS) - BSI Standard 200-2: IT-Grundschutz-Methodik

ewpage

Chapter 12

Policy: Zugriffssteuerung und Berechtigungen

Dokument-ID: 0200
Dokumenttyp: Policy (abstrakt)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

12.1 1. Zweck und Zielsetzung

Diese Policy definiert die Grundsätze für Zugriffssteuerung und Berechtigungen bei **AdminSend GmbH**.

Verantwortlich: Thomas Weber (ISB)

[TODO: Spezifische Zielsetzung ergänzen]

12.2 2. Geltungsbereich

Diese Policy gilt für: - Alle Mitarbeitenden von AdminSend GmbH - Alle IT-Systeme und Anwendungen - Alle Standorte: {{ meta.organization.locations }} - Externe Dienstleister mit Zugriff auf Systeme

Ausnahmen: - Ausnahmen sind nur über den Ausnahmenprozess (Dokument 0520) möglich - [TODO: Spezifische Ausnahmen dokumentieren]

12.3 3. Grundsätze

[TODO: Definieren Sie die strategischen Grundsätze für Zugriffssteuerung und Berechtigungen]

Beispielhafte Grundsätze: 1. **Grundsatz 1:** [TODO] 2. **Grundsatz 2:** [TODO] 3. **Grundsatz 3:** [TODO]

12.4 4. Verantwortlichkeiten

Rolle	Verantwortung	Name
Policy Owner	Gesamtverantwortung für Policy	Thomas Weber
Umsetzungsverantwortliche	Technische Umsetzung	Anna Schmidt
Kontrolle/Audit	Überwachung der Einhaltung	[TODO: Internal Audit]
Alle Mitarbeitenden	Einhaltung der Policy	Alle

12.5 5. Abgeleitete Richtlinien und Standards

Diese Policy wird konkretisiert durch: - **Richtlinie 0210:** Richtlinie: IAM Joiner Mover Leaver und Rezertifizierung - [TODO: Weitere Richtlinien und Standards]

12.6 6. Nachweise und Kontrolle

Evidence/Nachweise: - [TODO: Definieren Sie erforderliche Nachweise] - Beispiele: Konfigurationsnachweise, Logs, Audit-Berichte

Review-Intervall: - Diese Policy wird jährlich oder bei wesentlichen Änderungen überprüft - **Nächster Review:** {{ meta.document.next_review }}

12.7 7. Konsequenzen bei Verstößen

Verstöße gegen diese Policy können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

12.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Rolle	Name	Datum	Freigabe
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Dokument 0210: Richtlinie: IAM Joiner Mover Leaver und Rezertifizierung

ewpage

Chapter 13

Richtlinie: IAM Joiner Mover Leaver und Rezertifizierung

Dokument-ID: 0210
Dokumenttyp: Richtlinie/Standard (konkret)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

13.1 1. Zweck und Bezug

Diese Richtlinie konkretisiert die **Policy 0200: Policy: Zugriffssteuerung und Berechtigungen** und definiert spezifische Anforderungen für IAM-Prozesse.

Verantwortlich: Anna Schmidt (IT-Leitung)

[TODO: Spezifische Zielsetzung ergänzen]

13.2 2. Geltungsbereich

Systeme/Plattformen: - [TODO: Definieren Sie betroffene Systeme] - Beispiele: Active Directory, Cloud-Plattformen, Anwendungen

Zielgruppen: - IT-Administratoren - System-Owner - [TODO: Weitere Zielgruppen]

13.3 3. Mindestanforderungen (MUSS)

[TODO: Definieren Sie zwingende Anforderungen]

Beispielhafte MUSS-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO] 3. **Anforderung 3:** [TODO]

13.4 4. Empfohlene Anforderungen (SOLL)

[TODO: Definieren Sie empfohlene Anforderungen]

Beispielhafte SOLL-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO]

13.5 5. Prozess und Umsetzung

13.5.1 5.1 Prozessschritte

[TODO: Definieren Sie den Prozess]

Beispielhafter Prozess: 1. **Antrag:** [TODO] 2. **Genehmigung:** [TODO] 3. **Umsetzung:** [TODO] 4. **Review:** [TODO]

13.5.2 5.2 Tooling und Systeme

Verwendete Tools: - [TODO: Tool 1] - [TODO: Tool 2]

Verantwortlich: Anna Schmidt

13.6 6. Nachweise (Evidence)

Erforderliche Nachweise: - [TODO: Nachweis 1] - [TODO: Nachweis 2]

Aufbewahrungsdauer: [TODO: z.B. 3 Jahre]

13.7 7. Ausnahmen

Ausnahmen von dieser Richtlinie sind nur über den **Ausnahmenprozess (Dokument 0520)** möglich.

Ausnahmeantrag an: Thomas Weber (ISB)

13.8 8. Schulung und Awareness

[TODO: Definieren Sie Schulungsanforderungen]

Zielgruppe: [TODO]
Frequenz: [TODO]
Verantwortlich: Thomas Weber

13.9 9. Review und Aktualisierung

Diese Richtlinie wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Verantwortlich:** Anna Schmidt - **Nächster Review:** {{ meta.document.next_review }}

13.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - Dokument 0200: Policy: Zugriffssteuerung und Berechtigungen

ewpage

Chapter 14

Policy: Authentisierung und MFA

Dokument-ID: 0220
Dokumenttyp: Policy (abstrakt)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

14.1 1. Zweck und Zielsetzung

Diese Policy definiert die Grundsätze für Authentisierung und MFA bei **AdminSend GmbH**.

Verantwortlich: Thomas Weber (ISB)

[TODO: Spezifische Zielsetzung ergänzen]

14.2 2. Geltungsbereich

Diese Policy gilt für: - Alle Mitarbeitenden von AdminSend GmbH - Alle IT-Systeme und Anwendungen - Alle Standorte: {{ meta.organization.locations }} - Externe Dienstleister mit Zugriff auf Systeme

Ausnahmen: - Ausnahmen sind nur über den Ausnahmenprozess (Dokument 0520) möglich - [TODO: Spezifische Ausnahmen dokumentieren]

14.3 3. Grundsätze

[TODO: Definieren Sie die strategischen Grundsätze für Authentisierung und MFA]

Beispielhafte Grundsätze: 1. **Grundsatz 1:** [TODO] 2. **Grundsatz 2:** [TODO] 3. **Grundsatz 3:** [TODO]

14.4 4. Verantwortlichkeiten

Rolle	Verantwortung	Name
Policy Owner	Gesamtverantwortung für Policy	Thomas Weber
Umsetzungsverantwortliche	Technische Umsetzung	Anna Schmidt
Kontrolle/Audit	Überwachung der Einhaltung	[TODO: Internal Audit]
Alle Mitarbeitenden	Einhaltung der Policy	Alle

14.5 5. Abgeleitete Richtlinien und Standards

Diese Policy wird konkretisiert durch: - **Richtlinie 0230:** Richtlinie: Passwort MFA und Sitzungsregeln - [TODO: Weitere Richtlinien und Standards]

14.6 6. Nachweise und Kontrolle

Evidence/Nachweise: - [TODO: Definieren Sie erforderliche Nachweise] - Beispiele: Konfigurationsnachweise, Logs, Audit-Berichte

Review-Intervall: - Diese Policy wird jährlich oder bei wesentlichen Änderungen überprüft - **Nächster Review:** {{ meta.document.next_review }}

14.7 7. Konsequenzen bei Verstößen

Verstöße gegen diese Policy können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

14.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Dokument 0230: Richtlinie: Passwort MFA und Sitzungsregeln

ewpage

Chapter 15

Richtlinie: Passwort MFA und Sitzungsregeln

Dokument-ID: 0230
Dokumenttyp: Richtlinie/Standard (konkret)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

15.1 1. Zweck und Bezug

Diese Richtlinie konkretisiert die **Policy 0220: Policy: Authentisierung und MFA** und definiert spezifische Anforderungen für Passwort- und MFA-Anforderungen.

Verantwortlich: Anna Schmidt (IT-Leitung)

[TODO: Spezifische Zielsetzung ergänzen]

15.2 2. Geltungsbereich

Systeme/Plattformen: - [TODO: Definieren Sie betroffene Systeme] - Beispiele: Active Directory, Cloud-Plattformen, Anwendungen

Zielgruppen: - IT-Administratoren - System-Owner - [TODO: Weitere Zielgruppen]

15.3 3. Mindestanforderungen (MUSS)

[TODO: Definieren Sie zwingende Anforderungen]

Beispielhafte MUSS-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO] 3. **Anforderung 3:** [TODO]

15.4 4. Empfohlene Anforderungen (SOLL)

[TODO: Definieren Sie empfohlene Anforderungen]

Beispielhafte SOLL-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO]

15.5 5. Prozess und Umsetzung

15.5.1 5.1 Prozessschritte

[TODO: Definieren Sie den Prozess]

Beispielhafter Prozess: 1. **Antrag:** [TODO] 2. **Genehmigung:** [TODO] 3. **Umsetzung:** [TODO] 4. **Review:** [TODO]

15.5.2 5.2 Tooling und Systeme

Verwendete Tools: - [TODO: Tool 1] - [TODO: Tool 2]

Verantwortlich: Anna Schmidt

15.6 6. Nachweise (Evidence)

Erforderliche Nachweise: - [TODO: Nachweis 1] - [TODO: Nachweis 2]

Aufbewahrungsdauer: [TODO: z.B. 3 Jahre]

15.7 7. Ausnahmen

Ausnahmen von dieser Richtlinie sind nur über den **Ausnahmenprozess (Dokument 0520)** möglich.

Ausnahmeantrag an: Thomas Weber (ISB)

15.8 8. Schulung und Awareness

[TODO: Definieren Sie Schulungsanforderungen]

Zielgruppe: [TODO]
Frequenz: [TODO]
Verantwortlich: Thomas Weber

15.9 9. Review und Aktualisierung

Diese Richtlinie wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Verantwortlich:** Anna Schmidt - **Nächster Review:** {{ meta.document.next_review }}

15.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - Dokument 0220: Policy: Authentisierung und MFA

ewpage

Chapter 16

Policy: Asset und Inventarmanagement

Dokument-ID: 0240
Dokumenttyp: Policy (abstrakt)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

16.1 1. Zweck und Zielsetzung

Diese Policy definiert die Grundsätze für Asset-Management bei **AdminSend GmbH**.

Verantwortlich: Thomas Weber (ISB)

[TODO: Spezifische Zielsetzung ergänzen]

16.2 2. Geltungsbereich

Diese Policy gilt für: - Alle Mitarbeitenden von AdminSend GmbH - Alle IT-Systeme und Anwendungen - Alle Standorte: {{ meta.organization.locations }} - Externe Dienstleister mit Zugriff auf Systeme

Ausnahmen: - Ausnahmen sind nur über den Ausnahmenprozess (Dokument 0520) möglich - [TODO: Spezifische Ausnahmen dokumentieren]

16.3 3. Grundsätze

[TODO: Definieren Sie die strategischen Grundsätze für Asset-Management]

Beispielhafte Grundsätze: 1. **Grundsatz 1:** [TODO] 2. **Grundsatz 2:** [TODO] 3. **Grundsatz 3:** [TODO]

16.4 4. Verantwortlichkeiten

Rolle	Verantwortung	Name
Policy Owner	Gesamtverantwortung für Policy	Thomas Weber
Umsetzungsverantwortliche	Technische Umsetzung	Anna Schmidt
Kontrolle/Audit	Überwachung der Einhaltung	[TODO: Internal Audit]
Alle Mitarbeitenden	Einhaltung der Policy	Alle

16.5 5. Abgeleitete Richtlinien und Standards

Diese Policy wird konkretisiert durch: - **Richtlinie 0250:** Richtlinie: Asset Lifecycle Tagging und Entsorgung - [TODO: Weitere Richtlinien und Standards]

16.6 6. Nachweise und Kontrolle

Evidence/Nachweise: - [TODO: Definieren Sie erforderliche Nachweise] - Beispiele: Konfigurationsnachweise, Logs, Audit-Berichte

Review-Intervall: - Diese Policy wird jährlich oder bei wesentlichen Änderungen überprüft - **Nächster Review:** {{ meta.document.next_review }}

16.7 7. Konsequenzen bei Verstößen

Verstöße gegen diese Policy können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

16.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Dokument 0250: Richtlinie: Asset Lifecycle Tagging und Entsorgung

ewpage

Chapter 17

Richtlinie: Asset Lifecycle Tagging und Entsorgung

Dokument-ID: 0250
Dokumenttyp: Richtlinie/Standard (konkret)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

17.1 1. Zweck und Bezug

Diese Richtlinie konkretisiert die **Policy 0240: Policy: Asset und Inventarmanagement** und definiert spezifische Anforderungen für Asset-Lifecycle.

Verantwortlich: Anna Schmidt (IT-Leitung)

[TODO: Spezifische Zielsetzung ergänzen]

17.2 2. Geltungsbereich

Systeme/Plattformen: - [TODO: Definieren Sie betroffene Systeme] - Beispiele: Active Directory, Cloud-Plattformen, Anwendungen

Zielgruppen: - IT-Administratoren - System-Owner - [TODO: Weitere Zielgruppen]

17.3 3. Mindestanforderungen (MUSS)

[TODO: Definieren Sie zwingende Anforderungen]

Beispielhafte MUSS-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO] 3. **Anforderung 3:** [TODO]

17.4 4. Empfohlene Anforderungen (SOLL)

[TODO: Definieren Sie empfohlene Anforderungen]

Beispielhafte SOLL-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO]

17.5 5. Prozess und Umsetzung

17.5.1 5.1 Prozessschritte

[TODO: Definieren Sie den Prozess]

Beispielhafter Prozess: 1. **Antrag:** [TODO] 2. **Genehmigung:** [TODO] 3. **Umsetzung:** [TODO] 4. **Review:** [TODO]

17.5.2 5.2 Tooling und Systeme

Verwendete Tools: - [TODO: Tool 1] - [TODO: Tool 2]

Verantwortlich: Anna Schmidt

17.6 6. Nachweise (Evidence)

Erforderliche Nachweise: - [TODO: Nachweis 1] - [TODO: Nachweis 2]

Aufbewahrungsdauer: [TODO: z.B. 3 Jahre]

17.7 7. Ausnahmen

Ausnahmen von dieser Richtlinie sind nur über den **Ausnahmenprozess (Dokument 0520)** möglich.

Ausnahmeantrag an: Thomas Weber (ISB)

17.8 8. Schulung und Awareness

[TODO: Definieren Sie Schulungsanforderungen]

Zielgruppe: [TODO]
Frequenz: [TODO]
Verantwortlich: Thomas Weber

17.9 9. Review und Aktualisierung

Diese Richtlinie wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Verantwortlich:** Anna Schmidt - **Nächster Review:** {{ meta.document.next_review }}

17.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - Dokument 0240: Policy: Asset und Inventarmanagement

ewpage

Chapter 18

Policy: Konfiguration und Hardening

Dokument-ID: 0260
Dokumenttyp: Policy (abstrakt)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

18.1 1. Zweck und Zielsetzung

Diese Policy definiert die Grundsätze für System-Härtung bei **AdminSend GmbH**.

Verantwortlich: Thomas Weber (ISB)

[TODO: Spezifische Zielsetzung ergänzen]

18.2 2. Geltungsbereich

Diese Policy gilt für: - Alle Mitarbeitenden von AdminSend GmbH - Alle IT-Systeme und Anwendungen - Alle Standorte: {{ meta.organization.locations }} - Externe Dienstleister mit Zugriff auf Systeme

Ausnahmen: - Ausnahmen sind nur über den Ausnahmenprozess (Dokument 0520) möglich - [TODO: Spezifische Ausnahmen dokumentieren]

18.3 3. Grundsätze

[TODO: Definieren Sie die strategischen Grundsätze für System-Härtung]

Beispielhafte Grundsätze: 1. **Grundsatz 1:** [TODO] 2. **Grundsatz 2:** [TODO] 3. **Grundsatz 3:** [TODO]

18.4 4. Verantwortlichkeiten

Rolle	Verantwortung	Name
Policy Owner	Gesamtverantwortung für Policy	Thomas Weber
Umsetzungsverantwortliche	Technische Umsetzung	Anna Schmidt
Kontrolle/Audit	Überwachung der Einhaltung	[TODO: Internal Audit]
Alle Mitarbeitenden	Einhaltung der Policy	Alle

18.5 5. Abgeleitete Richtlinien und Standards

Diese Policy wird konkretisiert durch: - **Richtlinie 0270:** Richtlinie: Sicherheitsbaselines und Abweichungsmanagement - [TODO: Weitere Richtlinien und Standards]

18.6 6. Nachweise und Kontrolle

Evidence/Nachweise: - [TODO: Definieren Sie erforderliche Nachweise] - Beispiele: Konfigurationsnachweise, Logs, Audit-Berichte

Review-Intervall: - Diese Policy wird jährlich oder bei wesentlichen Änderungen überprüft - **Nächster Review:** {{ meta.document.next_review }}

18.7 7. Konsequenzen bei Verstößen

Verstöße gegen diese Policy können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

18.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Dokument 0270: Richtlinie: Sicherheitsbaselines und Abweichungsmanagement

ewpage

Chapter 19

Richtlinie: Sicherheitsbaselines und Abweichungsmanagement

Dokument-ID: 0270
Dokumenttyp: Richtlinie/Standard (konkret)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

19.1 1. Zweck und Bezug

Diese Richtlinie konkretisiert die **Policy 0260: Policy: Konfiguration und Hardening** und definiert spezifische Anforderungen für Sicherheitsbaselines.

Verantwortlich: Anna Schmidt (IT-Leitung)

[TODO: Spezifische Zielsetzung ergänzen]

19.2 2. Geltungsbereich

Systeme/Plattformen: - [TODO: Definieren Sie betroffene Systeme] - Beispiele: Active Directory, Cloud-Plattformen, Anwendungen

Zielgruppen: - IT-Administratoren - System-Owner - [TODO: Weitere Zielgruppen]

19.3 3. Mindestanforderungen (MUSS)

[TODO: Definieren Sie zwingende Anforderungen]

Beispielhafte MUSS-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO] 3. **Anforderung 3:** [TODO]

19.4 4. Empfohlene Anforderungen (SOLL)

[TODO: Definieren Sie empfohlene Anforderungen]

Beispielhafte SOLL-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO]

19.5 5. Prozess und Umsetzung

19.5.1 5.1 Prozessschritte

[TODO: Definieren Sie den Prozess]

Beispielhafter Prozess: 1. **Antrag:** [TODO] 2. **Genehmigung:** [TODO] 3. **Umsetzung:** [TODO] 4. **Review:** [TODO]

19.5.2 5.2 Tooling und Systeme

Verwendete Tools: - [TODO: Tool 1] - [TODO: Tool 2]

Verantwortlich: Anna Schmidt

19.6 6. Nachweise (Evidence)

Erforderliche Nachweise: - [TODO: Nachweis 1] - [TODO: Nachweis 2]

Aufbewahrungsdauer: [TODO: z.B. 3 Jahre]

19.7 7. Ausnahmen

Ausnahmen von dieser Richtlinie sind nur über den **Ausnahmenprozess (Dokument 0520)** möglich.

Ausnahmeantrag an: Thomas Weber (ISB)

19.8 8. Schulung und Awareness

[TODO: Definieren Sie Schulungsanforderungen]

Zielgruppe: [TODO]
Frequenz: [TODO]
Verantwortlich: Thomas Weber

19.9 9. Review und Aktualisierung

Diese Richtlinie wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Verantwortlich:** Anna Schmidt - **Nächster Review:** {{ meta.document.next_review }}

19.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - Dokument 0260: Policy: Konfiguration und Hardening

ewpage

Chapter 20

Policy: Patch und Vulnerability Management

Dokument-ID: 0280
Dokumenttyp: Policy (abstrakt)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

20.1 1. Zweck und Zielsetzung

Diese Policy definiert die Grundsätze für Patch-Management bei **AdminSend GmbH**.

Verantwortlich: Thomas Weber (ISB)

[TODO: Spezifische Zielsetzung ergänzen]

20.2 2. Geltungsbereich

Diese Policy gilt für: - Alle Mitarbeitenden von AdminSend GmbH - Alle IT-Systeme und Anwendungen - Alle Standorte: {{ meta.organization.locations }} - Externe Dienstleister mit Zugriff auf Systeme

Ausnahmen: - Ausnahmen sind nur über den Ausnahmenprozess (Dokument 0520) möglich - [TODO: Spezifische Ausnahmen dokumentieren]

20.3 3. Grundsätze

[TODO: Definieren Sie die strategischen Grundsätze für Patch-Management]

Beispielhafte Grundsätze: 1. **Grundsatz 1:** [TODO] 2. **Grundsatz 2:** [TODO] 3. **Grundsatz 3:** [TODO]

20.4 4. Verantwortlichkeiten

Rolle	Verantwortung	Name
Policy Owner	Gesamtverantwortung für Policy	Thomas Weber
Umsetzungsverantwortliche	Technische Umsetzung	Anna Schmidt
Kontrolle/Audit	Überwachung der Einhaltung	[TODO: Internal Audit]
Alle Mitarbeitenden	Einhaltung der Policy	Alle

20.5 5. Abgeleitete Richtlinien und Standards

Diese Policy wird konkretisiert durch: - **Richtlinie 0290:** Richtlinie: Scans Patching und Exploitation Response - [TODO: Weitere Richtlinien und Standards]

20.6 6. Nachweise und Kontrolle

Evidence/Nachweise: - [TODO: Definieren Sie erforderliche Nachweise] - Beispiele: Konfigurationsnachweise, Logs, Audit-Berichte

Review-Intervall: - Diese Policy wird jährlich oder bei wesentlichen Änderungen überprüft - **Nächster Review:** {{ meta.document.next_review }}

20.7 7. Konsequenzen bei Verstößen

Verstöße gegen diese Policy können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

20.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Dokument 0290: Richtlinie: Scans Patching und Exploitation Response

ewpage

Chapter 21

Richtlinie: Scans Patching und Exploitation Response

Dokument-ID: 0290
Dokumenttyp: Richtlinie/Standard (konkret)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

21.1 1. Zweck und Bezug

Diese Richtlinie konkretisiert die **Policy 0280: Policy: Patch und Vulnerability Management** und definiert spezifische Anforderungen für Schwachstellen-Management.

Verantwortlich: Anna Schmidt (IT-Leitung)

[TODO: Spezifische Zielsetzung ergänzen]

21.2 2. Geltungsbereich

Systeme/Plattformen: - [TODO: Definieren Sie betroffene Systeme] - Beispiele: Active Directory, Cloud-Plattformen, Anwendungen

Zielgruppen: - IT-Administratoren - System-Owner - [TODO: Weitere Zielgruppen]

21.3 3. Mindestanforderungen (MUSS)

[TODO: Definieren Sie zwingende Anforderungen]

Beispielhafte MUSS-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO] 3. **Anforderung 3:** [TODO]

21.4 4. Empfohlene Anforderungen (SOLL)

[TODO: Definieren Sie empfohlene Anforderungen]

Beispielhafte SOLL-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO]

21.5 5. Prozess und Umsetzung

21.5.1 5.1 Prozessschritte

[TODO: Definieren Sie den Prozess]

Beispielhafter Prozess: 1. **Antrag:** [TODO] 2. **Genehmigung:** [TODO] 3. **Umsetzung:** [TODO] 4. **Review:** [TODO]

21.5.2 5.2 Tooling und Systeme

Verwendete Tools: - [TODO: Tool 1] - [TODO: Tool 2]

Verantwortlich: Anna Schmidt

21.6 6. Nachweise (Evidence)

Erforderliche Nachweise: - [TODO: Nachweis 1] - [TODO: Nachweis 2]

Aufbewahrungsdauer: [TODO: z.B. 3 Jahre]

21.7 7. Ausnahmen

Ausnahmen von dieser Richtlinie sind nur über den **Ausnahmenprozess (Dokument 0520)** möglich.

Ausnahmeantrag an: Thomas Weber (ISB)

21.8 8. Schulung und Awareness

[TODO: Definieren Sie Schulungsanforderungen]

Zielgruppe: [TODO]
Frequenz: [TODO]
Verantwortlich: Thomas Weber

21.9 9. Review und Aktualisierung

Diese Richtlinie wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Verantwortlich:** Anna Schmidt - **Nächster Review:** {{ meta.document.next_review }}

21.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - Dokument 0280: Policy: Patch und Vulnerability Management

ewpage

Chapter 22

Policy: Logging Monitoring und Detektion

Dokument-ID: 0300
Dokumenttyp: Policy (abstrakt)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

22.1 1. Zweck und Zielsetzung

Diese Policy definiert die Grundsätze für Logging und Monitoring bei **AdminSend GmbH**.

Verantwortlich: Thomas Weber (ISB)

[TODO: Spezifische Zielsetzung ergänzen]

22.2 2. Geltungsbereich

Diese Policy gilt für: - Alle Mitarbeitenden von AdminSend GmbH - Alle IT-Systeme und Anwendungen - Alle Standorte: {{ meta.organization.locations }} - Externe Dienstleister mit Zugriff auf Systeme

Ausnahmen: - Ausnahmen sind nur über den Ausnahmenprozess (Dokument 0520) möglich - [TODO: Spezifische Ausnahmen dokumentieren]

22.3 3. Grundsätze

[TODO: Definieren Sie die strategischen Grundsätze für Logging und Monitoring]

Beispielhafte Grundsätze: 1. **Grundsatz 1:** [TODO] 2. **Grundsatz 2:** [TODO] 3. **Grundsatz 3:** [TODO]

22.4 4. Verantwortlichkeiten

Rolle	Verantwortung	Name
Policy Owner	Gesamtverantwortung für Policy	Thomas Weber
Umsetzungsverantwortliche	Technische Umsetzung	Anna Schmidt
Kontrolle/Audit	Überwachung der Einhaltung	[TODO: Internal Audit]
Alle Mitarbeitenden	Einhaltung der Policy	Alle

22.5 5. Abgeleitete Richtlinien und Standards

Diese Policy wird konkretisiert durch: - **Richtlinie 0310:** Richtlinie: Log Standards SIEM Use-Cases und Retention - [TODO: Weitere Richtlinien und Standards]

22.6 6. Nachweise und Kontrolle

Evidence/Nachweise: - [TODO: Definieren Sie erforderliche Nachweise] - Beispiele: Konfigurationsnachweise, Logs, Audit-Berichte

Review-Intervall: - Diese Policy wird jährlich oder bei wesentlichen Änderungen überprüft - **Nächster Review:** {{ meta.document.next_review }}

22.7 7. Konsequenzen bei Verstößen

Verstöße gegen diese Policy können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

22.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Dokument 0310: Richtlinie: Log Standards SIEM UseCases und Retention

ewpage

Chapter 23

Richtlinie: Log Standards SIEM UseCases und Retention

Dokument-ID: 0310
Dokumenttyp: Richtlinie/Standard (konkret)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

23.1 1. Zweck und Bezug

Diese Richtlinie konkretisiert die **Policy 0300: Policy: Logging Monitoring und Detektion** und definiert spezifische Anforderungen für SIEM und Log-Management.

Verantwortlich: Anna Schmidt (IT-Leitung)

[TODO: Spezifische Zielsetzung ergänzen]

23.2 2. Geltungsbereich

Systeme/Plattformen: - [TODO: Definieren Sie betroffene Systeme] - Beispiele: Active Directory, Cloud-Plattformen, Anwendungen

Zielgruppen: - IT-Administratoren - System-Owner - [TODO: Weitere Zielgruppen]

23.3 3. Mindestanforderungen (MUSS)

[TODO: Definieren Sie zwingende Anforderungen]

Beispielhafte MUSS-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO] 3. **Anforderung 3:** [TODO]

23.4 4. Empfohlene Anforderungen (SOLL)

[TODO: Definieren Sie empfohlene Anforderungen]

Beispielhafte SOLL-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO]

23.5 5. Prozess und Umsetzung

23.5.1 5.1 Prozessschritte

[TODO: Definieren Sie den Prozess]

Beispielhafter Prozess: 1. **Antrag:** [TODO] 2. **Genehmigung:** [TODO] 3. **Umsetzung:** [TODO] 4. **Review:** [TODO]

23.5.2 5.2 Tooling und Systeme

Verwendete Tools: - [TODO: Tool 1] - [TODO: Tool 2]

Verantwortlich: Anna Schmidt

23.6 6. Nachweise (Evidence)

Erforderliche Nachweise: - [TODO: Nachweis 1] - [TODO: Nachweis 2]

Aufbewahrungsdauer: [TODO: z.B. 3 Jahre]

23.7 7. Ausnahmen

Ausnahmen von dieser Richtlinie sind nur über den **Ausnahmenprozess (Dokument 0520)** möglich.

Ausnahmeantrag an: Thomas Weber (ISB)

23.8 8. Schulung und Awareness

[TODO: Definieren Sie Schulungsanforderungen]

Zielgruppe: [TODO]
Frequenz: [TODO]
Verantwortlich: Thomas Weber

23.9 9. Review und Aktualisierung

Diese Richtlinie wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Verantwortlich:** Anna Schmidt - **Nächster Review:** {{ meta.document.next_review }}

23.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - Dokument 0300: Policy: Logging Monitoring und Detektion

ewpage

Chapter 24

Policy: Incident Management

Dokument-ID: 0320
Dokumenttyp: Policy (abstrakt)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

24.1 1. Zweck und Zielsetzung

Diese Policy definiert die Grundsätze für Incident-Management bei **AdminSend GmbH**.

Verantwortlich: Thomas Weber (ISB)

[TODO: Spezifische Zielsetzung ergänzen]

24.2 2. Geltungsbereich

Diese Policy gilt für: - Alle Mitarbeitenden von AdminSend GmbH - Alle IT-Systeme und Anwendungen - Alle Standorte: {{ meta.organization.locations }} - Externe Dienstleister mit Zugriff auf Systeme

Ausnahmen: - Ausnahmen sind nur über den Ausnahmenprozess (Dokument 0520) möglich - [TODO: Spezifische Ausnahmen dokumentieren]

24.3 3. Grundsätze

[TODO: Definieren Sie die strategischen Grundsätze für Incident-Management]

Beispielhafte Grundsätze: 1. **Grundsatz 1:** [TODO] 2. **Grundsatz 2:** [TODO] 3. **Grundsatz 3:** [TODO]

24.4 4. Verantwortlichkeiten

Rolle	Verantwortung	Name
Policy Owner	Gesamtverantwortung für Policy	Thomas Weber
Umsetzungsverantwortliche	Technische Umsetzung	Anna Schmidt
Kontrolle/Audit	Überwachung der Einhaltung	[TODO: Internal Audit]
Alle Mitarbeitenden	Einhaltung der Policy	Alle

24.5 5. Abgeleitete Richtlinien und Standards

Diese Policy wird konkretisiert durch: - **Richtlinie 0330:** Richtlinie: Incident Response Eskalation und Forensik - [TODO: Weitere Richtlinien und Standards]

24.6 6. Nachweise und Kontrolle

Evidence/Nachweise: - [TODO: Definieren Sie erforderliche Nachweise] - Beispiele: Konfigurationsnachweise, Logs, Audit-Berichte

Review-Intervall: - Diese Policy wird jährlich oder bei wesentlichen Änderungen überprüft - **Nächster Review:** {{ meta.document.next_review }}

24.7 7. Konsequenzen bei Verstößen

Verstöße gegen diese Policy können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

24.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Dokument 0330: Richtlinie: Incident Response Eskalation und Forensik

ewpage

Chapter 25

Richtlinie: Incident Response Eskalation und Forensik

Dokument-ID: 0330
Dokumenttyp: Richtlinie/Standard (konkret)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

25.1 1. Zweck und Bezug

Diese Richtlinie konkretisiert die **Policy 0320: Policy: Incident Management** und definiert spezifische Anforderungen für Incident-Response-Prozess.

Verantwortlich: Anna Schmidt (IT-Leitung)

[TODO: Spezifische Zielsetzung ergänzen]

25.2 2. Geltungsbereich

Systeme/Plattformen: - [TODO: Definieren Sie betroffene Systeme] - Beispiele: Active Directory, Cloud-Plattformen, Anwendungen

Zielgruppen: - IT-Administratoren - System-Owner - [TODO: Weitere Zielgruppen]

25.3 3. Mindestanforderungen (MUSS)

[TODO: Definieren Sie zwingende Anforderungen]

Beispielhafte MUSS-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO] 3. **Anforderung 3:** [TODO]

25.4 4. Empfohlene Anforderungen (SOLL)

[TODO: Definieren Sie empfohlene Anforderungen]

Beispielhafte SOLL-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO]

25.5 5. Prozess und Umsetzung

25.5.1 5.1 Prozessschritte

[TODO: Definieren Sie den Prozess]

Beispielhafter Prozess: 1. **Antrag:** [TODO] 2. **Genehmigung:** [TODO] 3. **Umsetzung:** [TODO] 4. **Review:** [TODO]

25.5.2 5.2 Tooling und Systeme

Verwendete Tools: - [TODO: Tool 1] - [TODO: Tool 2]

Verantwortlich: Anna Schmidt

25.6 6. Nachweise (Evidence)

Erforderliche Nachweise: - [TODO: Nachweis 1] - [TODO: Nachweis 2]

Aufbewahrungsdauer: [TODO: z.B. 3 Jahre]

25.7 7. Ausnahmen

Ausnahmen von dieser Richtlinie sind nur über den **Ausnahmenprozess (Dokument 0520)** möglich.

Ausnahmeantrag an: Thomas Weber (ISB)

25.8 8. Schulung und Awareness

[TODO: Definieren Sie Schulungsanforderungen]

Zielgruppe: [TODO]
Frequenz: [TODO]
Verantwortlich: Thomas Weber

25.9 9. Review und Aktualisierung

Diese Richtlinie wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Verantwortlich:** Anna Schmidt - **Nächster Review:** {{ meta.document.next_review }}

25.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - Dokument 0320: Policy: Incident Management

ewpage

Chapter 26

Policy: Kryptografie und Key Management

Dokument-ID: 0340
Dokumenttyp: Policy (abstrakt)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

26.1 1. Zweck und Zielsetzung

Diese Policy definiert die Grundsätze für Kryptografie bei **AdminSend GmbH**.

Verantwortlich: Thomas Weber (ISB)

[TODO: Spezifische Zielsetzung ergänzen]

26.2 2. Geltungsbereich

Diese Policy gilt für: - Alle Mitarbeitenden von AdminSend GmbH - Alle IT-Systeme und Anwendungen - Alle Standorte: {{ meta.organization.locations }} - Externe Dienstleister mit Zugriff auf Systeme

Ausnahmen: - Ausnahmen sind nur über den Ausnahmenprozess (Dokument 0520) möglich - [TODO: Spezifische Ausnahmen dokumentieren]

26.3 3. Grundsätze

[TODO: Definieren Sie die strategischen Grundsätze für Kryptografie]

Beispielhafte Grundsätze: 1. **Grundsatz 1:** [TODO] 2. **Grundsatz 2:** [TODO] 3. **Grundsatz 3:** [TODO]

26.4 4. Verantwortlichkeiten

Rolle	Verantwortung	Name
Policy Owner	Gesamtverantwortung für Policy	Thomas Weber
Umsetzungsverantwortliche	Technische Umsetzung	Anna Schmidt
Kontrolle/Audit	Überwachung der Einhaltung	[TODO: Internal Audit]
Alle Mitarbeitenden	Einhaltung der Policy	Alle

26.5 5. Abgeleitete Richtlinien und Standards

Diese Policy wird konkretisiert durch: - **Richtlinie 0350:** Richtlinie: Verschluesselung Key Rotation und Zertifikate - [TODO: Weitere Richtlinien und Standards]

26.6 6. Nachweise und Kontrolle

Evidence/Nachweise: - [TODO: Definieren Sie erforderliche Nachweise] - Beispiele: Konfigurationsnachweise, Logs, Audit-Berichte

Review-Intervall: - Diese Policy wird jährlich oder bei wesentlichen Änderungen überprüft - **Nächster Review:** {{ meta.document.next_review }}

26.7 7. Konsequenzen bei Verstößen

Verstöße gegen diese Policy können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

26.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Dokument 0350: Richtlinie: Verschluesselung Key Rotation und Zertifikate

ewpage

Chapter 27

Richtlinie: Verschluesselung Key Rotation und Zertifikate

Dokument-ID: 0350
Dokumenttyp: Richtlinie/Standard (konkret)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

27.1 1. Zweck und Bezug

Diese Richtlinie konkretisiert die **Policy 0340: Policy: Kryptografie und Key Management** und definiert spezifische Anforderungen für Verschlüsselung und Schlüsselverwaltung.

Verantwortlich: Anna Schmidt (IT-Leitung)

[TODO: Spezifische Zielsetzung ergänzen]

27.2 2. Geltungsbereich

Systeme/Plattformen: - [TODO: Definieren Sie betroffene Systeme] - Beispiele: Active Directory, Cloud-Plattformen, Anwendungen

Zielgruppen: - IT-Administratoren - System-Owner - [TODO: Weitere Zielgruppen]

27.3 3. Mindestanforderungen (MUSS)

[TODO: Definieren Sie zwingende Anforderungen]

Beispielhafte MUSS-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO] 3. **Anforderung 3:** [TODO]

27.4 4. Empfohlene Anforderungen (SOLL)

[TODO: Definieren Sie empfohlene Anforderungen]

Beispielhafte SOLL-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO]

27.5 5. Prozess und Umsetzung

27.5.1 5.1 Prozessschritte

[TODO: Definieren Sie den Prozess]

Beispielhafter Prozess: 1. **Antrag:** [TODO] 2. **Genehmigung:** [TODO] 3. **Umsetzung:** [TODO] 4. **Review:** [TODO]

27.5.2 5.2 Tooling und Systeme

Verwendete Tools: - [TODO: Tool 1] - [TODO: Tool 2]

Verantwortlich: Anna Schmidt

27.6 6. Nachweise (Evidence)

Erforderliche Nachweise: - [TODO: Nachweis 1] - [TODO: Nachweis 2]

Aufbewahrungsdauer: [TODO: z.B. 3 Jahre]

27.7 7. Ausnahmen

Ausnahmen von dieser Richtlinie sind nur über den **Ausnahmenprozess (Dokument 0520)** möglich.

Ausnahmeantrag an: Thomas Weber (ISB)

27.8 8. Schulung und Awareness

[TODO: Definieren Sie Schulungsanforderungen]

Zielgruppe: [TODO]
Frequenz: [TODO]
Verantwortlich: Thomas Weber

27.9 9. Review und Aktualisierung

Diese Richtlinie wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Verantwortlich:** Anna Schmidt - **Nächster Review:** {{ meta.document.next_review }}

27.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - Dokument 0340: Policy: Kryptografie und Key Management

ewpage

Chapter 28

Policy: Sichere Softwareentwicklung

Dokument-ID: 0360
Dokumenttyp: Policy (abstrakt)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

28.1 1. Zweck und Zielsetzung

Diese Policy definiert die Grundsätze für Sichere Softwareentwicklung bei **AdminSend GmbH**.

Verantwortlich: Thomas Weber (ISB)

[TODO: Spezifische Zielsetzung ergänzen]

28.2 2. Geltungsbereich

Diese Policy gilt für: - Alle Mitarbeitenden von AdminSend GmbH - Alle IT-Systeme und Anwendungen - Alle Standorte: {{ meta.organization.locations }} - Externe Dienstleister mit Zugriff auf Systeme

Ausnahmen: - Ausnahmen sind nur über den Ausnahmenprozess (Dokument 0520) möglich - [TODO: Spezifische Ausnahmen dokumentieren]

28.3 3. Grundsätze

[TODO: Definieren Sie die strategischen Grundsätze für Sichere Softwareentwicklung]

Beispielhafte Grundsätze: 1. **Grundsatz 1:** [TODO] 2. **Grundsatz 2:** [TODO] 3. **Grundsatz 3:** [TODO]

28.4 4. Verantwortlichkeiten

Rolle	Verantwortung	Name
Policy Owner	Gesamtverantwortung für Policy	Thomas Weber
Umsetzungsverantwortliche	Technische Umsetzung	Anna Schmidt
Kontrolle/Audit	Überwachung der Einhaltung	[TODO: Internal Audit]
Alle Mitarbeitenden	Einhaltung der Policy	Alle

28.5 5. Abgeleitete Richtlinien und Standards

Diese Policy wird konkretisiert durch: - **Richtlinie 0370:** Richtlinie: Secure SDLC Code Reviews SAST DAST Secrets - [TODO: Weitere Richtlinien und Standards]

28.6 6. Nachweise und Kontrolle

Evidence/Nachweise: - [TODO: Definieren Sie erforderliche Nachweise] - Beispiele: Konfigurationsnachweise, Logs, Audit-Berichte

Review-Intervall: - Diese Policy wird jährlich oder bei wesentlichen Änderungen überprüft - **Nächster Review:** {{ meta.document.next_review }}

28.7 7. Konsequenzen bei Verstößen

Verstöße gegen diese Policy können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

28.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Dokument 0370: Richtlinie: Secure SDLC Code Reviews SAST DAST Secrets

ewpage

Chapter 29

Richtlinie: Secure SDLC Code Reviews SAST DAST Secrets

Dokument-ID: 0370
Dokumenttyp: Richtlinie/Standard (konkret)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

29.1 1. Zweck und Bezug

Diese Richtlinie konkretisiert die **Policy 0360: Policy: Sichere Softwareentwicklung** und definiert spezifische Anforderungen für Secure SDLC.

Verantwortlich: Anna Schmidt (IT-Leitung)

[TODO: Spezifische Zielsetzung ergänzen]

29.2 2. Geltungsbereich

Systeme/Plattformen: - [TODO: Definieren Sie betroffene Systeme] - Beispiele: Active Directory, Cloud-Plattformen, Anwendungen

Zielgruppen: - IT-Administratoren - System-Owner - [TODO: Weitere Zielgruppen]

29.3 3. Mindestanforderungen (MUSS)

[TODO: Definieren Sie zwingende Anforderungen]

Beispielhafte MUSS-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO] 3. **Anforderung 3:** [TODO]

29.4 4. Empfohlene Anforderungen (SOLL)

[TODO: Definieren Sie empfohlene Anforderungen]

Beispielhafte SOLL-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO]

29.5 5. Prozess und Umsetzung

29.5.1 5.1 Prozessschritte

[TODO: Definieren Sie den Prozess]

Beispielhafter Prozess: 1. **Antrag:** [TODO] 2. **Genehmigung:** [TODO] 3. **Umsetzung:** [TODO] 4. **Review:** [TODO]

29.5.2 5.2 Tooling und Systeme

Verwendete Tools: - [TODO: Tool 1] - [TODO: Tool 2]

Verantwortlich: Anna Schmidt

29.6 6. Nachweise (Evidence)

Erforderliche Nachweise: - [TODO: Nachweis 1] - [TODO: Nachweis 2]

Aufbewahrungsdauer: [TODO: z.B. 3 Jahre]

29.7 7. Ausnahmen

Ausnahmen von dieser Richtlinie sind nur über den **Ausnahmenprozess (Dokument 0520)** möglich.

Ausnahmeantrag an: Thomas Weber (ISB)

29.8 8. Schulung und Awareness

[TODO: Definieren Sie Schulungsanforderungen]

Zielgruppe: [TODO]
Frequenz: [TODO]
Verantwortlich: Thomas Weber

29.9 9. Review und Aktualisierung

Diese Richtlinie wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Verantwortlich:** Anna Schmidt - **Nächster Review:** {{ meta.document.next_review }}

29.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - Dokument 0360: Policy: Sichere Softwareentwicklung

ewpage

Chapter 30

Policy: Change und Release Management

Dokument-ID: 0380
Dokumenttyp: Policy (abstrakt)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

30.1 1. Zweck und Zielsetzung

Diese Policy definiert die Grundsätze für Change-Management bei **AdminSend GmbH**.

Verantwortlich: Thomas Weber (ISB)

[TODO: Spezifische Zielsetzung ergänzen]

30.2 2. Geltungsbereich

Diese Policy gilt für: - Alle Mitarbeitenden von AdminSend GmbH - Alle IT-Systeme und Anwendungen - Alle Standorte: {{ meta.organization.locations }} - Externe Dienstleister mit Zugriff auf Systeme

Ausnahmen: - Ausnahmen sind nur über den Ausnahmenprozess (Dokument 0520) möglich - [TODO: Spezifische Ausnahmen dokumentieren]

30.3 3. Grundsätze

[TODO: Definieren Sie die strategischen Grundsätze für Change-Management]

Beispielhafte Grundsätze: 1. **Grundsatz 1:** [TODO] 2. **Grundsatz 2:** [TODO] 3. **Grundsatz 3:** [TODO]

30.4 4. Verantwortlichkeiten

Rolle	Verantwortung	Name
Policy Owner	Gesamtverantwortung für Policy	Thomas Weber
Umsetzungsverantwortliche	Technische Umsetzung	Anna Schmidt
Kontrolle/Audit	Überwachung der Einhaltung	[TODO: Internal Audit]
Alle Mitarbeitenden	Einhaltung der Policy	Alle

30.5 5. Abgeleitete Richtlinien und Standards

Diese Policy wird konkretisiert durch: - **Richtlinie 0390:** Richtlinie: Change Freigaben und Sicherheitschecks - [TODO: Weitere Richtlinien und Standards]

30.6 6. Nachweise und Kontrolle

Evidence/Nachweise: - [TODO: Definieren Sie erforderliche Nachweise] - Beispiele: Konfigurationsnachweise, Logs, Audit-Berichte

Review-Intervall: - Diese Policy wird jährlich oder bei wesentlichen Änderungen überprüft - **Nächster Review:** {{ meta.document.next_review }}

30.7 7. Konsequenzen bei Verstößen

Verstöße gegen diese Policy können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

30.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Dokument 0390: Richtlinie: Change Freigaben und Sicherheitschecks

ewpage

Chapter 31

Richtlinie: Change Freigaben und Sicherheitschecks

Dokument-ID: 0390
Dokumenttyp: Richtlinie/Standard (konkret)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

31.1 1. Zweck und Bezug

Diese Richtlinie konkretisiert die **Policy 0380: Policy: Change und Release Management** und definiert spezifische Anforderungen für Change-Prozess.

Verantwortlich: Anna Schmidt (IT-Leitung)

[TODO: Spezifische Zielsetzung ergänzen]

31.2 2. Geltungsbereich

Systeme/Plattformen: - [TODO: Definieren Sie betroffene Systeme] - Beispiele: Active Directory, Cloud-Plattformen, Anwendungen

Zielgruppen: - IT-Administratoren - System-Owner - [TODO: Weitere Zielgruppen]

31.3 3. Mindestanforderungen (MUSS)

[TODO: Definieren Sie zwingende Anforderungen]

Beispielhafte MUSS-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO] 3. **Anforderung 3:** [TODO]

31.4 4. Empfohlene Anforderungen (SOLL)

[TODO: Definieren Sie empfohlene Anforderungen]

Beispielhafte SOLL-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO]

31.5 5. Prozess und Umsetzung

31.5.1 5.1 Prozessschritte

[TODO: Definieren Sie den Prozess]

Beispielhafter Prozess: 1. **Antrag:** [TODO] 2. **Genehmigung:** [TODO] 3. **Umsetzung:** [TODO] 4. **Review:** [TODO]

31.5.2 5.2 Tooling und Systeme

Verwendete Tools: - [TODO: Tool 1] - [TODO: Tool 2]

Verantwortlich: Anna Schmidt

31.6 6. Nachweise (Evidence)

Erforderliche Nachweise: - [TODO: Nachweis 1] - [TODO: Nachweis 2]

Aufbewahrungsdauer: [TODO: z.B. 3 Jahre]

31.7 7. Ausnahmen

Ausnahmen von dieser Richtlinie sind nur über den **Ausnahmenprozess (Dokument 0520)** möglich.

Ausnahmeantrag an: Thomas Weber (ISB)

31.8 8. Schulung und Awareness

[TODO: Definieren Sie Schulungsanforderungen]

Zielgruppe: [TODO]
Frequenz: [TODO]
Verantwortlich: Thomas Weber

31.9 9. Review und Aktualisierung

Diese Richtlinie wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Verantwortlich:** Anna Schmidt - **Nächster Review:** {{ meta.document.next_review }}

31.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - Dokument 0380: Policy: Change und Release Management

ewpage

Chapter 32

Policy: Lieferanten und Auslagerungsmanagement

Dokument-ID: 0400
Dokumenttyp: Policy (abstrakt)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

32.1 1. Zweck und Zielsetzung

Diese Policy definiert die Grundsätze für Lieferanten-Management bei **AdminSend GmbH**.

Verantwortlich: Thomas Weber (ISB)

[TODO: Spezifische Zielsetzung ergänzen]

32.2 2. Geltungsbereich

Diese Policy gilt für: - Alle Mitarbeitenden von AdminSend GmbH - Alle IT-Systeme und Anwendungen - Alle Standorte: {{ meta.organization.locations }} - Externe Dienstleister mit Zugriff auf Systeme

Ausnahmen: - Ausnahmen sind nur über den Ausnahmenprozess (Dokument 0520) möglich - [TODO: Spezifische Ausnahmen dokumentieren]

32.3 3. Grundsätze

[TODO: Definieren Sie die strategischen Grundsätze für Lieferanten-Management]

Beispielhafte Grundsätze: 1. **Grundsatz 1:** [TODO] 2. **Grundsatz 2:** [TODO] 3. **Grundsatz 3:** [TODO]

32.4 4. Verantwortlichkeiten

Rolle	Verantwortung	Name
Policy Owner	Gesamtverantwortung für Policy	Thomas Weber
Umsetzungsverantwortliche	Technische Umsetzung	Anna Schmidt
Kontrolle/Audit	Überwachung der Einhaltung	[TODO: Internal Audit]
Alle Mitarbeitenden	Einhaltung der Policy	Alle

32.5 5. Abgeleitete Richtlinien und Standards

Diese Policy wird konkretisiert durch: - **Richtlinie 0410:** Richtlinie: Third Party Risk Assessment und Vertragsklauseln - [TODO: Weitere Richtlinien und Standards]

32.6 6. Nachweise und Kontrolle

Evidence/Nachweise: - [TODO: Definieren Sie erforderliche Nachweise] - Beispiele: Konfigurationsnachweise, Logs, Audit-Berichte

Review-Intervall: - Diese Policy wird jährlich oder bei wesentlichen Änderungen überprüft - **Nächster Review:** {{ meta.document.next_review }}

32.7 7. Konsequenzen bei Verstößen

Verstöße gegen diese Policy können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

32.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Dokument 0410: Richtlinie: Third Party Risk Assessment und Vertragsklauseln

ewpage

Chapter 33

Richtlinie: Third Party Risk Assessment und Vertragsklauseln

Dokument-ID: 0410
Dokumenttyp: Richtlinie/Standard (konkret)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

33.1 1. Zweck und Bezug

Diese Richtlinie konkretisiert die **Policy 0400: Policy: Lieferanten und Auslagerungsmanagement** und definiert spezifische Anforderungen für Third-Party-Risikomanagement.

Verantwortlich: Anna Schmidt (IT-Leitung)

[TODO: Spezifische Zielsetzung ergänzen]

33.2 2. Geltungsbereich

Systeme/Plattformen: - [TODO: Definieren Sie betroffene Systeme] - Beispiele: Active Directory, Cloud-Plattformen, Anwendungen

Zielgruppen: - IT-Administratoren - System-Owner - [TODO: Weitere Zielgruppen]

33.3 3. Mindestanforderungen (MUSS)

[TODO: Definieren Sie zwingende Anforderungen]

Beispielhafte MUSS-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO] 3. **Anforderung 3:** [TODO]

33.4 4. Empfohlene Anforderungen (SOLL)

[TODO: Definieren Sie empfohlene Anforderungen]

Beispielhafte SOLL-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO]

33.5 5. Prozess und Umsetzung

33.5.1 5.1 Prozessschritte

[TODO: Definieren Sie den Prozess]

Beispielhafter Prozess: 1. **Antrag:** [TODO] 2. **Genehmigung:** [TODO] 3. **Umsetzung:** [TODO] 4. **Review:** [TODO]

33.5.2 5.2 Tooling und Systeme

Verwendete Tools: - [TODO: Tool 1] - [TODO: Tool 2]

Verantwortlich: Anna Schmidt

33.6 6. Nachweise (Evidence)

Erforderliche Nachweise: - [TODO: Nachweis 1] - [TODO: Nachweis 2]

Aufbewahrungsdauer: [TODO: z.B. 3 Jahre]

33.7 7. Ausnahmen

Ausnahmen von dieser Richtlinie sind nur über den **Ausnahmenprozess (Dokument 0520)** möglich.

Ausnahmeantrag an: Thomas Weber (ISB)

33.8 8. Schulung und Awareness

[TODO: Definieren Sie Schulungsanforderungen]

Zielgruppe: [TODO]
Frequenz: [TODO]
Verantwortlich: Thomas Weber

33.9 9. Review und Aktualisierung

Diese Richtlinie wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Verantwortlich:** Anna Schmidt - **Nächster Review:** {{ meta.document.next_review }}

33.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - Dokument 0400: Policy: Lieferanten und Auslagerungsmanagement

ewpage

Chapter 34

Policy: Datenschutz und Datenhandling

Dokument-ID: 0420
Dokumenttyp: Policy (abstrakt)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

34.1 1. Zweck und Zielsetzung

Diese Policy definiert die Grundsätze für Datenschutz bei **AdminSend GmbH**.

Verantwortlich: Thomas Weber (ISB)

[TODO: Spezifische Zielsetzung ergänzen]

34.2 2. Geltungsbereich

Diese Policy gilt für: - Alle Mitarbeitenden von AdminSend GmbH - Alle IT-Systeme und Anwendungen - Alle Standorte: {{ meta.organization.locations }} - Externe Dienstleister mit Zugriff auf Systeme

Ausnahmen: - Ausnahmen sind nur über den Ausnahmenprozess (Dokument 0520) möglich - [TODO: Spezifische Ausnahmen dokumentieren]

34.3 3. Grundsätze

[TODO: Definieren Sie die strategischen Grundsätze für Datenschutz]

Beispielhafte Grundsätze: 1. **Grundsatz 1:** [TODO] 2. **Grundsatz 2:** [TODO] 3. **Grundsatz 3:** [TODO]

34.4 4. Verantwortlichkeiten

Rolle	Verantwortung	Name
Policy Owner	Gesamtverantwortung für Policy	Thomas Weber
Umsetzungsverantwortliche	Technische Umsetzung	Anna Schmidt
Kontrolle/Audit	Überwachung der Einhaltung	[TODO: Internal Audit]
Alle Mitarbeitenden	Einhaltung der Policy	Alle

34.5 5. Abgeleitete Richtlinien und Standards

Diese Policy wird konkretisiert durch: - **Richtlinie 0430:** Richtlinie: Datenklassifizierung Labeling und Weitergabe - [TODO: Weitere Richtlinien und Standards]

34.6 6. Nachweise und Kontrolle

Evidence/Nachweise: - [TODO: Definieren Sie erforderliche Nachweise] - Beispiele: Konfigurationsnachweise, Logs, Audit-Berichte

Review-Intervall: - Diese Policy wird jährlich oder bei wesentlichen Änderungen überprüft - **Nächster Review:** {{ meta.document.next_review }}

34.7 7. Konsequenzen bei Verstößen

Verstöße gegen diese Policy können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

34.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Dokument 0430: Richtlinie: Datenklassifizierung Labeling und Weitergabe

ewpage

Chapter 35

Richtlinie: Datenklassifizierung Labeling und Weitergabe

Dokument-ID: 0430
Dokumenttyp: Richtlinie/Standard (konkret)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

35.1 1. Zweck und Bezug

Diese Richtlinie konkretisiert die **Policy 0420: Policy: Datenschutz und Datenhandling** und definiert spezifische Anforderungen für Datenklassifizierung.

Verantwortlich: Anna Schmidt (IT-Leitung)

[TODO: Spezifische Zielsetzung ergänzen]

35.2 2. Geltungsbereich

Systeme/Plattformen: - [TODO: Definieren Sie betroffene Systeme] - Beispiele: Active Directory, Cloud-Plattformen, Anwendungen

Zielgruppen: - IT-Administratoren - System-Owner - [TODO: Weitere Zielgruppen]

35.3 3. Mindestanforderungen (MUSS)

[TODO: Definieren Sie zwingende Anforderungen]

Beispielhafte MUSS-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO] 3. **Anforderung 3:** [TODO]

35.4 4. Empfohlene Anforderungen (SOLL)

[TODO: Definieren Sie empfohlene Anforderungen]

Beispielhafte SOLL-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO]

35.5 5. Prozess und Umsetzung

35.5.1 5.1 Prozessschritte

[TODO: Definieren Sie den Prozess]

Beispielhafter Prozess: 1. **Antrag:** [TODO] 2. **Genehmigung:** [TODO] 3. **Umsetzung:** [TODO] 4. **Review:** [TODO]

35.5.2 5.2 Tooling und Systeme

Verwendete Tools: - [TODO: Tool 1] - [TODO: Tool 2]

Verantwortlich: Anna Schmidt

35.6 6. Nachweise (Evidence)

Erforderliche Nachweise: - [TODO: Nachweis 1] - [TODO: Nachweis 2]

Aufbewahrungsdauer: [TODO: z.B. 3 Jahre]

35.7 7. Ausnahmen

Ausnahmen von dieser Richtlinie sind nur über den **Ausnahmenprozess (Dokument 0520)** möglich.

Ausnahmeantrag an: Thomas Weber (ISB)

35.8 8. Schulung und Awareness

[TODO: Definieren Sie Schulungsanforderungen]

Zielgruppe: [TODO]
Frequenz: [TODO]
Verantwortlich: Thomas Weber

35.9 9. Review und Aktualisierung

Diese Richtlinie wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Verantwortlich:** Anna Schmidt - **Nächster Review:** {{ meta.document.next_review }}

35.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - Dokument 0420: Policy: Datenschutz und Datenhandling

ewpage

Chapter 36

Policy: Backup und Wiederherstellung

Dokument-ID: 0440
Dokumenttyp: Policy (abstrakt)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

36.1 1. Zweck und Zielsetzung

Diese Policy definiert die Grundsätze für Backup und Recovery bei **AdminSend GmbH**.

Verantwortlich: Thomas Weber (ISB)

[TODO: Spezifische Zielsetzung ergänzen]

36.2 2. Geltungsbereich

Diese Policy gilt für: - Alle Mitarbeitenden von AdminSend GmbH - Alle IT-Systeme und Anwendungen - Alle Standorte: {{ meta.organization.locations }} - Externe Dienstleister mit Zugriff auf Systeme

Ausnahmen: - Ausnahmen sind nur über den Ausnahmenprozess (Dokument 0520) möglich - [TODO: Spezifische Ausnahmen dokumentieren]

36.3 3. Grundsätze

[TODO: Definieren Sie die strategischen Grundsätze für Backup und Recovery]

Beispielhafte Grundsätze: 1. **Grundsatz 1:** [TODO] 2. **Grundsatz 2:** [TODO] 3. **Grundsatz 3:** [TODO]

36.4 4. Verantwortlichkeiten

Rolle	Verantwortung	Name
Policy Owner	Gesamtverantwortung für Policy	Thomas Weber
Umsetzungsverantwortliche	Technische Umsetzung	Anna Schmidt
Kontrolle/Audit	Überwachung der Einhaltung	[TODO: Internal Audit]
Alle Mitarbeitenden	Einhaltung der Policy	Alle

36.5 5. Abgeleitete Richtlinien und Standards

Diese Policy wird konkretisiert durch: - **Richtlinie 0450:** Richtlinie: Backup Restore und Regelmaessige Tests - [TODO: Weitere Richtlinien und Standards]

36.6 6. Nachweise und Kontrolle

Evidence/Nachweise: - [TODO: Definieren Sie erforderliche Nachweise] - Beispiele: Konfigurationsnachweise, Logs, Audit-Berichte

Review-Intervall: - Diese Policy wird jährlich oder bei wesentlichen Änderungen überprüft - **Nächster Review:** {{ meta.document.next_review }}

36.7 7. Konsequenzen bei Verstößen

Verstöße gegen diese Policy können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

36.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Dokument 0450: Richtlinie: Backup Restore und Regelmaessige Tests

ewpage

Chapter 37

Richtlinie: Backup Restore und Regelmaessige Tests

Dokument-ID: 0450
Dokumenttyp: Richtlinie/Standard (konkret)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

37.1 1. Zweck und Bezug

Diese Richtlinie konkretisiert die **Policy 0440: Policy: Backup und Wiederherstellung** und definiert spezifische Anforderungen für Backup-Prozess.

Verantwortlich: Anna Schmidt (IT-Leitung)

[TODO: Spezifische Zielsetzung ergänzen]

37.2 2. Geltungsbereich

Systeme/Plattformen: - [TODO: Definieren Sie betroffene Systeme] - Beispiele: Active Directory, Cloud-Plattformen, Anwendungen

Zielgruppen: - IT-Administratoren - System-Owner - [TODO: Weitere Zielgruppen]

37.3 3. Mindestanforderungen (MUSS)

[TODO: Definieren Sie zwingende Anforderungen]

Beispielhafte MUSS-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO] 3. **Anforderung 3:** [TODO]

37.4 4. Empfohlene Anforderungen (SOLL)

[TODO: Definieren Sie empfohlene Anforderungen]

Beispielhafte SOLL-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO]

37.5 5. Prozess und Umsetzung

37.5.1 5.1 Prozessschritte

[TODO: Definieren Sie den Prozess]

Beispielhafter Prozess: 1. **Antrag:** [TODO] 2. **Genehmigung:** [TODO] 3. **Umsetzung:** [TODO] 4. **Review:** [TODO]

37.5.2 5.2 Tooling und Systeme

Verwendete Tools: - [TODO: Tool 1] - [TODO: Tool 2]

Verantwortlich: Anna Schmidt

37.6 6. Nachweise (Evidence)

Erforderliche Nachweise: - [TODO: Nachweis 1] - [TODO: Nachweis 2]

Aufbewahrungsdauer: [TODO: z.B. 3 Jahre]

37.7 7. Ausnahmen

Ausnahmen von dieser Richtlinie sind nur über den **Ausnahmenprozess (Dokument 0520)** möglich.

Ausnahmeantrag an: Thomas Weber (ISB)

37.8 8. Schulung und Awareness

[TODO: Definieren Sie Schulungsanforderungen]

Zielgruppe: [TODO]
Frequenz: [TODO]
Verantwortlich: Thomas Weber

37.9 9. Review und Aktualisierung

Diese Richtlinie wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Verantwortlich:** Anna Schmidt - **Nächster Review:** {{ meta.document.next_review }}

37.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - Dokument 0440: Policy: Backup und Wiederherstellung

ewpage

Chapter 38

Policy: Netzwerk und Kommunikationssicherheit

Dokument-ID: 0460
Dokumenttyp: Policy (abstrakt)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

38.1 1. Zweck und Zielsetzung

Diese Policy definiert die Grundsätze für Netzwerksicherheit bei **AdminSend GmbH**.

Verantwortlich: Thomas Weber (ISB)

[TODO: Spezifische Zielsetzung ergänzen]

38.2 2. Geltungsbereich

Diese Policy gilt für: - Alle Mitarbeitenden von AdminSend GmbH - Alle IT-Systeme und Anwendungen - Alle Standorte: {{ meta.organization.locations }} - Externe Dienstleister mit Zugriff auf Systeme

Ausnahmen: - Ausnahmen sind nur über den Ausnahmenprozess (Dokument 0520) möglich - [TODO: Spezifische Ausnahmen dokumentieren]

38.3 3. Grundsätze

[TODO: Definieren Sie die strategischen Grundsätze für Netzwerksicherheit]

Beispielhafte Grundsätze: 1. **Grundsatz 1:** [TODO] 2. **Grundsatz 2:** [TODO] 3. **Grundsatz 3:** [TODO]

38.4 4. Verantwortlichkeiten

Rolle	Verantwortung	Name
Policy Owner	Gesamtverantwortung für Policy	Thomas Weber
Umsetzungsverantwortliche	Technische Umsetzung	Anna Schmidt
Kontrolle/Audit	Überwachung der Einhaltung	[TODO: Internal Audit]
Alle Mitarbeitenden	Einhaltung der Policy	Alle

38.5 5. Abgeleitete Richtlinien und Standards

Diese Policy wird konkretisiert durch: - **Richtlinie 0470:** Richtlinie: Segmentierung Firewalling VPN und Admin Zugaenge - [TODO: Weitere Richtlinien und Standards]

38.6 6. Nachweise und Kontrolle

Evidence/Nachweise: - [TODO: Definieren Sie erforderliche Nachweise] - Beispiele: Konfigurationsnachweise, Logs, Audit-Berichte

Review-Intervall: - Diese Policy wird jährlich oder bei wesentlichen Änderungen überprüft - **Nächster Review:** {{ meta.document.next_review }}

38.7 7. Konsequenzen bei Verstößen

Verstöße gegen diese Policy können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

38.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Dokument 0470: Richtlinie: Segmentierung Firewalling VPN und Admin Zugaenge

ewpage

Chapter 39

Richtlinie: Segmentierung Firewalling VPN und Admin Zugaenge

Dokument-ID: 0470
Dokumenttyp: Richtlinie/Standard (konkret)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

39.1 1. Zweck und Bezug

Diese Richtlinie konkretisiert die **Policy 0460: Policy: Netzwerk und Kommunikationssicherheit** und definiert spezifische Anforderungen für Netzwerksegmentierung.

Verantwortlich: Anna Schmidt (IT-Leitung)

[TODO: Spezifische Zielsetzung ergänzen]

39.2 2. Geltungsbereich

Systeme/Plattformen: - [TODO: Definieren Sie betroffene Systeme] - Beispiele: Active Directory, Cloud-Plattformen, Anwendungen

Zielgruppen: - IT-Administratoren - System-Owner - [TODO: Weitere Zielgruppen]

39.3 3. Mindestanforderungen (MUSS)

[TODO: Definieren Sie zwingende Anforderungen]

Beispielhafte MUSS-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO] 3. **Anforderung 3:** [TODO]

39.4 4. Empfohlene Anforderungen (SOLL)

[TODO: Definieren Sie empfohlene Anforderungen]

Beispielhafte SOLL-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO]

39.5 5. Prozess und Umsetzung

39.5.1 5.1 Prozessschritte

[TODO: Definieren Sie den Prozess]

Beispielhafter Prozess: 1. **Antrag:** [TODO] 2. **Genehmigung:** [TODO] 3. **Umsetzung:** [TODO] 4. **Review:** [TODO]

39.5.2 5.2 Tooling und Systeme

Verwendete Tools: - [TODO: Tool 1] - [TODO: Tool 2]

Verantwortlich: Anna Schmidt

39.6 6. Nachweise (Evidence)

Erforderliche Nachweise: - [TODO: Nachweis 1] - [TODO: Nachweis 2]

Aufbewahrungsdauer: [TODO: z.B. 3 Jahre]

39.7 7. Ausnahmen

Ausnahmen von dieser Richtlinie sind nur über den **Ausnahmenprozess (Dokument 0520)** möglich.

Ausnahmeantrag an: Thomas Weber (ISB)

39.8 8. Schulung und Awareness

[TODO: Definieren Sie Schulungsanforderungen]

Zielgruppe: [TODO]
Frequenz: [TODO]
Verantwortlich: Thomas Weber

39.9 9. Review und Aktualisierung

Diese Richtlinie wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Verantwortlich:** Anna Schmidt - **Nächster Review:** {{ meta.document.next_review }}

39.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - Dokument 0460: Policy: Netzwerk und Kommunikationssicherheit

ewpage

Chapter 40

Policy: Endpoint und Mobile Security

Dokument-ID: 0480
Dokumenttyp: Policy (abstrakt)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

40.1 1. Zweck und Zielsetzung

Diese Policy definiert die Grundsätze für Endpoint-Sicherheit bei **AdminSend GmbH**.

Verantwortlich: Thomas Weber (ISB)

[TODO: Spezifische Zielsetzung ergänzen]

40.2 2. Geltungsbereich

Diese Policy gilt für: - Alle Mitarbeitenden von AdminSend GmbH - Alle IT-Systeme und Anwendungen - Alle Standorte: {{ meta.organization.locations }} - Externe Dienstleister mit Zugriff auf Systeme

Ausnahmen: - Ausnahmen sind nur über den Ausnahmenprozess (Dokument 0520) möglich - [TODO: Spezifische Ausnahmen dokumentieren]

40.3 3. Grundsätze

[TODO: Definieren Sie die strategischen Grundsätze für Endpoint-Sicherheit]

Beispielhafte Grundsätze: 1. **Grundsatz 1:** [TODO] 2. **Grundsatz 2:** [TODO] 3. **Grundsatz 3:** [TODO]

40.4 4. Verantwortlichkeiten

Rolle	Verantwortung	Name
Policy Owner	Gesamtverantwortung für Policy	Thomas Weber
Umsetzungsverantwortliche	Technische Umsetzung	Anna Schmidt
Kontrolle/Audit	Überwachung der Einhaltung	[TODO: Internal Audit]
Alle Mitarbeitenden	Einhaltung der Policy	Alle

40.5 5. Abgeleitete Richtlinien und Standards

Diese Policy wird konkretisiert durch: - **Richtlinie 0490:** Richtlinie: MDM EDR Device Compliance und Remote Work - [TODO: Weitere Richtlinien und Standards]

40.6 6. Nachweise und Kontrolle

Evidence/Nachweise: - [TODO: Definieren Sie erforderliche Nachweise] - Beispiele: Konfigurationsnachweise, Logs, Audit-Berichte

Review-Intervall: - Diese Policy wird jährlich oder bei wesentlichen Änderungen überprüft - **Nächster Review:** {{ meta.document.next_review }}

40.7 7. Konsequenzen bei Verstößen

Verstöße gegen diese Policy können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

40.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Dokument 0490: Richtlinie: MDM EDR Device Compliance und Remote Work

ewpage

Chapter 41

Richtlinie: MDM EDR Device Compliance und Remote Work

Dokument-ID: 0490
Dokumenttyp: Richtlinie/Standard (konkret)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

41.1 1. Zweck und Bezug

Diese Richtlinie konkretisiert die **Policy 0480: Policy: Endpoint und Mobile Security** und definiert spezifische Anforderungen für Mobile Device Management.

Verantwortlich: Anna Schmidt (IT-Leitung)

[TODO: Spezifische Zielsetzung ergänzen]

41.2 2. Geltungsbereich

Systeme/Plattformen: - [TODO: Definieren Sie betroffene Systeme] - Beispiele: Active Directory, Cloud-Plattformen, Anwendungen

Zielgruppen: - IT-Administratoren - System-Owner - [TODO: Weitere Zielgruppen]

41.3 3. Mindestanforderungen (MUSS)

[TODO: Definieren Sie zwingende Anforderungen]

Beispielhafte MUSS-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO] 3. **Anforderung 3:** [TODO]

41.4 4. Empfohlene Anforderungen (SOLL)

[TODO: Definieren Sie empfohlene Anforderungen]

Beispielhafte SOLL-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO]

41.5 5. Prozess und Umsetzung

41.5.1 5.1 Prozessschritte

[TODO: Definieren Sie den Prozess]

Beispielhafter Prozess: 1. **Antrag:** [TODO] 2. **Genehmigung:** [TODO] 3. **Umsetzung:** [TODO] 4. **Review:** [TODO]

41.5.2 5.2 Tooling und Systeme

Verwendete Tools: - [TODO: Tool 1] - [TODO: Tool 2]

Verantwortlich: Anna Schmidt

41.6 6. Nachweise (Evidence)

Erforderliche Nachweise: - [TODO: Nachweis 1] - [TODO: Nachweis 2]

Aufbewahrungsdauer: [TODO: z.B. 3 Jahre]

41.7 7. Ausnahmen

Ausnahmen von dieser Richtlinie sind nur über den **Ausnahmenprozess (Dokument 0520)** möglich.

Ausnahmeantrag an: Thomas Weber (ISB)

41.8 8. Schulung und Awareness

[TODO: Definieren Sie Schulungsanforderungen]

Zielgruppe: [TODO]
Frequenz: [TODO]
Verantwortlich: Thomas Weber

41.9 9. Review und Aktualisierung

Diese Richtlinie wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Verantwortlich:** Anna Schmidt - **Nächster Review:** {{ meta.document.next_review }}

41.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - Dokument 0480: Policy: Endpoint und Mobile Security

ewpage

Chapter 42

Policy: Physische Sicherheit

Dokument-ID: 0500
Dokumenttyp: Policy (abstrakt)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

42.1 1. Zweck und Zielsetzung

Diese Policy definiert die Grundsätze für Physische Sicherheit bei **AdminSend GmbH**.

Verantwortlich: Thomas Weber (ISB)

[TODO: Spezifische Zielsetzung ergänzen]

42.2 2. Geltungsbereich

Diese Policy gilt für: - Alle Mitarbeitenden von AdminSend GmbH - Alle IT-Systeme und Anwendungen - Alle Standorte: {{ meta.organization.locations }} - Externe Dienstleister mit Zugriff auf Systeme

Ausnahmen: - Ausnahmen sind nur über den Ausnahmenprozess (Dokument 0520) möglich - [TODO: Spezifische Ausnahmen dokumentieren]

42.3 3. Grundsätze

[TODO: Definieren Sie die strategischen Grundsätze für Physische Sicherheit]

Beispielhafte Grundsätze: 1. **Grundsatz 1:** [TODO] 2. **Grundsatz 2:** [TODO] 3. **Grundsatz 3:** [TODO]

42.4 4. Verantwortlichkeiten

Rolle	Verantwortung	Name
Policy Owner	Gesamtverantwortung für Policy	Thomas Weber
Umsetzungsverantwortliche	Technische Umsetzung	Anna Schmidt
Kontrolle/Audit	Überwachung der Einhaltung	[TODO: Internal Audit]
Alle Mitarbeitenden	Einhaltung der Policy	Alle

42.5 5. Abgeleitete Richtlinien und Standards

Diese Policy wird konkretisiert durch: - **Richtlinie 0510:** Richtlinie: Zutritt Besucher und Schutz von Equipment - [TODO: Weitere Richtlinien und Standards]

42.6 6. Nachweise und Kontrolle

Evidence/Nachweise: - [TODO: Definieren Sie erforderliche Nachweise] - Beispiele: Konfigurationsnachweise, Logs, Audit-Berichte

Review-Intervall: - Diese Policy wird jährlich oder bei wesentlichen Änderungen überprüft - **Nächster Review:** {{ meta.document.next_review }}

42.7 7. Konsequenzen bei Verstößen

Verstöße gegen diese Policy können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

42.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Dokument 0510: Richtlinie: Zutritt Besucher und Schutz von Equipment

ewpage

Chapter 43

Richtlinie: Zutritt Besucher und Schutz von Equipment

Dokument-ID: 0510
Dokumenttyp: Richtlinie/Standard (konkret)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

43.1 1. Zweck und Bezug

Diese Richtlinie konkretisiert die **Policy 0500: Policy: Physische Sicherheit** und definiert spezifische Anforderungen für Zutrittskontrollen.

Verantwortlich: Anna Schmidt (IT-Leitung)

[TODO: Spezifische Zielsetzung ergänzen]

43.2 2. Geltungsbereich

Systeme/Plattformen: - [TODO: Definieren Sie betroffene Systeme] - Beispiele: Active Directory, Cloud-Plattformen, Anwendungen

Zielgruppen: - IT-Administratoren - System-Owner - [TODO: Weitere Zielgruppen]

43.3 3. Mindestanforderungen (MUSS)

[TODO: Definieren Sie zwingende Anforderungen]

Beispielhafte MUSS-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO] 3. **Anforderung 3:** [TODO]

43.4 4. Empfohlene Anforderungen (SOLL)

[TODO: Definieren Sie empfohlene Anforderungen]

Beispielhafte SOLL-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO]

43.5 5. Prozess und Umsetzung

43.5.1 5.1 Prozessschritte

[TODO: Definieren Sie den Prozess]

Beispielhafter Prozess: 1. **Antrag:** [TODO] 2. **Genehmigung:** [TODO] 3. **Umsetzung:** [TODO] 4. **Review:** [TODO]

43.5.2 5.2 Tooling und Systeme

Verwendete Tools: - [TODO: Tool 1] - [TODO: Tool 2]

Verantwortlich: Anna Schmidt

43.6 6. Nachweise (Evidence)

Erforderliche Nachweise: - [TODO: Nachweis 1] - [TODO: Nachweis 2]

Aufbewahrungsdauer: [TODO: z.B. 3 Jahre]

43.7 7. Ausnahmen

Ausnahmen von dieser Richtlinie sind nur über den **Ausnahmenprozess (Dokument 0520)** möglich.

Ausnahmeantrag an: Thomas Weber (ISB)

43.8 8. Schulung und Awareness

[TODO: Definieren Sie Schulungsanforderungen]

Zielgruppe: [TODO]
Frequenz: [TODO]
Verantwortlich: Thomas Weber

43.9 9. Review und Aktualisierung

Diese Richtlinie wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Verantwortlich:** Anna Schmidt - **Nächster Review:** {{ meta.document.next_review }}

43.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - Dokument 0500: Policy: Physische Sicherheit

ewpage

Chapter 44

Policy: Ausnahmenprozess und Risikoakzeptanz

Dokument-ID: 0520
Dokumenttyp: Policy (abstrakt)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

44.1 1. Zweck und Zielsetzung

Diese Policy definiert die Grundsätze für Ausnahmenprozess bei **AdminSend GmbH**.

Verantwortlich: Thomas Weber (ISB)

[TODO: Spezifische Zielsetzung ergänzen]

44.2 2. Geltungsbereich

Diese Policy gilt für: - Alle Mitarbeitenden von AdminSend GmbH - Alle IT-Systeme und Anwendungen - Alle Standorte: {{ meta.organization.locations }} - Externe Dienstleister mit Zugriff auf Systeme

Ausnahmen: - Ausnahmen sind nur über den Ausnahmenprozess (Dokument 0520) möglich - [TODO: Spezifische Ausnahmen dokumentieren]

44.3 3. Grundsätze

[TODO: Definieren Sie die strategischen Grundsätze für Ausnahmenprozess]

Beispielhafte Grundsätze: 1. **Grundsatz 1:** [TODO] 2. **Grundsatz 2:** [TODO] 3. **Grundsatz 3:** [TODO]

44.4 4. Verantwortlichkeiten

Rolle	Verantwortung	Name
Policy Owner	Gesamtverantwortung für Policy	Thomas Weber
Umsetzungsverantwortliche	Technische Umsetzung	Anna Schmidt
Kontrolle/Audit	Überwachung der Einhaltung	[TODO: Internal Audit]
Alle Mitarbeitenden	Einhaltung der Policy	Alle

44.5 5. Abgeleitete Richtlinien und Standards

Diese Policy wird konkretisiert durch: - **Richtlinie 0530:** Richtlinie: Ausnahmen Risk Waiver und Review - [TODO: Weitere Richtlinien und Standards]

44.6 6. Nachweise und Kontrolle

Evidence/Nachweise: - [TODO: Definieren Sie erforderliche Nachweise] - Beispiele: Konfigurationsnachweise, Logs, Audit-Berichte

Review-Intervall: - Diese Policy wird jährlich oder bei wesentlichen Änderungen überprüft - **Nächster Review:** {{ meta.document.next_review }}

44.7 7. Konsequenzen bei Verstößen

Verstöße gegen diese Policy können zu folgenden Maßnahmen führen: - Abmahnung - Disziplinarische Maßnahmen - Arbeitsrechtliche Konsequenzen - Strafrechtliche Verfolgung (bei schwerwiegenden Verstößen)

44.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Geschäftsführung	Max Mustermann	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - BSI Standards 200-1, 200-2, 200-3 - Dokument 0530: Richtlinie: Ausnahmen Risk Waiver und Review

ewpage

Chapter 45

Richtlinie: Ausnahmen Risk Waiver und Review

Dokument-ID: 0530
Dokumenttyp: Richtlinie/Standard (konkret)
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

45.1 1. Zweck und Bezug

Diese Richtlinie konkretisiert die **Policy 0520: Policy: Ausnahmenprozess und Risikoakzeptanz** und definiert spezifische Anforderungen für Ausnahmen-Management.

Verantwortlich: Anna Schmidt (IT-Leitung)

[TODO: Spezifische Zielsetzung ergänzen]

45.2 2. Geltungsbereich

Systeme/Plattformen: - [TODO: Definieren Sie betroffene Systeme] - Beispiele: Active Directory, Cloud-Plattformen, Anwendungen

Zielgruppen: - IT-Administratoren - System-Owner - [TODO: Weitere Zielgruppen]

45.3 3. Mindestanforderungen (MUSS)

[TODO: Definieren Sie zwingende Anforderungen]

Beispielhafte MUSS-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO] 3. **Anforderung 3:** [TODO]

45.4 4. Empfohlene Anforderungen (SOLL)

[TODO: Definieren Sie empfohlene Anforderungen]

Beispielhafte SOLL-Anforderungen: 1. **Anforderung 1:** [TODO] 2. **Anforderung 2:** [TODO]

45.5 5. Prozess und Umsetzung

45.5.1 5.1 Prozessschritte

[TODO: Definieren Sie den Prozess]

Beispielhafter Prozess: 1. **Antrag:** [TODO] 2. **Genehmigung:** [TODO] 3. **Umsetzung:** [TODO] 4. **Review:** [TODO]

45.5.2 5.2 Tooling und Systeme

Verwendete Tools: - [TODO: Tool 1] - [TODO: Tool 2]

Verantwortlich: Anna Schmidt

45.6 6. Nachweise (Evidence)

Erforderliche Nachweise: - [TODO: Nachweis 1] - [TODO: Nachweis 2]

Aufbewahrungsdauer: [TODO: z.B. 3 Jahre]

45.7 7. Ausnahmen

Ausnahmen von dieser Richtlinie sind nur über den **Ausnahmenprozess (Dokument 0520)** möglich.

Ausnahmeantrag an: Thomas Weber (ISB)

45.8 8. Schulung und Awareness

[TODO: Definieren Sie Schulungsanforderungen]

Zielgruppe: [TODO]
Frequenz: [TODO]
Verantwortlich: Thomas Weber

45.9 9. Review und Aktualisierung

Diese Richtlinie wird regelmäßig überprüft: - **Frequenz:** Jährlich oder bei wesentlichen Änderungen - **Verantwortlich:** Anna Schmidt - **Nächster Review:** {{ meta.document.next_review }}

45.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium - Dokument 0520: Policy: Ausnahmenprozess und Risikoakzeptanz

ewpage

Chapter 46

Schulung und Awareness – Programm

Dokument-ID: 0600
Dokumenttyp: Programm
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

46.1 1. Zweck und Zielsetzung

Das Schulungs- und Awareness-Programm von **AdminSend GmbH** stellt sicher, dass alle Mitarbeitenden über erforderliche Sicherheitskenntnisse verfügen.

Verantwortlich: Thomas Weber (ISB)

46.2 2. Zielgruppen

Zielgruppe	Anzahl	Spezifische Anforderungen
Alle Mitarbeitenden	[TODO]	Basis-Awareness
IT-Administratoren	[TODO]	Technische Sicherheit, Privileged Access
Entwickler	[TODO]	Secure Coding, SDLC
Führungskräfte	[TODO]	Sicherheitsstrategie, Risikomanagement
Externe Dienstleister	[TODO]	Relevante Sicherheitsanforderungen

46.3 3. Schulungskatalog

Training	Zielgruppe	Frequenz	Dauer	Inhalte	Nachweis	Owner
Grundlagentraining Informationssicherheit	Alle	Jährlich	1h	Policies, Phishing, Passwörter, Incident-Meldung	LMS-Zertifikat	Thomas Weber
Onboarding Security	Neue Mitarbeitende	Bei Eintritt	30min	Grundlagen, Policies	Teilnahmeliste	HR
Phishing-Simulation	Alle	Quartalsweise	10min	Phishing-Erkennung	Klickrate	Thomas Weber
Admin-Schulung	IT-Admins	Jährlich	4h	Privileged Access, Härtung, Logging	Teilnahmeliste	Anna Schmidt
Secure Coding	Entwickler	Jährlich	8h	OWASP Top 10, SAST/DAST	Teilnahmeliste	Anna Schmidt
[TODO: Weitere Schulungen]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

46.4 4. Wirksamkeitsmessung

46.4.1 4.1 Metriken (KPIs)

KPI	Ziel	Messung	Frequenz
Schulungsquote	100%	% Mitarbeitende mit aktuellem Training	Quartalsweise
Phishing-Test-Erfolgsrate	> 90%	% Mitarbeitende, die Phishing erkennen	Quartalsweise
Quiz-Erfolgsrate	> 80%	% bestandene Abschlusstests	Nach Schulung

46.4.2 4.2 Feedback und Verbesserung

- **Feedback-Umfragen:** Nach jeder Schulung
- **Lessons Learned:** Aus Sicherheitsvorfällen
- **Kontinuierliche Verbesserung:** Jährliche Programm-Review

46.5 5. Schulungsmaterialien

Verfügbare Materialien: - E-Learning-Module (LMS) - Präsentationen - Checklisten und Quick Reference Guides - Poster und Infografiken - Newsletter und Intranet-Artikel

Ablageort: [TODO: z.B. Intranet/Schulungsportal]

46.6 6. Kommunikation und Awareness-Kampagnen

Regelmäßige Aktivitäten: - Monatlicher Security-Newsletter - Quartalsweise Awareness-Kampagnen (Themen: Phishing, Passwörter, etc.) - Security Champions Programm - Jährlicher Security Awareness Month

46.7 7. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
HR	[TODO]	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI Standard 200-1: ISMS - BSI IT-Grundschutz-Kompendium: ORP.3 Sensibilisierung und Schulung

ewpage

Chapter 47

Internes Auditprogramm (Template)

Dokument-ID: 0610
Dokumenttyp: Programm/Template
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

47.1 1. Zweck und Zielsetzung

Das interne Auditprogramm von **AdminSend GmbH** stellt die Wirksamkeit des ISMS sicher.

Verantwortlich: [TODO: Internal Audit]

47.2 2. Audit-Ansatz

Prinzipien: - **Risikobasiert:** Fokus auf kritische Bereiche - **Unabhängig:** Auditoren sind unabhängig vom auditierten Bereich - **Scope-bezogen:** Audits decken den gesamten ISMS-Scope ab - **Systematisch:** Strukturierter Audit-Prozess

47.3 3. Audit-Plan

Zeitraum	Audit-Thema	Kriterien	Auditor	Auditee	Status	Ergebnis	Maßnahmen
Q1 {{ meta.document.next_review }}	Basis-Sicherheitscheck Stich-probe	Policies, Richtlin-ien, Evidence	[TODO]	Anna Schmidt	Geplant	-	-

Zeitraum	Audit-Thema	Kriterien	Auditor	Auditee	Status	Ergebnis	Maßnahmen
Q2 {{ meta.document.year }}	Risikomanagement-Prozess	Dokument 0090, Risikoregister	[TODO]	Thomas Weber	Geplant	-	-
Q3 {{ meta.document.year }}	Incident Management	Dokument 0320/0330, Incident-Logs	[TODO]	Anna Schmidt	Geplant	-	-
Q4 {{ meta.document.year }}	Dokumentenlenkung	Dokument 0030, Dokumentenregister	[TODO]	Thomas Weber	Geplant	-	-

47.4 4. Audit-Checkpunkte

Standardprüfungen: - Sind Dokumente aktuell und freigegeben? - Ist Evidence vorhanden und nachvollziehbar? - Ist der Maßnahmenstatus plausibel? - Sind Abweichungen dokumentiert und behandelt? - Werden Prozesse gelebt (nicht nur dokumentiert)?

47.5 5. Audit-Prozess

1. **Planung:** Audit-Scope, Kriterien, Zeitplan
2. **Vorbereitung:** Dokumentenreview, Checklisten
3. **Durchführung:** Interviews, Stichproben, Begehungen
4. **Berichterstattung:** Audit-Bericht mit Findings
5. **Follow-up:** Nachverfolgung von Korrekturmaßnahmen

47.6 6. Audit-Bericht Template

Struktur: 1. Executive Summary 2. Audit-Scope und Kriterien 3. Audit-Methodik 4. Findings (Kategorisiert: Kritisch/Hoch/Mittel/Niedrig) 5. Positive Beobachtungen 6. Empfehlungen 7. Maßnahmenplan

47.7 7. Findings-Kategorisierung

Kategorie	Beschreibung	Reaktionszeit
Kritisch	Schwerwiegende Abweichung, hohes Risiko	Sofort
Hoch	Wesentliche Abweichung	30 Tage
Mittel	Verbesserungspotenzial	90 Tage
Niedrig	Kleinere Abweichung	180 Tage

47.8 8. Freigabe

Rolle	Name	Datum	Freigabe
Internal Audit	[TODO]	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI Standard 200-1: ISMS - BSI IT-Grundschutz-Kompendium: DER.3.1 Audits und Revisionen

ewpage

Chapter 48

Managementbewertung (Management Review) – Template

Dokument-ID: 0620
Dokumenttyp: Nachweis/Template
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

48.1 1. Teilnehmer, Zeitraum, Scope

Datum: [TODO]
Ort: [TODO]
Dauer: [TODO]

Teilnehmer: - Geschäftsführung: Max Mustermann - ISB: Thomas Weber - IT-Leitung: Anna Schmidt - [TODO: Weitere Teilnehmer]

Informationsverbund(e): [TODO: Siehe Dokument 0040]

48.2 2. Inputs für Management Review

48.2.1 2.1 Status Maßnahmenplan

Maßnahmenumsetzung: [TODO: % abgeschlossen]
Kritische Maßnahmen: [TODO: Status]
Verzögerungen: [TODO: Beschreibung und Gründe]

Referenz: Dokument 0100 (Maßnahmenplan)

48.2.2 2.2 Ergebnisse Audits und Checks

Interne Audits: [TODO: Zusammenfassung]
Basis-Sicherheitscheck: [TODO: Erfüllungsgrad]
Externe Audits: [TODO: falls durchgeführt]

Referenz: Dokument 0610 (Auditprogramm), Dokument 0080 (Basis-Check)

48.2.3 2.3 Sicherheitsvorfälle und Lessons Learned

Anzahl Vorfälle: [TODO]
Kritische Vorfälle: [TODO: Beschreibung]
Lessons Learned: [TODO: Erkenntnisse]
Präventivmaßnahmen: [TODO]

Referenz: Dokument 0320/0330 (Incident Management)

48.2.4 2.4 Änderungen im Kontext

Technologie: - [TODO: Neue Systeme, Cloud-Migration, etc.]

Organisation: - [TODO: Umstrukturierungen, neue Standorte, etc.]

Lieferanten: - [TODO: Neue Dienstleister, Vertragsänderungen]

Rechtliche Anforderungen: - [TODO: Neue Gesetze, Regulierungen]

48.2.5 2.5 Risikolage und Top-Risiken

Risiko-Exposition: [TODO: Anzahl "Sehr hoch"/"Hoch"-Risiken]
Top 5 Risiken: [TODO: Siehe Dokument 0090]
Neue Bedrohungen: [TODO]

Referenz: Dokument 0090 (Risikoanalyse)

48.2.6 2.6 KPI-Performance

IT-Grundschutz-Erfüllungsgrad: [TODO: %]
Patch-Compliance: [TODO: %]
Schulungsquote: [TODO: %]
Weitere KPIs: [TODO]

Referenz: Dokument 0110 (KPIs)

48.3 3. Outputs und Entscheidungen

48.3.1 3.1 Anpassung Leitlinie und Ziele

Entscheidung: [TODO: Leitlinie anpassen? Ja/Nein]
Begründung: [TODO]
Neue Sicherheitsziele: [TODO]

Verantwortlich: Max Mustermann

48.3.2 3.2 Ressourcen und Investitionen

Budget-Anpassung: [TODO: Erhöhung/Reduzierung]
Personalressourcen: [TODO: Zusätzliche Stellen?]
Externe Unterstützung: [TODO]

Verantwortlich: Max Mustermann

48.3.3 3.3 Risikoakzeptanzen

Akzeptierte Risiken: [TODO: Risiko-IDs]
Begründung: [TODO]
Gültigkeitsdauer: [TODO]

Verantwortlich: Max Mustermann

48.3.4 3.4 Verbesserungsmaßnahmen

Maßnahme	Beschreibung	Owner	Zieltermin	Priorität
[TODO]	[TODO]	[TODO]	[TODO]	Hoch/Mittel/Niedrig

48.3.5 3.5 Scope-Änderungen

Scope-Erweiterung: [TODO: Neue Systeme/Standorte]
Scope-Reduzierung: [TODO: falls zutreffend]

Referenz: Dokument 0040 (Scope)

48.4 4. Zusammenfassung und Fazit

Gesamtbewertung ISMS: [TODO: Effektiv/Verbesserungsbedarf]
Haupterkenntnisse: [TODO]
Nächste Schritte: [TODO]

48.5 5. Freigabe

Rolle	Name	Datum	Unterschrift
Geschäftsführung	Max Mustermann	[TODO]	[TODO]
ISB	Thomas Weber	[TODO]	[TODO]

Referenzen: - BSI Standard 200-1: ISMS (Management Review) - Alle ISMS-Dokumente (0010-0630)

ewpage

Chapter 49

Nichtkonformitäten und Korrekturmaßnahmen

Dokument-ID: 0630
Dokumenttyp: Prozess/Template
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

49.1 1. Zweck und Zielsetzung

Dieser Prozess stellt sicher, dass Abweichungen von ISMS-Anforderungen systematisch erfasst, behandelt und deren Wirksamkeit geprüft wird.

Verantwortlich: Thomas Weber (ISB)

49.2 2. Quellen für Nichtkonformitäten

Nichtkonformitäten können identifiziert werden durch: - Interne Audits (Dokument 0610) - Basis-Sicherheitscheck (Dokument 0080) - Sicherheitsvorfälle (Dokument 0320/0330) - Penetrationstests und Vulnerability Scans - Policy-Verstöße - Management Review (Dokument 0620) - Externe Audits

49.3 3. Prozess

49.3.1 3.1 Erfassen

Schritt 1: Identifikation und Dokumentation - Nichtkonformität wird identifiziert - Finding wird im Findings-Register erfasst (siehe Abschnitt 4) - Kategorisierung: Kritisch/Hoch/Mittel/Niedrig

Verantwortlich: Identifizierende Person (Auditor, ISB, etc.)

49.3.2 3.2 Ursachenanalyse

Schritt 2: Root Cause Analysis - Warum ist die Nichtkonformität aufgetreten? - Welche Prozesse/Kontrollen haben versagt? - Ist dies ein Einzelfall oder systemisches Problem?

Methoden: - 5-Why-Analyse - Fishbone-Diagramm - Prozessanalyse

Verantwortlich: ISB, betroffener Bereichsverantwortlicher

49.3.3 3.3 Maßnahme definieren

Schritt 3: Korrekturmaßnahme festlegen - Sofortmaßnahme (Symptom beheben) - Korrekturmaßnahme (Ursache beheben) - Präventivmaßnahme (Wiederholung verhindern)

Verantwortlich: ISB, Maßnahmen-Owner

49.3.4 3.4 Umsetzung

Schritt 4: Maßnahme umsetzen - Maßnahme wird implementiert - Fortschritt wird getrackt - Dokumentation der Umsetzung

Verantwortlich: Maßnahmen-Owner

49.3.5 3.5 Wirksamkeitsprüfung

Schritt 5: Effectiveness Check - Wurde die Nichtkonformität behoben? - Ist die Ursache beseitigt? - Sind keine neuen Probleme entstanden?

Methoden: - Follow-up Audit - Stichprobenprüfung - KPI-Monitoring

Verantwortlich: ISB, Internal Audit

49.3.6 3.6 Abschluss

Schritt 6: Closure - Wirksamkeit bestätigt - Finding geschlossen - Lessons Learned dokumentiert

Verantwortlich: ISB

49.4 4. Findings-Register

Finding-ID	Quelle	Datum	Beschreibung	Kategorie	Root Cause	Maßnahme	Owner	Fällig	Status	Wirksamkeit geprüft am
F-001	Audit Q1	[TODO]	[TODO]	Hoch	[TODO]	[TODO]	[TODO]	[TODO]	Offen	-
F-002	Basis-Check	[TODO]	[TODO]	Mittel	[TODO]	[TODO]	[TODO]	[TODO]	In Bearbeitung	-
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Status-Werte: - **Offen:** Neu identifiziert - **In Analyse:** Ursachenanalyse läuft - **In Bearbeitung:** Maßnahme wird umgesetzt - **Wirksamkeitsprüfung:** Maßnahme umgesetzt, Prüfung ausstehend - **Geschlossen:** Wirksamkeit bestätigt

49.5 5. Kategorisierung und Reaktionszeiten

Kategorie	Beschreibung	Reaktionszeit	Eskalation
Kritisch	Schwerwiegende Abweichung, hohes Risiko	Sofort	Geschäftsführung
Hoch	Wesentliche Abweichung	7 Tage	ISB
Mittel	Verbesserungspotenzial	30 Tage	Bereichsverantwortlicher
Niedrig	Kleinere Abweichung	90 Tage	Bereichsverantwortlicher

49.6 6. Reporting

Monatlich: - Anzahl offener Findings (nach Kategorie) - Überfällige Findings - Abgeschlossene Findings

Quartalsweise: - Trend-Analyse - Top-Findings-Kategorien - Wirksamkeit von Korrekturmaßnahmen

Verantwortlich: Thomas Weber
Empfänger: Geschäftsführung, ISMS-Team

49.7 7. Lessons Learned

Nach Abschluss kritischer oder wiederkehrender Findings: 1. **Retrospektive:** Was lief gut? Was nicht? 2. **Prozessverbesserung:** Anpassung von Prozessen/Kontrollen 3. **Dokumentation:** Lessons Learned dokumentieren 4. **Kommunikation:** Erkenntnisse teilen (Awareness)

49.8 8. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI Standard 200-1: ISMS (Non-conformities and Corrective Actions) - Dokument 0610: Internes Auditprogramm

ewpage

Chapter 50

Anhang: Nachweisregister (Evidence)

Dokument-ID: 0700
Dokumenttyp: Anhang/Template
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

50.1 1. Zweck und Zielsetzung

Das Nachweisregister von **AdminSend GmbH** bietet eine zentrale Übersicht über alle Nachweise (Evidence), die die Umsetzung von Sicherheitsmaßnahmen, Policies und Richtlinien belegen.

Verantwortlich: Thomas Weber (ISB)

50.2 2. Nachweisregister

Evidence-ID	Thema/Maßnahme	Beschreibung	Dokumententyp	Ort/Link	Owner	Aufbewahrungsfrist	Letzte Prüfung	Nächste Prüfung	Status
E-001	Patch-Compliance	Monatlicher Patch-Status-Report	Report	[TODO: SharePoint/CMDB]	Anna Schmidt	3 Jahre	[TODO]	[TODO]	Aktuell
E-002	Backup-Tests	Quartalsweise Restore-Tests	Testprotokoll	[TODO]	Anna Schmidt	3 Jahre	[TODO]	[TODO]	Aktuell

Evidence-ID	Thema/Maßnahme	Beschreibung	Dokumententyp	Ort/Link	Owner	Aufbewahrungsfrist	Letzte Prüfung	Nächste Prüfung	Status
E-003	Schulungsnachweise	Teilnahmebestätigungen Security Awareness	Teilnehmerliste	[TODO: LMS]	Thomas Weber	5 Jahre	[TODO]	[TODO]	Aktuell
E-004	Audit-Berichte	Interne Audit-Berichte	Audit-Bericht	[TODO]	Internal Audit	10 Jahre	[TODO]	[TODO]	Aktuell
E-005	Risikoakzeptanzen	Dokumentierte Risikoakzeptanzen	Freigabe-Dokument	[TODO]	Max Mustermann	5 Jahre	[TODO]	[TODO]	Aktuell
E-006	Vulnerability Scans	Monatliche Vulnerability Scan Reports	Scan-Report	[TODO: Vulnerability Management Tool]	Thomas Weber	2 Jahre	[TODO]	[TODO]	Aktuell
E-007	Penetrationstests	Jährliche Pentest-Berichte	Pentest-Bericht	[TODO]	Thomas Weber	5 Jahre	[TODO]	[TODO]	Aktuell
E-008	Incident-Dokumentation	Incident-Reports und Postmortems	Incident-Report	[TODO: ITSM]	Anna Schmidt	3 Jahre	[TODO]	[TODO]	Aktuell
E-009	Change-Approvals	Change-Freigaben mit Security-Review	Change-Record	[TODO: ITSM]	Anna Schmidt	2 Jahre	[TODO]	[TODO]	Aktuell
E-010	Zugriffsprotokolle	Privileged Access Logs	Log-Archiv	[TODO: SIEM]	Thomas Weber	1 Jahr	[TODO]	[TODO]	Aktuell
E-011	Lieferanten-Assessments	Third-Party Risk Assessments	Assessment-Report	[TODO]	Thomas Weber	3 Jahre	[TODO]	[TODO]	Aktuell

Evidence-ID	Thema/Maßnahme	Beschreibung	Dokumententyp	Ort/Link	Owner	Aufbewahrungsfrist	Letzte Prüfung	Nächste Prüfung	Status
E-012	Management Review	Jährliches Management Review Protokolle	Protokoll	[TODO]	Max Mustermann	10 Jahre	[TODO]	[TODO]	Aktuell
E-013	Basis-Sicherheitscheck	BSI Basis-Check Ergebnisse	Gap-Analyse	[TODO]	Thomas Weber	3 Jahre	[TODO]	[TODO]	Aktuell
E-014	Schutzbedarfsfeststellung	Dokumentierte Schutzbedarfe	Bewertung	[TODO]	Thomas Weber	5 Jahre	[TODO]	[TODO]	Aktuell
E-015	Notfallübungen	BCM/DR Test-Protokolle	Testprotokoll	[TODO]	Thomas Weber	3 Jahre	[TODO]	[TODO]	Aktuell
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

50.3 3. Kategorien von Nachweisen

50.3.1 3.1 Technische Nachweise

- Scan-Reports (Vulnerability, Compliance)
- Log-Daten und SIEM-Auswertungen
- Backup-Protokolle
- Patch-Status-Reports
- Konfigurationsdokumentation

50.3.2 3.2 Organisatorische Nachweise

- Policies und Richtlinien (freigegeben)
- Schulungsnachweise
- Audit-Berichte
- Management Review Protokolle
- Risikoakzeptanzen

50.3.3 3.3 Prozess-Nachweise

- Incident-Reports
- Change-Records
- Problem-Management-Dokumentation
- Testprotokolle (DR, Backup, etc.)

50.3.4 3.4 Compliance-Nachweise

- Zertifikate (ISO, BSI, etc.)
- Externe Audit-Berichte
- Penetrationstests
- Datenschutz-Folgenabschätzungen (DPIA)

50.4 4. Aufbewahrungsfristen

Dokumenttyp	Aufbewahrungsfrist	Rechtsgrundlage
Audit-Berichte	10 Jahre	Handelsrecht
Schulungsnachweise	5 Jahre	Nachweispflicht
Incident-Reports	3 Jahre	Best Practice
Log-Daten	1 Jahr (Standard), 3 Jahre (kritische Systeme)	DSGVO, BSI
Risikoakzeptanzen	5 Jahre	Nachweispflicht
Verträge (Lieferanten)	Vertragslaufzeit + 3 Jahre	Handelsrecht

50.5 5. Zugriffskontrolle

Zugriff auf Nachweise: - **ISB:** Vollzugriff - **Internal Audit:** Vollzugriff (Lesezugriff) - **Geschäftsführung:** Vollzugriff - **Bereichsverantwortliche:** Zugriff auf eigene Nachweise - **Externe Auditoren:** Temporärer Lesezugriff (nach Freigabe)

Ablageorte: - Zentrale Dokumentenablage: [TODO: z.B. SharePoint, Confluence] - ITSM-System: [TODO: z.B. ServiceNow, Jira] - SIEM/Log-Management: [TODO] - CMDB: [TODO]

50.6 6. Prüfung und Aktualisierung

Regelmäßige Prüfung: - **Quartalsweise:** Vollständigkeitsprüfung - **Jährlich:** Aufbewahrungsfristen-Review - **Bei Audits:** Verfügbarkeit und Aktualität prüfen

Verantwortlich: Thomas Weber

50.7 7. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI Standard 200-1: ISMS (Dokumentation) - BSI Standard 200-2: IT-Grundschutz-Methodik (Nachweisführung) - Alle ISMS-Dokumente (0010-0630)

ewpage

Chapter 51

Anhang: Assetinventar (Template)

Dokument-ID: 0710
Dokumenttyp: Anhang/Template
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

51.1 1. Zweck und Zielsetzung

Das Assetinventar von **AdminSend GmbH** dokumentiert alle IT-Assets im Geltungsbereich des ISMS.

Verantwortlich: Anna Schmidt

51.2 2. Hinweis zur Pflege

Empfehlung: Dieses Inventar sollte in einer CMDB (Configuration Management Database) oder einem Asset-Management-Tool gepflegt werden. Dieses Dokument dient als Template/Export-Format.

CMDB-System: [TODO: z.B. ServiceNow, Device42, NetBox]
Ablageort: {{ netbox.url }} oder [TODO]

51.3 3. Asset-Kategorien

51.3.1 3.1 Hardware-Assets

- Server (physisch, virtuell)
- Netzwerkgeräte (Router, Switches, Firewalls)

- Storage-Systeme
- Endpoints (Laptops, Desktops, Mobile Devices)
- IoT-Geräte

51.3.2 3.2 Software-Assets

- Betriebssysteme
- Anwendungen (kommerziell, Open Source, Eigenentwicklung)
- Datenbanken
- Middleware

51.3.3 3.3 Daten-Assets

- Datenbanken
- Fileserver/Shares
- Cloud-Storage
- Backup-Medien

51.3.4 3.4 Services

- IT-Services (intern, extern)
- Cloud-Services (SaaS, PaaS, IaaS)

51.4 4. Asset-Register

Asset-ID	Name	Typ	Kategorie	Owner	Standort	Schutzbedarf (C/I/A/Legal)	Lebenszyklusstatus	Hersteller	Modell	Seriennummer	EOL-Datum	Anschaffungsdatum	Bemerkungen
{{ netbox.device.id }}	{{ netbox.device.name }}	Server	Hardware	Anna Schmidt	{{ netbox.site.name }}	[TODO]	Produktiv	{{ netbox.device.device_type.manufacturer.name }}	{{ netbox.device.device_type.model }}	{{ netbox.device.serial }}	[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Schutzbedarf-Kategorien: - **Normal:** Standard-Schutzbedarf - **Hoch:** Erhöhter Schutzbedarf - **Sehr hoch:** Kritischer Schutzbedarf

Lebenszyklusstatus: - **Planung:** In Beschaffung - **Entwicklung:** In Entwicklung/Konfiguration - **Produktiv:** Im Produktivbetrieb - **Wartung:** In Wartung/Support - **Außerbetrieb:** Stillgelegt - **Entsorgung:** Zur Entsorgung vorgesehen

51.5 5. NetBox-Integration

NetBox-Instanz: {{ netbox.url }}

Verfügbare Daten aus NetBox: - Geräte: {{ netbox.device.name }}, {{ netbox.device.type }}, {{ netbox.device.role }} - Standorte: {{ netbox.site.name }}, {{ netbox.site.region }} - IP-Adressen: {{ netbox.ipaddress.address }} - VLANs: {{ netbox.vlan.name }}, {{ netbox.vlan.id }} - Racks: {{ netbox.rack.name }}, {{ netbox.rack.location }}

Synchronisation: [TODO: Automatisch/Manuell, Frequenz]

51.6 6. Asset-Lifecycle-Management

51.6.1 6.1 Beschaffung

- Asset wird erfasst (Status: Planung)
- Schutzbedarf wird festgestellt
- Owner wird zugewiesen

51.6.2 6.2 Inbetriebnahme

- Asset wird konfiguriert und gehärtet
- Asset wird in Produktion überführt (Status: Produktiv)
- Monitoring wird aktiviert

51.6.3 6.3 Betrieb

- Regelmäßige Updates und Patches
- Monitoring und Wartung
- Änderungen werden dokumentiert (Change Management)

51.6.4 6.4 Außerbetriebnahme

- Asset wird stillgelegt (Status: Außerbetrieb)
- Daten werden sicher gelöscht
- Asset wird entsorgt (Status: Entsorgung)

Referenz: Dokument 0250 (Asset Lifecycle)

51.7 7. Verantwortlichkeiten (RACI)

Aktivität	IT-Leitung	Asset-Owner	CMDB-Admin	ISB
Asset erfassen	A	R	I	I
Schutzbedarf festlegen	A	C	I	R
Asset aktualisieren	I	R	A	I
Asset-Review (jährlich)	A	R	C	C
Asset-Entsorgung	A	R	I	C

Legende: - **R** = Responsible (Durchführungsverantwortung) - **A** = Accountable (Gesamtverantwortung) - **C** = Consulted (Konsultiert) - **I** = Informed (Informiert)

51.8 8. Asset-Tagging

Tagging-Schema: - **Environment:** Production, Staging, Development, Test - **Criticality:** Critical, High, Medium, Low - **Owner:** Bereichsverantwortlicher - **Compliance:** ISO27001, BSI, DSGVO, etc. - **Backup:** Yes/No - **DR:** Yes/No

Beispiel (Cloud-Ressourcen):

```
Environment: Production
Criticality: High
Owner: Anna Schmidt
Compliance: ISO27001, BSI
Backup: Yes
DR: Yes
```

51.9 9. Reporting

Regelmäßige Reports: - **Monatlich:** Asset-Bestandsübersicht - **Quartalsweise:** EOL-Report (Assets mit nahendem End-of-Life) - **Jährlich:** Vollständiger Asset-Review

Verantwortlich: Anna Schmidt

51.10 10. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium: OPS.1.1.1 Allgemeiner IT-Betrieb - BSI IT-Grundschutz-Kompendium: OPS.1.2.2 Archivierung - Dokument 0050: Strukturanalyse - Dokument 0060: Schutzbedarfsfeststellung - Dokument 0250: Asset Lifecycle

ewpage

Chapter 52

Anhang: Datenflüsse und Schnittstellen (Template)

Dokument-ID: 0720
Dokumenttyp: Anhang/Template
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

52.1 1. Zweck und Zielsetzung

Die Dokumentation der Datenflüsse und Schnittstellen von **AdminSend GmbH** unterstützt: - Schutzbedarfsfeststellung (Dokument 0060) - Risikoanalyse (Dokument 0090) - Kryptokonzept (Dokument 0340/0350) - Datenschutz-Compliance (Dokument 0420/0430)

Verantwortlich: Thomas Weber (ISB), Anna Schmidt (IT-Leitung)

52.2 2. Datenfluss-Register

Datenfluss-ID	Quelle	Ziel	Datenarten	Schutzbedarf (C/I/A)	Transportweg	Verschlüsselung	Speicherung	Provider/Drittland	Owner	Rechtsgrundlage	Notiz
DF-001	Webserver ({{ net-box.device.name }})	Datenbank-Server	Kundendaten (personenbezogen)	Hoch/Hoch/Hoch	{{ net-box.vlan.name }} (intern)	TLS 1.3	Verschlüsselt (AES-256)	Intern	Anna Schmidt	DSGVO Art. 6(1)(b)	[TODO]

Datenfluss-ID	Quelle	Ziel	Datenarten	Schutzbedarf (C/I/A)	Transportverschlüsselung	Speicherverschlüsselung	Provider/Drittland	Rechtsgrundlage	Notiz
DF-002	Backup-Server	Cloud-Storage (AWS S3)	Backup-Daten	Hoch/Hoch/Hoch	TLS 1.3 + IPsec (VPN)	Verschlüsselt (AES-256)	AWS (EU-West-1)	Anna Schmidt	DSGVO Art. 28	[TODO]
DF-003	Mitarbeiter (Remote)	VPN-Gateway	Geschäftsdaten	Hoch/Hoch/Normal	Internet IPsec/IKEv2	N/A	Intern	Anna Schmidt	-	[TODO]
DF-004	ERP-System	Payment-Gateway	Zahlungsdaten	Hoch/Sehr hoch/Hoch	Internet (HTTPS) TLS 1.3	Nicht gespeichert	Payment-Provider (EU)	Anna Schmidt	PCI-DSS	[TODO]
DF-005	SIEM	Log-Archiv	Log-Daten	Normal/{{ net-box.vlan.name }} (Management)	Hoch/Normal TLS 1.2	Verschlüsselt	Intern	Thomas Weber	-	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

52.3 3. Schnittstellen-Register

Schnittstellen-ID	System A	System B	Protokoll	Port	Authentisierung	Verschlüsselung	Datenrichtung	Frequenz	Owner	Notiz
IF-001	Webserver	Datenbank	PostgreSQL	5432	Zertifikat	TLS 1.3	Bidirektional	Permanent	Anna Schmidt	[TODO]
IF-002	ERP	CRM	REST API	443	OAuth 2.0	TLS 1.3	Bidirektional	Echtzeit	Anna Schmidt	[TODO]
IF-003	Monitoring	SIEM	Syslog	514	Zertifikat	TLS 1.2	Unidirektional	Permanent	Thomas Weber	[TODO]
IF-004	AD	LDAP-Clients	LDAPS	636	Kerberos	TLS 1.2	Bidirektional	On-Demand	Anna Schmidt	[TODO]
IF-005	Backup-Server	Cloud-Storage	S3 API	443	API-Key	TLS 1.3	Unidirektional	Täglich	Anna Schmidt	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

52.4 4. Externe Schnittstellen und Drittanbieter

Drittanbieter	Service	Datenarten	Schutzbedarf	Standort/Drittland	Vertrag	Datenschutz-Vereinbarung	Owner	Notiz
AWS	Cloud-Hosting (EC2, S3)	Geschäftsdaten, Backup	Hoch/Hoch/Hoch	EU: West-1	[TODO: Vertragsnummer]	Ja (Art. 28 DSGVO)	Anna Schmidt	[TODO]
Microsoft	Office 365	E-Mail, Dokumente	Hoch/Hoch/Normal	EU	[TODO]	Ja	Anna Schmidt	[TODO]
Payment Provider	Zahlungsabwicklung	Zahlungsdaten	Sehr hoch/Sehr hoch/Hoch	EU	[TODO]	Ja	Anna Schmidt	PCI-DSS zertifiziert
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Referenz: Dokument 0400/0410 (Lieferanten und Auslagerungsmanagement)

52.5 5. Datenfluss-Diagramme

Ablageort: `diagrams/dataflows.png` oder [TODO: Confluence/SharePoint]

Empfohlene Diagramme: 1. **High-Level Datenfluss:** Übersicht über alle Hauptdatenflüsse 2. **Detaillierte Datenflüsse:** Pro kritischem System/Service 3. **Externe Datenflüsse:** Alle Datenflüsse zu Drittanbietern 4. **Personenbezogene Daten:** DSGVO-relevante Datenflüsse

Tools: [TODO: z.B. Lucidchart, Draw.io, Visio]

52.6 6. Datenkategorien

52.6.1 6.1 Personenbezogene Daten (DSGVO)

- Kundendaten (Name, Adresse, E-Mail, etc.)
- Mitarbeiterdaten (HR-Daten)
- Besondere Kategorien (Art. 9 DSGVO): [TODO: falls zutreffend]

52.6.2 6.2 Geschäftsdaten

- Verträge
- Finanzdaten
- Geschäftsgeheimnisse
- Strategische Dokumente

52.6.3 6.3 Technische Daten

- Log-Daten
- Monitoring-Daten
- Konfigurationsdaten

52.6.4 6.4 Öffentliche Daten

- Marketing-Materialien
- Öffentliche Website-Inhalte

52.7 7. Verschlüsselungsanforderungen

Datenart	Schutzbedarf	Transport-Verschlüsselung	Speicher-Verschlüsselung	Schlüsselverwaltung
Personenbezogene Daten	Sehr hoch	TLS 1.3 (min. TLS 1.2)	AES-256	HSM/KMS
Geschäftsdaten	Hoch	TLS 1.3 (min. TLS 1.2)	AES-256	KMS
Log-Daten	Normal	TLS 1.2	Optional	KMS
Öffentliche Daten	Normal	TLS 1.2	Nicht erforderlich	-

Referenz: Dokument 0340/0350 (Kryptografie und Key Management)

52.8 8. Grenzüberschreitende Datenübermittlung

Datenübermittlung in Drittländer:

Zielland	Datenarten	Rechtsgrundlage	Garantien	Genehmigung	Notiz
USA	[TODO]	Standardvertragsklauseln (SCC)	[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Referenz: Dokument 0420/0430 (Datenschutz)

52.9 9. Verantwortlichkeiten (RACI)

Aktivität	IT-Leitung	ISB	Datenschutzbeauftragter	Fachbereich
Datenflüsse dokumentieren	A	C	C	R
Schutzbedarf festlegen	A	R	C	C
Verschlüsselung implementieren	R	C	I	I
Drittanbieter-Verträge prüfen	C	C	R	A
Jährlicher Review	A	R	C	C

Legende: - **R** = Responsible (Durchführungsverantwortung) - **A** = Accountable (Gesamtverantwortung) - **C** = Consulted (Konsultiert) - **I** = Informed (Informiert)

52.10 10. Änderungsmanagement

Änderungen an Datenflüssen: - Neue Datenflüsse müssen vor Inbetriebnahme dokumentiert werden - Änderungen an bestehenden Datenflüssen erfordern Change-Ticket - Sicherheitsrelevante Änderungen erfordern ISB-Freigabe

Referenz: Dokument 0380/0390 (Change Management)

52.11 11. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
Datenschutzbeauftragter	[TODO]	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI Standard 200-2: IT-Grundschutz-Methodik (Strukturanalyse) - BSI IT-Grundschutz-Kompendium: CON.1 Kryptokonzept - Dokument 0050: Strukturanalyse - Dokument 0060: Schutzbedarfsfeststellung - Dokument 0090: Risikoanalyse - Dokument 0340/0350: Kryptografie und Key Management - Dokument 0420/0430: Datenschutz

ewpage

Chapter 53

Anhang: Netzplan und Zonenmodell (Template)

Dokument-ID: 0730
Dokumenttyp: Anhang
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

53.1 1. Zweck und Zielsetzung

Die Dokumentation der Netzarchitektur und des Zonenmodells von **AdminSend GmbH** dient: - Strukturanalyse (Dokument 0050) - Risikoanalyse (Dokument 0090) - Netzwerksicherheit (Dokument 0460/0470) - Incident Response (Dokument 0320/0330)

Verantwortlich: Anna Schmidt (IT-Leitung)

53.2 2. High-Level Netzplan

Ablageort: `diagrams/network-highlevel.png` oder [TODO: Confluence/SharePoint]

Darstellung: - Alle Netzwerkzonen - Firewalls und Trust Boundaries - Hauptverbindungen (Internet, WAN, VPN) - Kritische Systeme

Tools: [TODO: z.B. Lucidchart, Draw.io, Visio]

53.3 3. Netzwerkzonen und Segmentierung

Zone-ID	Zonenname	Beschreibung	Trust Level	Zugriffskontrolle	Verantwortlich	Notiz
Z-001	Internet	Öffentliches Internet	Untrusted	Firewall (Deny All)	Anna Schmidt	[TODO]
Z-002	DMZ	Demilitarisierte Zone (Webserver, Mail-Gateway)	Low Trust	Firewall (Whitelist)	Anna Schmidt	[TODO]
Z-003	Internal LAN	Internes Unternehmensnetzwerk	Trusted	Firewall (Default Allow)	Anna Schmidt	{{ netbox.vlan.name }}
Z-004	Server VLAN	Produktionsserver	High Trust	Firewall (Whitelist)	Anna Schmidt	{{ netbox.vlan.name }}
Z-005	Database VLAN	Datenbank-Server	High Trust	Firewall (Strict Whitelist)	Anna Schmidt	{{ netbox.vlan.name }}
Z-006	Management VLAN	Management-Netzwerk (Monitoring, Backup, Admin)	High Trust	Firewall (Strict Whitelist)	Anna Schmidt	{{ netbox.vlan.name }}
Z-007	Guest WiFi	Gast-WLAN	Untrusted	Captive Portal, Firewall	Anna Schmidt	[TODO]
Z-008	VPN	Remote-Zugriff (VPN)	Trusted (nach Authentisierung)	VPN-Gateway, MFA	Anna Schmidt	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

53.4 4. Trust Boundaries und Firewall-Regeln

53.4.1 4.1 Trust Boundaries

Definition: Trust Boundaries sind Grenzen zwischen Netzwerkzonen mit unterschiedlichem Vertrauensniveau.

Hauptgrenzen: 1. **Internet DMZ:** Firewall mit strikten Regeln (nur HTTP/HTTPS eingehend) 2. **DMZ Internal LAN:** Firewall mit Whitelist (nur definierte Verbindungen) 3. **Internal LAN Server VLAN:** Firewall mit Whitelist 4. **Server VLAN Database VLAN:** Firewall mit strikter Whitelist (nur DB-Ports) 5. **Management VLAN Alle Zonen:** Firewall mit strikter Whitelist (nur Admin-Zugriffe)

53.4.2 4.2 Firewall-Regeln (Beispiel)

Regel-ID	Quelle	Ziel	Service/Port	Aktion	Begründung	Owner
FW-001	Internet	DMZ (Webserver)	HTTPS (443)	Allow	Öffentlicher Webzugriff	Anna Schmidt
FW-002	DMZ (Webserver)	Server VLAN (App-Server)	HTTPS (8443)	Allow	Backend-Kommunikation	Anna Schmidt
FW-003	Server VLAN (App-Server)	Database VLAN (DB-Server)	PostgreSQL (5432)	Allow	Datenbank-Zugriff	Anna Schmidt
FW-004	Management VLAN	Alle Zonen	SSH (22), RDP (3389)	Allow	Admin-Zugriff	Anna Schmidt
FW-005	Guest WiFi	Internet	HTTP/HTTPS (80/443)	Allow	Internet-Zugriff für Gäste	Anna Schmidt
FW-006	Guest WiFi	Internal LAN	Alle	Deny	Isolation von internem Netzwerk	Anna Schmidt
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Referenz: Dokument 0460/0470 (Netzwerksicherheit)

53.5 5. Netzwerkgeräte

Gerät-ID	Typ	Modell	Standort	IP-Adresse	Management-IP	Rolle	Owner	Notiz
{{ net-box.device.id }}	{{ net-box.device.type }}	{{ net-box.device.model }}	{{ net-box.site.name }}	{{ net-box.ipaddress.address }}	[TODO]	{{ net-box.device.role }}	Anna Schmidt	[TODO]
[TODO]	Firewall	[TODO]	[TODO]	[TODO]	[TODO]	Perimeter-Firewall	Anna Schmidt	[TODO]
[TODO]	Switch	[TODO]	[TODO]	[TODO]	[TODO]	Core-Switch	Anna Schmidt	[TODO]
[TODO]	Router	[TODO]	[TODO]	[TODO]	[TODO]	Internet-Router	Anna Schmidt	[TODO]

NetBox-Integration: {{ netbox.url }}

53.6 6. VLANs

VLAN-ID	VLAN-Name	Netzwerk (CIDR)	Gateway	Beschreibung	Zone	Notiz
{{ net-box.vlan.id }}	{{ net-box.vlan.name }}	[TODO: z.B. 10.0.10.0/24]	[TODO]	[TODO]	[TODO]	[TODO]
[TODO]	Management	[TODO]	[TODO]	Management-Netzwerk	Z-006	[TODO]
[TODO]	Servers	[TODO]	[TODO]	Produktionsserver	Z-004	[TODO]
[TODO]	Database	[TODO]	[TODO]	Datenbank-Server	Z-005	[TODO]

53.7 7. Administrative Zugänge

53.7.1 7.1 Bastion/Jump Hosts

Bastion Host: [TODO: Hostname/IP]
Zweck: Zentraler Zugangspunkt für administrative Zugriffe auf Produktionssysteme
Authentisierung: MFA (Multi-Factor Authentication)
Protokolle: SSH, RDP
Logging: Alle Zugriffe werden geloggt (SIEM)

Referenz: Dokument 0200/0210 (Zugriffssteuerung)

53.7.2 7.2 Remote Admin

VPN-Gateway: [TODO: Hostname/IP]
Authentisierung: MFA (Multi-Factor Authentication)
Protokoll: IPsec/IKEv2 oder OpenVPN
Zugriff: Nur für autorisierte Administratoren
Logging: Alle VPN-Verbindungen werden geloggt

Referenz: Dokument 0470 (VPN und Admin-Zugänge)

53.7.3 7.3 Break-Glass-Zugang

Notfallzugang: [TODO: Beschreibung]
Aktivierung: Nur in Notfällen (dokumentiert)
Überwachung: Sofortige Benachrichtigung bei Nutzung

Referenz: BCM-Dokument (Notfallzugang)

53.8 8. Netzwerk-Monitoring

Monitoring-Tools: - **SIEM:** [TODO: z.B. Splunk, ELK] - **Network Monitoring:** [TODO: z.B. Nagios, Zabbix, PRTG] - **Flow Analysis:** [TODO: z.B. NetFlow, sFlow]

Überwachte Metriken: - Bandbreitennutzung - Firewall-Logs - Anomalien (z.B. Port-Scans, DDoS) - VPN-Verbindungen

Referenz: Dokument 0300/0310 (Logging und Monitoring)

53.9 9. Netzwerk-Diagramme

Verfügbare Diagramme: 1. **High-Level Netzplan:** Übersicht über alle Zonen und Hauptverbindungen 2. **Detaillierter Netzplan:** Alle Geräte, VLANs, IP-Adressen 3. **Firewall-Topologie:** Alle Firewalls und Trust Boundaries 4. **WAN-Topologie:** Standortvernetzung (falls zutreffend) 5. **Cloud-Integration:** Verbindungen zu Cloud-Providern (AWS, Azure, etc.)

Ablageort: `diagrams/` oder [TODO: Confluence/SharePoint]

53.10 10. Standortvernetzung (WAN)

Falls zutreffend:

Standort	Verbindungstyp	Bandbreite	Provider	Backup-Verbindung	Verschlüsselung	Notiz
{{ netbox.site.name }}	[TODO: z.B. MPLS, VPN]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

53.11 11. Cloud-Integration

Cloud-Provider:

Provider	Service	Verbindungstyp	Verschlüsselung	Region	Notiz
AWS	EC2, S3, RDS	VPN (Site-to-Site)	IPsec	EU-West-1	[TODO]
Azure	[TODO]	ExpressRoute	[TODO]	West Europe	[TODO]
[TODO]	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

Referenz: Dokument 0400/0410 (Lieferanten und Cloud-Sicherheit)

53.12 12. Verantwortlichkeiten (RACI)

Aktivität	IT-Leitung	Netzwerk-Admin	ISB	Firewall-Admin
Netzplan pflegen	A	R	I	C
Firewall-Regeln ändern	A	C	C	R
VLAN-Konfiguration	A	R	I	I
Netzwerk-Monitoring	A	R	C	I
Jährlicher Review	A	R	C	C

Legende: - **R** = Responsible (Durchführungsverantwortung) - **A** = Accountable (Gesamtverantwortung) - **C** = Consulted (Konsultiert) - **I** = Informed (Informiert)

53.13 13. Änderungsmanagement

Änderungen an Netzwerkarchitektur: - Alle Änderungen erfordern Change-Ticket - Sicherheitsrelevante Änderungen erfordern ISB-Freigabe - Netzplan muss nach Änderungen aktualisiert werden

Referenz: Dokument 0380/0390 (Change Management)

53.14 14. Freigabe

Rolle	Name	Datum	Freigabe
IT-Leitung	Anna Schmidt	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium: NET.1.1 Netzarchitektur und -design - BSI IT-Grundschutz-Kompendium: NET.1.2 Netzmanagement - BSI IT-Grundschutz-Kompendium: NET.3.2 Firewall - Dokument 0050: Strukturanalyse - Dokument 0090: Risikoanalyse - Dokument 0460/0470: Netzwerksicherheit

ewpage

Chapter 54

Anhang: Begriffe und Abkürzungen

Dokument-ID: 0740
Dokumenttyp: Anhang
Referenzrahmen: BSI IT-Grundschutz (BSI Standards 200-1/200-2/200-3)
Owner: IT Operations Manager
Version: 1.0.0
Status: {{ meta.document.status }}
Klassifizierung: internal
Letzte Aktualisierung: {{ meta.document.last_updated }}
Nächster Review: {{ meta.document.next_review }}

54.1 1. Zweck

Dieses Dokument definiert zentrale Begriffe und Abkürzungen, die in der ISMS-Dokumentation von **AdminSend GmbH** verwendet werden.

54.2 2. Begriffe

54.2.1 A

Asset
Wertgegenstand (z.B. Hardware, Software, Daten, Prozesse), der für die Organisation von Wert ist und geschützt werden muss.

Authentisierung
Prozess zur Überprüfung der Identität eines Benutzers, Systems oder einer Anwendung.

Autorisierung
Prozess zur Gewährung von Zugriffsrechten auf Ressourcen nach erfolgreicher Authentisierung.

Availability (Verfügbarkeit)
Eigenschaft, dass Informationen und Systeme bei Bedarf verfügbar und nutzbar sind.

54.2.2 B

Backup
Sicherungskopie von Daten, die zur Wiederherstellung im Falle eines Datenverlusts verwendet werden kann.

Basis-Sicherheitscheck
Überprüfung der Umsetzung der BSI-Grundschutz-Anforderungen (Soll-Ist-Vergleich).

Baustein
Modulare Sicherheitsanforderungen im BSI IT-Grundschutz-Kompendium, die auf bestimmte Zielobjekte (z.B. Server, Anwendungen) angewendet werden.

BSI
Bundesamt für Sicherheit in der Informationstechnik (Deutschland).

54.2.3 C

CIA-Triade
Confidentiality (Vertraulichkeit), Integrity (Integrität), Availability (Verfügbarkeit) – die drei Grundprinzipien der Informationssicherheit.

CMDB
Configuration Management Database – Datenbank zur Verwaltung von IT-Assets und deren Konfigurationen.

Confidentiality (Vertraulichkeit)
Eigenschaft, dass Informationen nur autorisierten Personen zugänglich sind.

54.2.4 D

Datenschutz
Schutz personenbezogener Daten vor Missbrauch (rechtlicher Rahmen: DSGVO).

DMZ
Demilitarisierte Zone – Netzwerksegment zwischen internem Netzwerk und Internet, das öffentlich zugängliche Dienste hostet.

DSGVO
Datenschutz-Grundverordnung (EU-Verordnung 2016/679).

54.2.5 E

Encryption (Verschlüsselung)
Umwandlung von Daten in eine unleserliche Form, um Vertraulichkeit zu gewährleisten.

Endpoint
Endgerät (z.B. Laptop, Desktop, Smartphone), das mit dem Netzwerk verbunden ist.

54.2.6 F

Firewall
Sicherheitssystem zur Kontrolle des Netzwerkverkehrs zwischen verschiedenen Netzwerksegmenten.

54.2.7 G

Gap-Analyse
Vergleich zwischen Soll-Zustand (Anforderungen) und Ist-Zustand (Umsetzung) zur Identifikation von Lücken.

54.2.8 H

Hardening
Härtung von Systemen durch Entfernung unnötiger Dienste, Anwendung von Sicherheitspatches und Konfiguration nach Best Practices.

HSM
Hardware Security Module – Spezialhardware zur sicheren Verwaltung kryptografischer Schlüssel.

54.2.9 I

IAM
Identity and Access Management – Verwaltung von Benutzeridentitäten und Zugriffsrechten.

Incident
Sicherheitsvorfall, der die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen beeinträchtigt.

Informationsverbund
Abgegrenzte Menge aus Prozessen, Informationen, IT-Systemen, Personen und Räumen, die im Rahmen des ISMS betrachtet werden.

Integrity (Integrität)
Eigenschaft, dass Informationen vollständig, korrekt und unverändert sind.

ISB
Informationssicherheitsbeauftragter – Verantwortlicher für das ISMS.

ISMS
Informationssicherheitsmanagementsystem – Systematischer Ansatz zur Verwaltung von Informationssicherheit.

ISO 27001
Internationale Norm für Informationssicherheitsmanagementsysteme.

54.2.10 K

KMS
Key Management System – System zur Verwaltung kryptografischer Schlüssel.

KPI
Key Performance Indicator – Kennzahl zur Messung der Leistung/Wirksamkeit.

54.2.11 L

Least Privilege
Prinzip, dass Benutzer nur die minimal notwendigen Zugriffsrechte erhalten.

Logging
Aufzeichnung von Ereignissen und Aktivitäten in Systemen zur Nachvollziehbarkeit und Analyse.

54.2.12 M

MFA
Multi-Factor Authentication – Authentisierung mit mindestens zwei unabhängigen Faktoren (z.B. Passwort + Token).

Modellierung
Zuordnung von BSI-Bausteinen zu Zielobjekten im Informationsverbund.

54.2.13 N

NetBox
Open-Source-Tool zur Verwaltung von Netzwerk- und Datacenter-Infrastruktur (IPAM, DCIM).

54.2.14 P

Patch
Software-Update zur Behebung von Sicherheitslücken oder Fehlern.

Penetrationstest
Simulierter Angriff auf Systeme zur Identifikation von Sicherheitslücken.

Policy
Richtlinie auf hoher Ebene, die Sicherheitsziele und -prinzipien definiert.

54.2.15 R

RACI
Responsibility Assignment Matrix: Responsible, Accountable, Consulted, Informed – Modell zur Klärung von Verantwortlichkeiten.

Risikoanalyse
Systematische Identifikation, Bewertung und Behandlung von Risiken.

Risikoakzeptanz
Bewusste Entscheidung, ein identifiziertes Risiko zu akzeptieren (ohne weitere Maßnahmen).

RTO
Recovery Time Objective – Maximale tolerierbare Ausfallzeit eines Systems/Prozesses.

RPO
Recovery Point Objective – Maximaler tolerierbarer Datenverlust (Zeitspanne).

54.2.16 S

Schutzbedarf
Bewertung der Kritikalität von Assets hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit (Normal, Hoch, Sehr hoch).

SIEM
Security Information and Event Management – System zur zentralen Sammlung und Analyse von Sicherheitsereignissen.

SoA
Statement of Applicability – Erklärung zur Anwendbarkeit von Sicherheitsmaßnahmen (ISO 27001).

Strukturanalyse
Erfassung und Dokumentation der IT-Infrastruktur und Prozesse im Informationsverbund.

54.2.17 T

TLS
Transport Layer Security – Kryptografisches Protokoll zur sicheren Datenübertragung.

Trust Boundary
Grenze zwischen Netzwerksegmenten mit unterschiedlichem Vertrauensniveau.

54.2.18 V

VLAN
Virtual Local Area Network – Logische Segmentierung eines physischen Netzwerks.

Vulnerability
Schwachstelle in einem System, die von Angreifern ausgenutzt werden kann.

54.2.19 Z

Zero Trust
Sicherheitsmodell, das davon ausgeht, dass kein Benutzer oder System standardmäßig vertrauenswürdig ist.

54.3 3. Abkürzungen

Abkürzung	Bedeutung
AD	Active Directory
AES	Advanced Encryption Standard
API	Application Programming Interface
AV	Antivirus
AWS	Amazon Web Services
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
BSI	Bundesamt für Sicherheit in der Informationstechnik
C/I/A	Confidentiality / Integrity / Availability
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMDB	Configuration Management Database

Abkürzung	Bedeutung
CRM	Customer Relationship Management
DAST	Dynamic Application Security Testing
DB	Database
DCIM	Data Center Infrastructure Management
DDoS	Distributed Denial of Service
DMZ	Demilitarisierte Zone
DNS	Domain Name System
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DSGVO	Datenschutz-Grundverordnung
EDR	Endpoint Detection and Response
EOL	End of Life
ERP	Enterprise Resource Planning
GDPR	General Data Protection Regulation (DSGVO)
HR	Human Resources
HSM	Hardware Security Module
HTTP/HTTPS	Hypertext Transfer Protocol (Secure)
IAM	Identity and Access Management
IDS/IPS	Intrusion Detection/Prevention System
IoT	Internet of Things
IP	Internet Protocol
IPAM	IP Address Management
IPsec	Internet Protocol Security
ISB	Informationssicherheitsbeauftragter
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Informationstechnologie
ITSM	IT Service Management
KMS	Key Management System
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
LMS	Learning Management System
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MPLS	Multiprotocol Label Switching
NAC	Network Access Control
NDA	Non-Disclosure Agreement
OS	Operating System
PaaS	Platform as a Service
PCI-DSS	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
RACI	Responsible, Accountable, Consulted, Informed
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RPO	Recovery Point Objective
RTO	Recovery Time Objective

Abkürzung	Bedeutung
SaaS	Software as a Service
SAST	Static Application Security Testing
SCC	Standard Contractual Clauses
SDLC	Software Development Lifecycle
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SoA	Statement of Applicability
SOC	Security Operations Center
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer (veraltet, siehe TLS)
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

54.4 4. BSI-spezifische Begriffe

BSI Standard 200-1
Managementsysteme für Informationssicherheit (ISMS)

BSI Standard 200-2
IT-Grundschutz-Methodik

BSI Standard 200-3
Risikoanalyse auf der Basis von IT-Grundschutz

IT-Grundschutz-Kompendium
Sammlung von Bausteinen mit Sicherheitsanforderungen für verschiedene Zielobjekte

Baustein
Modulare Sicherheitsanforderungen im IT-Grundschutz-Kompendium (z.B. APP.3.1 Webanwendungen, SYS.1.1 Allgemeiner Server)

Basis-Anforderungen
Mindestanforderungen, die für den Basis-Schutz umgesetzt werden müssen

Standard-Anforderungen
Anforderungen für den Standard-Schutz (über Basis hinaus)

Anforderungen bei erhöhtem Schutzbedarf
Zusätzliche Anforderungen für Assets mit hohem oder sehr hohem Schutzbedarf

54.5 5. Freigabe

Rolle	Name	Datum	Freigabe
ISB	Thomas Weber	{{ meta.document.approval_date }}	{{ meta.document.approval_status }}

Referenzen: - BSI IT-Grundschutz-Kompendium: Glossar - ISO 27000: Information security management systems – Overview and vocabulary - Alle ISMS-Dokumente (0010-0630)

ewpage