Contents

Chapter 1

Information Security Management System Handbook

Document Metadata

- **Created on:** 2026-02-05
- **Author:** Andreas Huemmer [andreas.huemmer@adminsend.de]
- **Version:** 0.0.2
- **Type:** ISMS Handbook

---

ewpage

Chapter 2

ISMS Policy / Information Security Policy

Document ID: 0010
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Clause 5.2 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

2.1 1. Purpose

This Information Security Policy defines the strategic principles and commitments of **AdminSend GmbH** for protecting information assets. It forms the foundation for the Information Security Management System (ISMS) according to ISO/IEC 27001:2022 and ensures that information security is understood and implemented as an integral part of all business processes.

2.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Systems and Information:** All IT systems, applications, data, and information processing processes
- **Personnel:** All employees, contractors, suppliers, and third parties with access to information assets
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions to this policy are only permitted through the defined exception process (see `0640_Policy_Exceptions_and_Risk_Waivers.md`).

2.3 3. Principles (Policy Statements)

AdminSend GmbH commits to the following information security principles:

2.3.1 3.1 Confidentiality

Information is only made accessible to authorized persons, systems, and processes. Access follows the need-to-know principle and is protected by appropriate access controls.

2.3.2 3.2 Integrity

The accuracy, completeness, and timeliness of information is ensured through appropriate controls. Unauthorized or unintended modifications are prevented and detected.

2.3.3 3.3 Availability

Information and IT systems are available to authorized users when needed. Business-critical systems are protected through appropriate redundancy and recovery measures.

2.3.4 3.4 Compliance and Legal Requirements

The organization complies with all applicable legal, regulatory, and contractual information security requirements, including data protection (GDPR), industry standards, and customer requirements.

2.3.5 3.5 Risk-Based Approach

Information security measures are prioritized and implemented based on systematic risk analysis. Risks are identified, assessed, and treated according to defined criteria.

2.3.6 3.6 Continuous Improvement

The ISMS is continuously monitored, measured, and improved. Security incidents, audits, and reviews serve as the basis for improvement measures.

2.3.7 3.7 Awareness and Training

All employees are regularly trained on information security risks and their responsibilities. Security awareness is part of the corporate culture.

2.3.8 3.8 Supplier and Third-Party Management

Suppliers and third parties with access to information assets are evaluated according to security criteria and contractually obligated to comply with security requirements.

2.4 4. Roles and Responsibilities

2.4.1 RACI Matrix: ISMS Policy

Activity	CISO	CIO	Management	IT Operations	Business Units
Policy Creation	R/A	C	I	C	C
Policy Approval	C	C	A	I	I
Policy Communication	R	C	I	I	I
Policy Implementation	A	R	I	R	R
Policy Monitoring	R/A	C	I	C	C
Policy Review	R/A	C	C	I	I

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

2.4.2 Key Roles

- **CISO (Chief Information Security Officer):** Thomas Weber (thomas.weber@adminsend.de)
  - Responsible for developing, implementing, and monitoring the ISMS
  - Reports to: Anna Schmidt
- **CIO (Chief Information Officer):** Anna Schmidt (anna.schmidt@adminsend.de)
  - Responsible for IT strategy and IT operations
  - Supports ISMS implementation
- **Management:** {{ meta.management.ceo }}
  - Approves ISMS policy and provides resources
  - Bears overall responsibility for information security

2.5 5. Derivations (Policies/Standards/Processes)

This abstract policy is detailed through the following documents:

2.5.1 Basis ISMS Documents

- `0020_ISMS_Scope.md` - ISMS Scope Definition
- `0030_ISMS_Context_and_Interested_Parties.md` - Context of Organization
- `0040_ISMS_Governance_Roles_and_Responsibilities.md` - ISMS Governance
- `0060_ISMS_Risk_Management_Methodology.md` - Risk Management Methodology

2.5.2 Topic-Specific Policies (Abstract)

- `0220_Policy_Access_Control_and_Identity_Management.md`
- `0240_Policy_Authentication_and_Passwords.md`
- `0260_Policy_Cryptography_and_Key_Management.md`
- `0280_Policy_Data_Classification_and_Information_Handling.md`
- [Additional policies see ISMS document structure]

2.5.3 Detailed Guidelines

- See corresponding guideline documents (0210-0690, odd numbers)

2.6 6. Compliance, Monitoring, and Enforcement

2.6.1 Metrics and KPIs

- Number of security incidents per quarter
- Average time to remediate critical vulnerabilities
- Training participation rate (Target: 100% annually)
- Audit findings and remediation rate
- Compliance rate with security policies

2.6.2 Evidence and Documentation

- ISMS documentation and records
- Audit reports (internal and external)
- Risk register and risk treatment plans
- Training records and awareness campaigns
- Incident reports and lessons learned

2.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes and may result in disciplinary action, including: - Warning and retraining - Revocation of access rights - Employment consequences - Legal action for intentional or grossly negligent violations

2.7 7. Exceptions

Exceptions to this policy are only permitted in justified exceptional cases and must be requested through the defined exception process:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by the CISO and, if applicable, management
- **Documentation:** All exceptions are documented in the risk register and regularly reviewed
- **Time Limitation:** Exceptions are generally time-limited and must be renewed regularly

2.8 8. References

2.8.1 Internal Documents

- ISMS Document Structure (see README.md)
- Risk Register (`0080_ISMS_Risk_Register_Template.md`)
- Statement of Applicability (`0100_ISMS_Statement_of_Applicability_SoA_Template.md`)
- Internal Audit Program (`0130_ISMS_Internal_Audit_Program.md`)

2.8.2 External Standards and Regulations

- **ISO/IEC 27001:2022** - Information security management systems - Requirements
- **ISO/IEC 27001:2022/Amd 1:2024** - Amendment 1 (Annex A updates)
- **ISO/IEC 27002:2022** - Information security controls
- **GDPR (EU 2016/679)** - General Data Protection Regulation
- **BSI IT-Grundschutz** - German Federal Office for Information Security

---

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 3

ISMS Scope

Document ID: 0020
Document Type: ISMS Foundation Document
Standard Reference: ISO/IEC 27001:2022 Clause 4.3
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

3.1 1. Scope Definition

The scope of the Information Security Management System (ISMS) of **AdminSend GmbH** includes:

3.1.1 1.1 Organization

- **Organization Name:** AdminSend GmbH
- **Legal Form:** {{ meta.organization.legal_form }}
- **Headquarters:** Musterstraße 123
- **Number of Employees:** {{ meta.organization.employee_count }}
- **Industry:** {{ meta.organization.industry }}

3.1.2 1.2 Locations

The ISMS applies to the following locations:

- **Main Location:** {{ netbox.site.name }}
  - Address: {{ netbox.site.address }}
  - Function: Data center, offices, development

[TODO: Add additional locations]

3.1.3 1.3 Processes and Services

The ISMS covers the following business processes and IT services:

Core Processes: - IT operations and infrastructure management - Software development and DevOps - Data processing and data management - Customer service and support - [TODO: Additional core processes]

IT Services: - Network infrastructure ({{ netbox.device.core_switch.name }}) - Server and virtualization platforms - Cloud services and SaaS applications - Database systems - Backup and recovery systems - [TODO: Additional IT services]

3.1.4 1.4 Information Assets

The ISMS protects the following categories of information assets:

Data and Information: - Customer data (personal data according to GDPR) - Business data (contracts, financial data, strategic documents) - Technical data (source code, system documentation, configurations) - Employee data (HR data, access credentials)

IT Systems and Infrastructure: - Production systems and development environments - Network components (routers, switches, firewalls) - Endpoints (laptops, workstations, mobile devices) - Cloud infrastructure and virtual machines

Applications and Software: - Business applications (ERP, CRM, etc.) - Development tools and CI/CD pipelines - Communication platforms (email, collaboration tools)

3.1.5 1.5 Systems and Platforms

The ISMS includes the following technical platforms:

Network Infrastructure: - Core Switch: {{ netbox.device.core_switch.name }} - Management VLAN: {{ netbox.vlan.management.vid }} - [TODO: Additional network components from NetBox]

Servers and Virtualization: - [TODO: Server list from asset inventory]

Cloud Platforms: - [TODO: AWS/Azure/GCP accounts and services]

Security Systems: - Firewall, IDS/IPS, SIEM - Endpoint Protection (EDR/AV) - Identity and Access Management (IAM)

3.2 2. Scope Boundaries and Exclusions

3.2.1 2.1 Excluded Areas

The following areas are explicitly excluded from the ISMS scope:

[TODO: Define exclusions, e.g.:] - Production facilities (if not IT-relevant) - External supplier systems (outside our control) - Legacy systems being phased out (with decommission date)

3.2.2 2.2 Justification for Exclusions

A justification is documented for each exclusion:

[TODO: Justifications for exclusions] - **Example:** Legacy system XYZ will be decommissioned on [date] and no longer contains critical data.

3.2.3 2.3 Risks and Dependencies from Exclusions

Exclusions are recorded and assessed in the risk register:

[TODO: Risk assessment for exclusions] - See `0080_ISMS_Risk_Register_Template.md` for details

3.3 3. Interfaces

3.3.1 3.1 External Organizations and Providers

The ISMS has interfaces with the following external parties:

Cloud Providers: - [TODO: AWS/Azure/GCP - services and responsibilities]

Managed Service Providers: - [TODO: MSP partners and their access]

Suppliers and Service Providers: - [TODO: Critical suppliers with access to information assets]

3.3.2 3.2 Other Management Systems

The ISMS is integrated with the following other management systems:

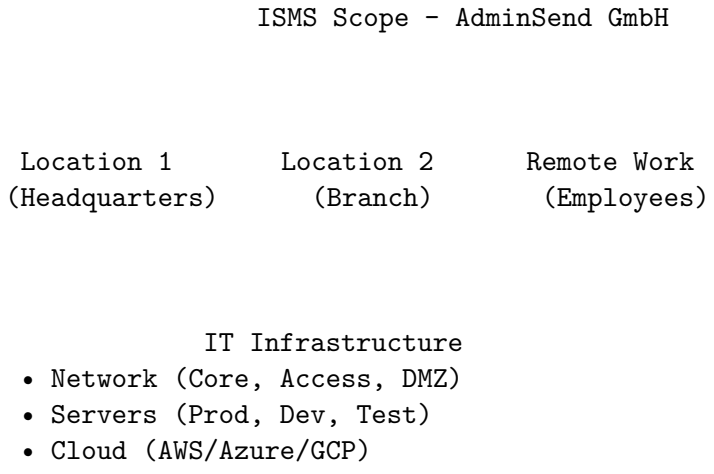
Business Continuity Management (BCM): - Interface to BCM handbook (see `0440_Policy_Business_Contin` - Joint risk analysis and BIA

Data Protection Management System (DPMS): - Interface to GDPR compliance (see `0560_Policy_Data_Protection_Interfaces.md`) - Joint processing records and data protection impact assessments

Quality Management System (QMS): - [TODO: Interfaces to ISO 9001 or other QMS]

3.4 4. Scope Diagram

The following diagram visualizes the ISMS scope:



- Endpoints (Laptops, Workstations, Mobile)

Business Processes

- IT Operations & Support
- Software Development
- Data Processing
- Customer Service

Information Assets

- Customer Data (GDPR-relevant)
- Business Data (Contracts, Finances)
- Technical Data (Code, Configs)
- Employee Data (HR)

```
External Interfaces:
  Cloud Providers (AWS/Azure/GCP)
  Managed Service Providers
  Suppliers and Service Providers
  Customers and Partners

Exclusions:
  [TODO: Excluded areas]
  [TODO: Legacy systems being phased out]
```

[TODO: Create detailed scope diagram and link] - File: `diagrams/isms_scope.png`

3.5 5. Scope Changes and Review

3.5.1 5.1 Change Management

Changes to the ISMS scope must be made through the change management process: - See `0360_Policy_Change_and_Release_Management.md` - Scope changes require approval by CISO and management - Impacts on risk analysis and SoA must be assessed

3.5.2 5.2 Regular Review

The ISMS scope is regularly reviewed: - **Annual Review:** As part of management review (see `0140_ISMS_Management_Review_Template.md`) - **Event-Driven Review:** For significant organizational changes (mergers, acquisitions, new locations, new services)

3.6 6. References

3.6.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0030_ISMS_Context_and_Interested_Parties.md` - Context of Organization
- `0050_ISMS_Structure_Analysis_Template.md` - Structure Analysis (if available)
- `0080_ISMS_Risk_Register_Template.md` - Risk Register
- `0100_ISMS_Statement_of_Applicability_SoA_Template.md` - SoA

3.6.2 External Standards

- **ISO/IEC 27001:2022** - Clause 4.3: Determining the scope of the ISMS
- **ISO/IEC 27002:2022** - Information security controls

Approved by:
Thomas Weber, CISO
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

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

ewpage

Chapter 4

Context of the Organization and Interested Parties

Document ID: 0030
Document Type: ISMS Foundation Document
Standard Reference: ISO/IEC 27001:2022 Clauses 4.1, 4.2
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

4.1 1. Context of the Organization

4.1.1 1.1 Internal Issues

Organizational Structure: - Organizational Form: {{ meta.organization.legal_form }} - Number of Employees: {{ meta.organization.employee_count }} - Organizational Structure: [TODO: Hierarchy, departments] - Locations: {{ netbox.site.name }} and others

Business Processes: - Core Business: {{ meta.organization.industry }} - Critical Business Processes: [TODO: List of critical processes] - IT Dependency: High / Medium / Low

Technology and IT Infrastructure: - IT Strategy: [TODO: Cloud-first, hybrid, on-premise] - Technology Stack: [TODO: Main technologies] - Digitalization Level: [TODO: Assessment] - Legacy Systems: [TODO: Number and criticality]

Corporate Culture: - Security Awareness: [TODO: Assessment] - Risk Appetite: Conservative / Moderate / Progressive - Innovation Culture: [TODO: Assessment] - Remote Work Percentage: [TODO: Percentage]

Resources: - IT Budget: [TODO: Magnitude] - Security Budget: [TODO: Percentage of IT budget] - Personnel Resources: [TODO: FTE for IT security] - External Support: [TODO: MSP, consultants]

4.1.2 1.2 External Issues

Market and Competition: - Industry: {{ meta.organization.industry }} - Market Position: [TODO: Market leader, challenger, niche] - Competitive Pressure: High / Medium / Low - Customer Expectations: [TODO: Security requirements]

Regulation and Compliance: - GDPR (EU 2016/679): Applicable - Industry-Specific Regulation: [TODO: e.g., KRITIS, NIS2, DORA] - International Standards: ISO 27001, ISO 27002 - Contractual Obligations: [TODO: Customer requirements]

Threat Landscape: - Cyber Threats: Ransomware, phishing, DDoS, APT - Threat Actors: Cybercriminals, hacktivists, nation-states - Industry-Specific Risks: [TODO: Specific threats] - Current Security Incidents: [TODO: Relevant incidents in the industry]

Supply Chains and Dependencies: - Cloud Providers: [TODO: AWS, Azure, GCP] - Managed Service Providers: [TODO: MSP partners] - Critical Suppliers: [TODO: Software suppliers, hardware suppliers] - Outsourcing: [TODO: Outsourced processes]

Technological Trends: - Cloud Computing: Increasing usage - AI and Automation: [TODO: Use cases] - IoT and OT: [TODO: Relevance] - Mobile and Remote Work: Increasing

4.2 2. Interested Parties (Stakeholders)

4.2.1 2.1 Stakeholder Analysis

Party	Expectations/Requirements	Relevance	Evidence/Source
Customers	Data protection, availability, confidentiality	High	Contracts, SLAs, NDA
Management	Risk minimization, compliance, business continuity	High	Corporate strategy
Employees	Secure work environment, data protection, training	High	HR policy, works council
Regulatory Authorities	GDPR compliance, reporting obligations	High	GDPR, NIS2, KRITIS
Suppliers/Partners	Security standards, confidentiality	Medium	Contracts, SLAs
Investors/Owners	Risk management, reputation	Medium	Business reports
Insurance	Security measures, incident response	Medium	Cyber insurance
Public/Media	Transparency, trust	Low	PR strategy

4.2.2 2.2 Detailed Stakeholder Requirements

Customers: - Requirements: Data protection (GDPR), availability (99.9% SLA), confidentiality (NDA) - Communication: Regular security updates, incident notifications - Evidence: SOC 2, ISO 27001 certificate, penetration test reports

Regulatory Authorities: - Requirements: GDPR compliance, reporting obligations (72h), data protection impact assessment - Communication: Incident reporting, audit cooperation - Evidence: Processing records, DPIA, incident reports

Employees: - Requirements: Secure work environment, data protection, training - Communication: Security awareness training, policy communication - Evidence: Training records, awareness campaigns

Suppliers and Partners: - Requirements: Security standards, confidentiality, incident notification - Communication: Security requirements in contracts, regular reviews - Evidence: Third-party risk assessments, security questionnaires

4.3 3. Requirements for the ISMS

4.3.1 3.1 Compliance Requirements (Legal/Regulatory)

Data Protection: - **GDPR (EU 2016/679):** General Data Protection Regulation - Requirements: Lawfulness, transparency, purpose limitation, data minimization - Implementation: See `0560_Policy_Data_Protection_Interfaces.md` - Evidence: Processing records, DPIA, privacy policy

Industry-Specific Regulation: - [TODO: KRITIS, NIS2, DORA, PCI-DSS, HIPAA, etc.] - Requirements: [TODO: Specific requirements] - Implementation: [TODO: Reference to relevant policies]

Labor Law and Works Council: - Co-determination on IT security measures - Data protection for employee data - Implementation: See `0520_Policy_HR_Security.md`

4.3.2 3.2 Contractual Requirements

Customer Contracts: - SLAs: Availability, performance, support - Security Requirements: Encryption, access control, audit rights - Certifications: ISO 27001, SOC 2, etc. - Incident Notification: Reporting obligations for security incidents

Supplier Contracts: - Security Requirements: See `0460_Policy_Suppliers_and_Cloud_Security.md` - SLAs and OLAs: Service Level Agreements - Audit Rights: Right to audit clauses

Insurance Contracts: - Cyber Insurance: Minimum requirements for security measures - Reporting Obligations: Incident reporting to insurance

4.3.3 3.3 Internal Requirements

Management: - Risk Management: Define acceptable risk levels - Business Continuity: RTO/RPO requirements - Compliance: Adherence to all legal and contractual obligations

IT Strategy: - Cloud-First Strategy: Security requirements for cloud services - DevOps and Agile: Security in DevOps (DevSecOps) - Innovation: Balance between innovation and security

Internal Policies: - See ISMS document structure (Policies 0200-0680) - Detailed guidelines (Guidelines 0210-0690)

4.4 4. Impact on the ISMS

4.4.1 4.1 Derivation of ISMS Objectives

From the context and stakeholder requirements, the following ISMS objectives are derived:

1. **Compliance:** Adherence to all legal and contractual requirements
2. **Risk Management:** Identification and treatment of information security risks
3. **Business Continuity:** Ensuring business continuity during security incidents
4. **Awareness:** Promoting security awareness among all employees
5. **Continuous Improvement:** Regular review and improvement of the ISMS

See `0110_ISMS_Security_Objectives_and_Metrics.md` for detailed objectives and KPIs.

4.4.2 4.2 Impact on Risk Analysis

The context and stakeholder requirements flow into the risk analysis: - See `0060_ISMS_Risk_Management_Methodol`
- See `0080_ISMS_Risk_Register_Template.md`

4.4.3 4.3 Impact on Statement of Applicability (SoA)

The requirements influence the selection and justification of Annex A controls: - See `0100_ISMS_Statement_of_Applicability_SoA_Template.md`

4.5 5. Review and Update

4.5.1 5.1 Regular Review

The context and stakeholder requirements are regularly reviewed: - **Annual Review:** As part of management review - **Event-Driven Review:** For significant changes (new regulation, new stakeholders, merger/acquisition)

4.5.2 5.2 Change Management

Changes to context or stakeholder requirements are documented and assessed: - Impact on ISMS scope, risk analysis, and SoA - Change management process: See `0360_Policy_Change_and_Release_Management.`

4.6 6. References

4.6.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0020_ISMS_Scope.md` - ISMS Scope
- `0060_ISMS_Risk_Management_Methodology.md` - Risk Management
- `0080_ISMS_Risk_Register_Template.md` - Risk Register
- `0100_ISMS_Statement_of_Applicability_SoA_Template.md` - SoA
- `0110_ISMS_Security_Objectives_and_Metrics.md` - Security Objectives

4.6.2 External Standards

- **ISO/IEC 27001:2022** - Clause 4.1: Understanding the organization and its context
- **ISO/IEC 27001:2022** - Clause 4.2: Understanding the needs and expectations of interested parties
- **GDPR (EU 2016/679)** - General Data Protection Regulation

---

Approved by:
Thomas Weber, CISO
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

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

ewpage

Chapter 5

ISMS Governance: Roles and Responsibilities

Document ID: 0040
Document Type: ISMS Foundation Document
Standard Reference: ISO/IEC 27001:2022 Clause 5.3
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

5.1 1. ISMS Governance Structure

5.1.1 1.1 Governance Overview

The ISMS governance of **AdminSend GmbH** is integrated into the overall organization and ensures that information security is anchored at all levels.

```
Management / Top Management
   ({{ meta.management.ceo }})
```

```
CIO                    CISO
Anna Schmidt          Thomas Weber
```

```
                ISMS Manager        Security
                                    Team



        Information Security Committee
        (Security Steering Committee)
  - CISO (Chair)
  - CIO
  - Business Unit Representatives
  - IT Operations
  - Data Protection Officer
  - Internal Audit (advisory)
```

5.1.2 1.2 Key Committees

Information Security Committee (Security Steering Committee): - **Chair:** Thomas Weber (CISO) - **Members:** CIO, business unit representatives, IT operations, data protection officer - **Frequency:** Quarterly or as needed - **Responsibilities:** - Strategic direction of the ISMS - Approval of security policies - Monitoring ISMS performance - Risk acceptance decisions - Budget approval for security measures

5.1.3 1.3 Interfaces to Other Functions

IT Service Management (ITSM): - Integration of security into ITIL processes - Incident management, change management, problem management - Contact: {{ meta.it.service_manager }}

Data Protection (DPMS): - Interface to GDPR compliance - Joint risk analysis and data protection impact assessment - Contact: {{ meta.privacy.dpo }}

Risk Management: - Integration into Enterprise Risk Management (ERM) - Shared risk register - Contact: {{ meta.risk.manager }}

Business Continuity Management (BCM): - Interface to BCM handbook - Joint BIA and emergency planning - Contact: {{ meta.bcm.manager }}

Internal Audit: - Independent review of the ISMS - Audit planning and execution - Contact: {{ meta.audit.manager }}

5.2 2. Role Descriptions

5.2.1 2.1 Management / Top Management

Role: {{ meta.management.ceo }}

Responsibilities: - Overall responsibility for information security - Approval of ISMS policy - Provision of resources for the ISMS - Promotion of security culture - Participation in management review

Authorities: - Approval of security budgets - Decision on strategic security initiatives - Approval of risk acceptances (for high risks)

5.2.2 2.2 CISO (Chief Information Security Officer)

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

Responsibilities: - Development, implementation, and monitoring of the ISMS - Leadership of the information security committee - Creation and maintenance of security policies - Conducting risk analyses - Incident response coordination - Reporting to management - Awareness and training

Authorities: - Approval of security policies - Ordering security measures - Escalation for critical security incidents - Access to all security-relevant information

Reporting Line: Reports to Anna Schmidt (CIO) and management

5.2.3 2.3 CIO (Chief Information Officer)

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

Responsibilities: - IT strategy and IT operations - Support of ISMS implementation - Provision of IT resources for security measures - Integration of security into IT processes

Authorities: - Approval of IT projects with security relevance - Resource allocation for IT security

5.2.4 2.4 ISMS Manager

Role: [TODO: Name and contact]

Responsibilities: - Operational implementation of the ISMS - Maintenance of ISMS documentation - Coordination of audits and reviews - Tracking of measures and findings - Support of the CISO

Authorities: - Coordination of ISMS activities - Request for information for audits

5.2.5 2.5 Asset Owner / Process Owner

Role: Business unit managers, process owners

Responsibilities: - Responsibility for information assets in their area - Classification of information - Definition of access rights - Implementation of security measures in their area - Reporting of security incidents

Authorities: - Approval of access rights for their assets - Decision on security measures in their area

5.2.6 2.6 Control Owner

Role: Responsible for specific security controls

Responsibilities: - Implementation and operation of security controls - Evidence of effectiveness - Reporting on control status - Remediation of control deficiencies

Authorities: - Implementation of security measures within their control

Examples: - Patch Management Control Owner: IT Operations - Access Control Owner: IAM Team - Backup Control Owner: Backup Administrator

5.2.7 2.7 IT Operations

Role: IT Operations Team

Responsibilities: - Implementation of technical security measures - Monitoring and alerting - Incident response (technical) - Patch management - Backup and recovery

Authorities: - Execution of security measures - Emergency access during incidents

5.2.8 2.8 Employees (all)

Role: All employees, contractors, third parties

Responsibilities: - Compliance with security policies - Reporting of security incidents - Participation in security awareness training - Protection of credentials and information

Authorities: - Access to information according to need-to-know principle

5.2.9 2.9 Internal Audit / Compliance

Role: {{ meta.audit.manager }}

Responsibilities: - Independent review of the ISMS - Audit planning and execution - Reporting of audit findings - Monitoring of measure implementation

Authorities: - Access to all ISMS-relevant information - Request for evidence and interviews

5.3 3. RACI Matrix: ISMS Processes

5.3.1 3.1 ISMS Core Processes

Activity	CISO	CIO	ISMS Manager	Asset Owner	IT Operations	Internal Audit
Develop ISMS strategy	R/A	C	C	I	I	I
Create policies	R/A	C	R	C	C	I
Conduct risk analysis	A	C	R	C	C	I
Plan risk treatment	A	C	R	C	R	I
Maintain SoA	A	I	R	C	C	I
Implement controls	A	C	C	R	R	I

Activity	CISO	CIO	ISMS Manager	Asset Owner	IT Operations	Internal Audit
Perform monitoring	A	I	C	I	R	I
Manage incidents	A	C	C	I	R	I
Conduct audits	C	C	C	C	C	R/A
Management review	R	C	R	I	I	C
Awareness training	A	C	R	I	I	I

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

5.3.2 3.2 Annex A Controls (Examples)

Control	Control Owner	Responsible	Accountable	Consulted	Informed
A.5.1 Policies	CISO	ISMS Manager	CISO	CIO, Business Units	All
A.5.7 Threat Intelligence	Security Team	Security Analyst	CISO	IT Operations	ISMS Manager
A.5.10 Acceptable Use	CISO	HR	CISO	IT Operations	All
A.5.15 Access Control	IAM Team	IAM Admin	CIO	CISO	IT Operations
A.5.23 Cloud Services	Cloud Architect	Cloud Admin	CIO	CISO	IT Operations
A.8.8 Backup	IT Operations	Backup Admin	CIO	CISO	ISMS Manager
A.8.16 Monitoring	Security Team	SOC Analyst	CISO	IT Operations	ISMS Manager

5.4 4. Escalation Paths

5.4.1 4.1 Security Incidents

```
Incident Detection


IT Operations / SOC


CISO (for critical incidents)


CIO / Management (for major incidents)


External Reporting (authorities, customers)
```

See `0400_Policy_Incident_Management.md` for details.

5.4.2 4.2 Risk Acceptance

```
Risk Identification


CISO (risk assessment)


CISO (risk acceptance for low/medium risks)


Management (risk acceptance for high risks)
```

See `0070_ISMS_Risk_Acceptance_Criteria.md` for details.

5.5 5. References

5.5.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0030_ISMS_Context_and_Interested_Parties.md` - Context
- `0060_ISMS_Risk_Management_Methodology.md` - Risk Management
- `0130_ISMS_Internal_Audit_Program.md` - Internal Audit Program

5.5.2 External Standards

- **ISO/IEC 27001:2022** - Clause 5.3: Organizational roles, responsibilities and authorities
- **ISO/IEC 27002:2022** - Control 5.2: Information security roles and responsibilities

---

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

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

ewpage

Chapter 6

Document Control / Documented Information

Document ID: 0050
Document Type: ISMS Foundation Document
Standard Reference: ISO/IEC 27001:2022 Clause 7.5
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

6.1 1. Purpose and Scope

This document defines the requirements for controlling documented information within the ISMS of **AdminSend GmbH**. It ensures that: - Documents are available and suitable for use - Documents are adequately protected - Documents are controlled in their creation, review, approval, and update

6.2 2. Storage and Access

6.2.1 2.1 Official Storage Location

Primary Storage: - **System:** [TODO: SharePoint, Confluence, DMS] - **Path:** [TODO: /ISMS/Documentation/] - **URL:** [TODO: https://docs.organization.com/isms/]

Backup and Archiving: - **Backup System:** {{ netbox.backup.system }} - **Backup Frequency:** Daily - **Archiving Duration:** 10 years after decommissioning

6.2.2 2.2 Access Control

Access Permissions:

Document Type	CISO	ISMS Manager	IT Operations	Business Units	All Employees
ISMS Policy	R/W	R/W	R	R	R
Policies (Abstract)	R/W	R/W	R	R	R
Guidelines (Detailed)	R/W	R/W	R/W	R	R
Risk Register	R/W	R/W	R	-	-
Audit Reports	R/W	R/W	-	-	-
Incident Reports	R/W	R/W	R/W	-	-

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

Access Management: - Access rights are managed via IAM system - See `0220_Policy_Access_Control_and_Ide` - Recertification: Quarterly

6.2.3 2.3 Offline/Emergency Access

Emergency Access: - Critical documents (emergency plans, contact lists) are additionally stored offline - Storage Location: [TODO: Physical safe, encrypted USB stick] - Responsible: Thomas Weber

Break-Glass Access: - See `0200_Emergency_Access_BreakGlass.md` (BCM Handbook) - Emergency access to ISMS documentation in case of primary system failure

6.3 3. Document Lifecycle

6.3.1 3.1 Creation

Process: 1. **Initiation:** Need is identified (e.g., new policy, new requirement) 2. **Assign Author:** CISO or ISMS Manager assigns author 3. **Use Template:** Author uses appropriate template 4. **Create Draft:** Author creates draft with status "Draft" 5. **Capture Metadata:** Document ID, owner, version, classification

Responsible: Document author (assigned by CISO)

6.3.2 3.2 Review

Review Process: 1. **Peer Review:** Technical review by colleagues 2. **Stakeholder Review:** Consultation with affected stakeholders 3. **CISO Review:** Final review by CISO 4. **Change Status:** From "Draft" to "In Review"

Review Criteria: - Technical correctness - Completeness - Consistency with other ISMS documents - Compliance with ISO 27001:2022 - Understandability and implementability

Responsible: CISO or ISMS Manager

6.3.3 3.3 Approval

Approval Process: 1. **Approval Request:** After successful review 2. **Approval:** By CISO (policies) or management (ISMS policy) 3. **Change Status:** From "In Review" to "Approved" 4. **Version Number:** Assign final version number (e.g., 1.0)

Approval Authorities:

Document Type	Approved By
ISMS Policy	Management
Policies (Abstract)	CISO
Guidelines (Detailed)	CISO or ISMS Manager
Process Documents	CISO or ISMS Manager
Templates	ISMS Manager

Responsible: See table above

6.3.4 3.4 Publication and Communication

Publication: 1. **Upload:** Document is published in official storage location 2. **Update Document Register:** Entry in document register 3. **Archive Old Version:** Previous version is archived

Communication: - **New Documents:** Email notification to all affected stakeholders - **Significant Changes:** Email notification + awareness campaign - **Minor Changes:** Entry in change log, no separate notification

Communication Channels: - Email to all employees - Intranet news - Security awareness training - Team meetings

Responsible: ISMS Manager

6.3.5 3.5 Change Management

Change Process: 1. **Change Request:** Need for change is identified 2. **Impact Assessment:** Assess impact of change 3. **Implement Change:** Document is updated 4. **Review and Approval:** As with new creation 5. **Increment Version Number:** Major (1.0 $\rightarrow$ 2.0) or Minor (1.0 $\rightarrow$ 1.1)

Versioning Scheme: - **Major Version (X.0):** Significant changes, new requirements - **Minor Version (X.Y):** Minor changes, corrections, clarifications

Change Log: Each document contains a change log with: - Version number - Date - Author - Description of change - Approver

Responsible: Document author, CISO

6.3.6 3.6 Regular Review

Review Intervals:

Document Type	Review Interval
ISMS Policy	Annually
Policies (Abstract)	Annually
Guidelines (Detailed)	Annually or as needed
Risk Register	Quarterly
SoA	Annually or upon scope change
Process Documents	Every 2 years

Review Triggers (event-driven): - New legal requirements - Significant organizational changes - Security incidents with lessons learned - Audit findings - Technology changes

Review Process: 1. **Review Reminder:** ISMS Manager reminds owner 2. **Conduct Review:** Owner checks currency and relevance 3. **Decision:** No change / Change required 4. **Documentation:** Update review date in document

Responsible: Document owner (see document register)

6.3.7 3.7 Archiving and Deletion

Archiving: - **Old Versions:** Are archived once new version is approved - **Archiving Duration:** 10 years - **Archiving Location:** [TODO: Archive system]

Deletion: - **Decommissioning:** Documents are deleted after archiving period expires - **Deletion Process:** Secure deletion according to `0580_Policy_Retention_and_Deletion.md` - **Approval:** Deletion must be approved by CISO

Responsible: ISMS Manager

6.4 4. Versioning

6.4.1 4.1 Versioning Scheme

Format: X.Y

- **X (Major Version):** Significant changes
  - New requirements
  - Structural changes
  - Change in scope
- **Y (Minor Version):** Minor changes
  - Corrections
  - Clarifications
  - Update of contact information

Examples: - 0.1 → Draft - 1.0 → First approved version - 1.1 → Minor correction - 2.0 → Major revision

6.4.2 4.2 Change Log

Each document contains a change log at the end:

```
## Change History

| Version | Date | Author | Description | Approved By |
|---------|------|--------|-------------|-------------|
| 1.0 | 2026-01-15 | Thomas Weber | Initial version | Management |
| 1.1 | 2026-03-20 | ISMS Manager | Contact information updated | CISO |
| 2.0 | 2026-12-01 | Thomas Weber | New requirements from NIS2 | Management |
```

6.5 5. Document Register

The document register is the central overview of all ISMS documents.

6.5.1 5.1 Document Register Structure

Document ID	Document Title	Owner	Status	Version	Last Change	Next Review
0010	ISMS Policy	Thomas Weber	Approved	1.0	{{ meta.document.date }}	{{ data.document.next_review }}
0020	ISMS Scope	Thomas Weber	Approved	1.0	{{ meta.document.date }}	{{ data.document.next_review }}
0030	Context and Stakeholders	Thomas Weber	Approved	1.0	{{ meta.document.date }}	{{ data.document.next_review }}
0040	ISMS Governance	Thomas Weber	Approved	1.0	{{ meta.document.date }}	{{ data.document.next_review }}
0050	Document Control	Thomas Weber	Approved	1.0	{{ meta.document.date }}	{{ data.document.next_review }}
...	...	...	...	...	...	...

[TODO: Create and maintain complete document register]

6.5.2 5.2 Maintenance of Document Register

Responsible: ISMS Manager

Updates: - With every document change - With status changes - With owner changes

Access: - Document register is readable by all employees - Storage location: [TODO: Link to document register]

6.6 6. Document Classification

All ISMS documents are classified according to `0280_Policy_Data_Classification_and_Information_Handling`

Classification	Description	Examples
Public	No confidentiality	Public policies
Internal	For employees only	Most ISMS documents
Confidential	Restricted access	Risk register, audit reports
Strictly Confidential	Very restricted access	Incident reports with sensitive data

Marking: - Classification is indicated in document header - Classification determines access rights and handling

6.7 7. External Documents

External Documents (e.g., supplier policies, certificates) are also controlled:

Process: 1. **Identification:** Identify relevant external documents 2. **Assessment:** Check relevance and trustworthiness 3. **Storage:** Store in separate area 4. **Marking:** Mark as "External Document" 5. **Review:** Regularly check for currency

Responsible: ISMS Manager

6.8 8. Retention Periods

Document Type	Retention Period	Legal Basis
ISMS Policy	10 years after decommissioning	ISO 27001
Policies and Guidelines	10 years after decommissioning	ISO 27001
Risk Register	10 years	ISO 27001
Audit Reports	10 years	ISO 27001, Commercial Law
Incident Reports	10 years	GDPR, NIS2
Training Records	10 years	Evidence requirement
Contracts	According to contract law	Commercial Law

See `0580_Policy_Retention_and_Deletion.md` for details.

6.9 9. References

6.9.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0040_ISMS_Governance_Roles_and_Responsibilities.md` - Governance
- `0280_Policy_Data_Classification_and_Information_Handling.md` - Data Classification
- `0360_Policy_Change_and_Release_Management.md` - Change Management
- `0580_Policy_Retention_and_Deletion.md` - Retention and Deletion

6.9.2 External Standards

- **ISO/IEC 27001:2022** - Clause 7.5: Documented information
- **ISO/IEC 27002:2022** - Control 5.1: Policies for information security

---

Approved by:
Thomas Weber, CISO
Date: {{ meta.document.approval_date }}

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

ewpage

Chapter 7

Risk Management – Methodology

Document ID: 0060
Document Type: ISMS Foundation Document
Standard Reference: ISO/IEC 27001:2022 Clause 6.1.2
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

7.1 1. Objective and Scope

7.1.1 1.1 Objective

This methodology defines how **AdminSend GmbH** systematically identifies, assesses, treats, and monitors information security risks. It ensures that: - Risks are assessed consistently and transparently - Risk treatment measures are prioritized - Risks are reduced to an acceptable level - Management can make informed decisions

7.1.2 1.2 Scope

This methodology applies to all information security risks within the ISMS scope (see `0020_ISMS_Scope.md`): - IT systems and infrastructure - Business processes - Information assets and data - Suppliers and third parties - Physical security

7.2 2. Risk Objects

7.2.1 2.1 Assets (Information Assets)

Categories: - **Information and Data:** Customer data, business data, technical data, employee data - **IT Systems:** Servers, network components, endpoints, cloud infrastructure - **Applications:** Business applications, development tools, communication platforms - **Services:** IT services,

business services - **People:** Employees with critical knowledge - **Physical Assets:** Data centers, offices, hardware

Asset Inventory: - See `0720_Appendix_Asset_and_System_Inventory_Template.md` - Asset owners are responsible for their assets

7.2.2 2.2 Business Processes

Critical Business Processes: - [TODO: List of critical business processes] - See Business Impact Analysis (BIA) in BCM handbook

Process Owners: - Responsible for risks in their process - See `0040_ISMS_Governance_Roles_and_Responsibili`

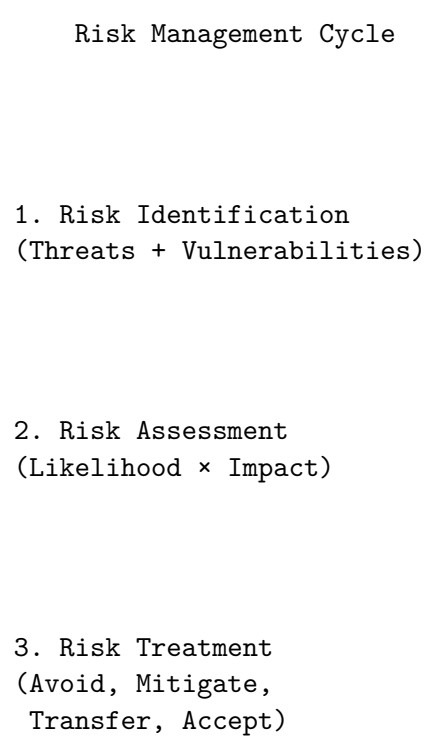
7.2.3 2.3 Suppliers and Outsourcing

Critical Suppliers: - Cloud providers (AWS, Azure, GCP) - Managed service providers - Software suppliers - See `0460_Policy_Suppliers_and_Cloud_Security.md`

Third-Party Risk Assessment: - Separate risk assessment for critical suppliers - See `0470_Guideline_Third_Party_Risk_Assessment_and_Cloud_Controls.md`

7.3 3. Risk Management Methodology

7.3.1 3.1 Risk Management Process



```
4. Risk Monitoring
(Monitoring, Review)
```

```
Continuous
Improvement
```

7.3.2 3.2 Risk Identification

Methods: 1. **Asset-based:** Identification of threats and vulnerabilities for each asset 2. **Scenario-based:** Analysis of threat scenarios (e.g., ransomware, DDoS, insider threat) 3. **Compliance-based:** Identification of compliance risks (GDPR, NIS2, etc.)

Risk Formula:

```
Risk = Threat × Vulnerability × Asset Value
```

Threats: - **Cyber Threats:** Ransomware, phishing, DDoS, APT, malware - **Human Threats:** Insider threat, social engineering, errors - **Environmental Threats:** Fire, water, power outage, natural disasters - **Technical Threats:** Hardware failure, software bugs, configuration errors

Vulnerabilities: - **Technical Vulnerabilities:** Unpatched systems, misconfigurations, weak encryption - **Organizational Vulnerabilities:** Missing policies, insufficient training, weak processes - **Physical Vulnerabilities:** Insufficient access control, missing redundancy

Sources for Risk Identification: - Threat Intelligence (CERT, MITRE ATT&CK, vendor advisories) - Vulnerability Scans (CVE, CVSS) - Penetration Tests - Security Incidents and Lessons Learned - Audit Findings - Compliance Requirements

7.3.3 3.3 Risk Assessment

Assessment Scales:

Likelihood:

Level	Description	Frequency
1 - Very Unlikely	Event is theoretically possible but very unlikely	$<$ 1 in 10 years
2 - Unlikely	Event could occur but is unlikely	1 in 5-10 years
3 - Possible	Event could occur	1 in 1-5 years
4 - Likely	Event will probably occur	1-5 times per year
5 - Very Likely	Event will almost certainly occur	$>$ 5 times per year

Impact:

Level	Description	Financial Damage	Reputational Damage	Compliance
1 - Negligible	Minimal impact	< €10,000	None	None
2 - Low	Minor impact	€10,000 - €50,000	Local	Minor violations
3 - Medium	Moderate impact	€50,000 - €250,000	Regional	Reportable incidents
4 - High	Significant impact	€250,000 - €1M	National	Fines
5 - Very High	Catastrophic impact	> €1M	International	Business prohibition

Risk Matrix:

```
Impact ↑
  5    M   H   H   VH  VH
  4    M   M   H   H   VH
  3    L   M   M   H   H
  2    L   L   M   M   H
  1    VL  L   L   M   M
                → Likelihood
       1   2   3   4   5

Legend:
VL = Very Low
L  = Low
M  = Medium
H  = High
VH = Very High
```

Risk Score Calculation:

```
Risk Score = Likelihood × Impact

Example:
Likelihood = 4 (Likely)
Impact = 3 (Medium)
Risk Score = 4 × 3 = 12 (High)
```

7.3.4 3.4 Risk Owner

Responsibilities: - Each identified risk has a risk owner - Risk owner is responsible for risk treatment - Typically: Asset owner, process owner, or CISO

Escalation: - High and very high risks are escalated to management - See `0070_ISMS_Risk_Acceptance_Criteria`

7.4 4. Sources for Risk Information

7.4.1 4.1 Threat Intelligence

External Sources: - **CERT-Bund:** https://www.cert-bund.de/ - **MITRE ATT&CK:** https://attack.mitre.org/ - **NIST NVD:** https://nvd.nist.gov/ - **Vendor Security Advisories:** Microsoft, Cisco, etc. - **Threat Intelligence Feeds:** [TODO: Commercial feeds]

Internal Sources: - Security incidents and lessons learned - Penetration test reports - Red team exercises

7.4.2 4.2 Vulnerabilities

Vulnerability Scanning: - **Tools:** [TODO: Nessus, Qualys, OpenVAS] - **Frequency:** Weekly (automated) - **Scope:** All systems in ISMS scope

CVE and CVSS: - Common Vulnerabilities and Exposures (CVE) - Common Vulnerability Scoring System (CVSS) - Prioritization by CVSS score

Patch Management: - See `0340_Policy_Vulnerability_and_Patch_Management.md`

7.4.3 4.3 Incidents and Findings

Security Incidents: - Each incident is reviewed for risk relevance - Lessons learned flow into risk analysis - See `0400_Policy_Incident_Management.md`

Audit Findings: - Internal and external audit findings - Findings are assessed as risks - See `0130_ISMS_Internal_Audit_Program.md`

7.5 5. Outputs of Risk Management

7.5.1 5.1 Risk Register

Content: - All identified risks - Risk assessment (likelihood, impact, score) - Risk owner - Risk treatment strategy - Status and measures

Document: `0080_ISMS_Risk_Register_Template.md`

Maintenance: - Quarterly review - Event-driven updates (new threats, incidents)

7.5.2 5.2 Risk Treatment Plan (RTP)

Content: - Planned measures for risk treatment - Responsible parties and deadlines - Budget and resources - Prioritization

Document: `0090_ISMS_Risk_Treatment_Plan_RTP_Template.md`

Tracking: - Measures are tracked in RTP - Regular reporting to CISO and management

7.5.3 5.3 Statement of Applicability (SoA)

Content: - Selection and justification of Annex A controls - Based on risk analysis and compliance requirements - Documentation of exclusions

Document: `0100_ISMS_Statement_of_Applicability_SoA_Template.md`

Relationship: - Risk analysis → Identification of required controls - SoA → Documentation of control selection - RTP → Implementation of controls

7.6 6. Risk Management Cycle

7.6.1 6.1 Regular Review

Frequency: - **Quarterly:** Review of risk register - **Annually:** Complete risk analysis - **Event-driven:** For significant changes

Triggers for Event-Driven Review: - New threats (e.g., zero-day exploits) - Significant organizational changes - New compliance requirements - Major security incidents - Audit findings

7.6.2 6.2 Risk Monitoring

Continuous Monitoring: - Security monitoring (SIEM, IDS/IPS) - Vulnerability scanning - Threat intelligence feeds - Incident tracking

KPIs: - Number of open risks (by risk level) - Average time to risk remediation - Number of accepted risks - Trend of risk scores

Reporting: - Quarterly to information security committee - Annually in management review

7.6.3 6.3 Continuous Improvement

Lessons Learned: - From security incidents - From audit findings - From penetration tests

Improvement Measures: - Adjustment of risk assessment scales - Improvement of risk identification methods - Optimization of risk management process

7.7 7. Roles and Responsibilities

7.7.1 7.1 RACI Matrix: Risk Management

Activity	CISO	ISMS Manager	Risk Owner	IT Operations	Management
Define risk management methodology	R/A	C	C	C	I
Risk identification	A	R	C	C	I
Risk assessment	A	R	C	C	I
Plan risk treatment	A	C	R	C	I
Implement measures	A	C	R	R	I

Activity	CISO	ISMS Manager	Risk Owner	IT Operations	Management
Risk acceptance (low/medium)	A	I	C	I	I
Risk acceptance (high/very high)	C	I	C	I	A
Risk monitoring	A	R	C	C	I
Risk reporting	R	R	C	I	I

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

7.8 8. References

7.8.1 Internal Documents

- `0020_ISMS_Scope.md` - ISMS Scope
- `0040_ISMS_Governance_Roles_and_Responsibilities.md` - Governance
- `0070_ISMS_Risk_Acceptance_Criteria.md` - Risk Acceptance Criteria
- `0080_ISMS_Risk_Register_Template.md` - Risk Register
- `0090_ISMS_Risk_Treatment_Plan_RTP_Template.md` - Risk Treatment Plan
- `0100_ISMS_Statement_of_Applicability_SoA_Template.md` - SoA
- `0340_Policy_Vulnerability_and_Patch_Management.md` - Vulnerability Management
- `0400_Policy_Incident_Management.md` - Incident Management

7.8.2 External Standards

- **ISO/IEC 27001:2022** - Clause 6.1.2: Information security risk assessment
- **ISO/IEC 27001:2022** - Clause 6.1.3: Information security risk treatment
- **ISO/IEC 27005:2022** - Information security risk management
- **NIST SP 800-30** - Guide for Conducting Risk Assessments

Approved by:
Thomas Weber, CISO
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

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

ewpage

Chapter 8

Risk Criteria and Risk Acceptance

Document ID: 0070
Document Type: ISMS Foundation Document
Standard Reference: ISO/IEC 27001:2022 Clause 6.1.2
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

8.1 1. Risk Appetite and Tolerance

8.1.1 1.1 Risk Appetite

AdminSend GmbH defines its risk appetite as follows:

General Risk Appetite: [TODO: Conservative / Moderate / Progressive]

Tolerance Thresholds by Risk Level:

Risk Level	Risk Score	Acceptable	Treatment Required
Very Low	1-2	Yes	Monitoring
Low	3-6	Yes	Monitoring
Medium	7-12	Conditional	Risk treatment recommended
High	13-20	No	Risk treatment required
Very High	21-25	No	Immediate risk treatment

8.1.2 1.2 Acceptance Criteria

Automatically Acceptable: - Risk score 6 (Low) - No compliance violations - No critical assets affected

Conditionally Acceptable: - Risk score 7-12 (Medium) - With compensating controls - Time-limited (max. 12 months)

Not Acceptable: - Risk score 13 (High/Very High) - Compliance violations - Critical assets without protection measures

8.2 2. Assessment Dimensions

8.2.1 2.1 CIA Triad

Confidentiality: - Protection against unauthorized disclosure - Classification: Public, Internal, Confidential, Strictly Confidential

Integrity: - Protection against unauthorized modification - Correctness and completeness of information

Availability: - Ensuring access when needed - RTO/RPO requirements

8.2.2 2.2 Additional Dimensions

Legal and Regulatory: - GDPR compliance - Industry-specific regulation - Contractual obligations

Reputation: - Impact on corporate image - Customer trust - Media coverage

8.3 3. Acceptance Process

8.3.1 3.1 Acceptance Authorities

Risk Level	Accepted By	Documentation	Approval
Very Low / Low	CISO	Risk register	CISO
Medium	CISO	Risk register + justification	CISO + CIO
High	Management	Risk register + formal risk acceptance	Management
Very High	Management	Risk register + formal risk acceptance + action plan	Management

8.3.2 3.2 Documentation Requirements

Minimum Information: - Risk ID and description - Risk assessment (likelihood, impact, score) - Justification for acceptance - Compensating controls (if any) - Acceptance date and validity period - Accepting person

Document: See `0080_ISMS_Risk_Register_Template.md`

8.3.3 3.3 Duration of Acceptances

Time Limits: - Low risks: Unlimited (with annual review) - Medium risks: Max. 12 months - High risks: Max. 6 months - Very high risks: Max. 3 months (exception)

Renewal: - Requires re-assessment and approval - Justification for renewal required

8.3.4 3.4 Review of Accepted Risks

Regular Review: - Quarterly: All accepted risks - Annually: Complete re-assessment

Triggers for Unscheduled Review: - New threats or vulnerabilities - Change in business environment - Security incidents - Audit findings

8.4 4. References

8.4.1 Internal Documents

- `0060_ISMS_Risk_Management_Methodology.md` - Risk Management Methodology
- `0080_ISMS_Risk_Register_Template.md` - Risk Register
- `0090_ISMS_Risk_Treatment_Plan_RTP_Template.md` - Risk Treatment Plan

8.4.2 External Standards

- **ISO/IEC 27001:2022** - Clause 6.1.2: Information security risk assessment
- **ISO/IEC 27005:2022** - Information security risk management

---

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

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

ewpage

Chapter 9

Risk Register (Template)

Document ID: 0080
Document Type: ISMS Register/Template
Standard Reference: ISO/IEC 27001:2022 Clause 6.1.2
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Confidential
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

9.1 1. Purpose and Instructions

9.1.1 1.1 Purpose

The risk register documents all identified information security risks within the ISMS scope of **AdminSend GmbH**. It serves as: - Central overview of all risks - Basis for risk treatment decisions - Evidence for audits and compliance - Basis for risk reporting

9.1.2 1.2 Usage Instructions

Each row describes a risk: - Unique risk ID (R-001, R-002, etc.) - Affected asset or process - Threat and vulnerability - Risk assessment (likelihood, impact, score) - Risk owner - Treatment strategy - Link to controls and measures

Maintenance: - Quarterly review by ISMS Manager - Event-driven updates for new risks - Archiving of treated/closed risks

Links: - Controls: See `0100_ISMS_Statement_of_Applicability_SoA_Template.md` - Measures: See `0090_ISMS_Risk_Treatment_Plan_RTP_Template.md` - Evidence: See `0700_Appendix_Evidence_Register.m`

9.2 2. Risk Register Table

9.2.1 2.1 Active Risks

Risk ID	Asset/Process	Threat	Vulnerability	Impact (1-5)	Likelihood (1-5)	Score	Risk Level	Risk Owner	Treatment	Measure/Status	Target Date	Remarks
R-001	{{ net-box.device }}	Hardware failure	No redundancy	4	3	12	Medium	Anna Schmidt	Mitigate	Procure redundant switch	Open	2026-06-30	Budget approved
R-002	Customer data (GDPR)	Ransomware	Insufficient backups	5	4	20	High	Thomas Weber	Mitigate	Implement immutable backups	In Progress	2026-03-31	See M-002
R-003	Email system	Phishing	Missing MFA	4	4	16	High	Anna Schmidt	Mitigate	MFA for all users	In Progress	2026-02-28	80% complete
R-004	Development environment	Secrets in code	No secret scanning	3	3	9	Medium	Dev Lead	Mitigate	Secret scanning tool	Planned	2026-04-30	Tool evaluation ongoing
R-005	Remote access	Unauthorized access	Weak VPN configuration	4	2	8	Medium	IT Operations	Mitigate	VPN hardening	Open	2026-05-31	-

[TODO: Add additional risks based on risk analysis]

9.2.2 2.2 Accepted Risks

Risk ID	Asset/Process	Threat	Vulnerability	Score	Risk Level	Risk Owner	Accepted By	Acceptance Date	Valid Until	Justification	Review Status
R-010	Legacy system XYZ	Unpatched vulnerabilities	System being phased out	9	Medium	Anna Schmidt	Thomas Weber	2026-01-15	2026-06-30	System will be decommissioned on 30.06.2026	Active

Risk ID	Asset/Process	Threat	Vulnerability	Score	Risk Level	Risk Owner	Accepted By	Acceptance Date	Valid Until	Justification	Review Status
R-011	Test environment	Missing encryption	No production data	6	Low	Dev Lead	Thomas Weber	2026-01-20	2027-01-20	Test environment contains only synthetic data	Active

[TODO: Document accepted risks]

9.2.3 2.3 Closed/Treated Risks (Archive)

Risk ID	Asset/Process	Threat	Score	Treatment	Closure Date	Remarks
R-020	Web server	Unpatched vulnerability CVE-2025-1234	15	Mitigate	2026-01-10	Patch installed, vulnerability scan confirmed
R-021	Firewall	Misconfiguration	12	Mitigate	2026-01-15	Configuration corrected, audit performed

[TODO: Archive closed risks]

9.3 3. Risk Categories and Classification

9.3.1 3.1 Risk Categories

Technical Risks: - Infrastructure (hardware, network, cloud) - Applications (software, development) - Data (databases, backups, encryption)

Organizational Risks: - Processes (missing or insufficient processes) - Personnel (lack of competence, insider threat) - Suppliers (third-party risks)

Physical Risks: - Locations (access, environmental risks) - Hardware (theft, destruction)

Compliance Risks: - Regulatory requirements (GDPR, NIS2, etc.) - Contractual obligations

9.3.2 3.2 Threat Sources

External Threats: - Cybercriminals (ransomware, phishing, DDoS) - Hacktivists - Nation-states (APT) - Competitors

Internal Threats: - Insiders (malicious or negligent) - Human errors - Process failures

Environmental Threats: - Natural disasters (fire, water, storm) - Infrastructure failures (power, cooling)

9.4 4. Risk Assessment

9.4.1 4.1 Assessment Scales

Likelihood:

Level	Description	Frequency
1	Very unlikely	$<$ 1 in 10 years
2	Unlikely	1 in 5-10 years
3	Possible	1 in 1-5 years
4	Likely	1-5 times per year
5	Very likely	$>$ 5 times per year

Impact:

Level	Description	Financial	Reputation	Compliance
1	Negligible	$<$ €10k	None	None
2	Low	€10-50k	Local	Minor violations
3	Medium	€50-250k	Regional	Reportable
4	High	€250k-1M	National	Fines
5	Very high	$>$ €1M	International	Business prohibition

Risk Score: Likelihood × Impact

Risk Levels:

Score	Risk Level	Color	Treatment
1-2	Very low	Green	Monitoring
3-6	Low	Green	Monitoring
7-12	Medium	Yellow	Treatment recommended
13-20	High	Orange	Treatment required
21-25	Very high	Red	Immediate treatment

9.4.2 4.2 Treatment Strategies

Avoid: - Discontinue activity causing the risk - Example: Avoid risky technology

Mitigate: - Measures to reduce likelihood or impact - Example: Implement controls (firewall, MFA, encryption)

Transfer: - Transfer risk to third parties - Example: Cyber insurance, outsourcing with SLA

Accept: - Conscious decision to bear the risk - Only for low/medium risks after approval - See `0070_ISMS_Risk_Acceptance_Criteria.md`

9.5 5. Risk Owners and Responsibilities

9.5.1 5.1 Risk Owner

Responsibilities: - Responsible for risk treatment - Decision on treatment strategy - Monitoring of measure implementation - Regular risk assessment

Typical Risk Owners: - **CISO:** Cross-cutting security risks - **CIO:** IT infrastructure risks - **Asset Owner:** Asset-specific risks - **Process Owner:** Process-specific risks

9.5.2 5.2 RACI Matrix: Risk Management

Activity	CISO	ISMS Manager	Risk Owner	IT Operations
Identify risk	A	R	C	C
Assess risk	A	R	C	C
Plan treatment	A	C	R	C
Implement measures	A	C	R	R
Monitor risk	A	R	C	C
Maintain risk register	A	R	C	I

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

9.6 6. Risk Reporting

9.6.1 6.1 Regular Reporting

Quarterly: - Risk dashboard to information security committee - Number of risks by level - Trend of risk scores - Status of risk treatment

Annually: - Complete risk report in management review - See `0140_ISMS_Management_Review_Template.md`

9.6.2 6.2 Ad-hoc Reporting

Triggers: - New critical risks (score 13) - Significant change in existing risks - Security incidents with risk relevance

Escalation: - High risks: Immediate notification to CISO and CIO - Very high risks: Immediate notification to management

9.7 7. Risk Review and Update

9.7.1 7.1 Regular Review

Quarterly: - Review of all active risks - Update of assessments - Status update of measures - Review of accepted risks

Annually: - Complete risk analysis - Identification of new risks - Archiving of closed risks

9.7.2 7.2 Triggers for Unscheduled Review

External Triggers: - New threats (zero-day exploits, new malware) - New vulnerabilities (CVE publications) - Change in threat landscape - New compliance requirements

Internal Triggers: - Security incidents - Audit findings - Significant organizational changes - New assets or processes

9.8 8. Links and References

9.8.1 8.1 Links to Other ISMS Documents

Risk Treatment Plan (RTP): - Each risk with treatment "Mitigate" has measures in RTP - See `0090_ISMS_Risk_Treatment_Plan_RTP_Template.md`

Statement of Applicability (SoA): - Controls in SoA are selected based on risk analysis - See `0100_ISMS_Statement_of_Applicability_SoA_Template.md`

Asset Inventory: - Risks are linked to assets - See `0720_Appendix_Asset_and_System_Inventory_Template.md`

Incident Reports: - Incidents can identify new risks - See `0400_Policy_Incident_Management.md`

9.8.2 8.2 Internal Documents

- `0060_ISMS_Risk_Management_Methodology.md` - Risk Management Methodology
- `0070_ISMS_Risk_Acceptance_Criteria.md` - Risk Acceptance Criteria
- `0090_ISMS_Risk_Treatment_Plan_RTP_Template.md` - Risk Treatment Plan
- `0100_ISMS_Statement_of_Applicability_SoA_Template.md` - SoA

9.8.3 8.3 External Standards

- **ISO/IEC 27001:2022** - Clause 6.1.2: Information security risk assessment
- **ISO/IEC 27005:2022** - Information security risk management
- **NIST SP 800-30** - Guide for Conducting Risk Assessments

9.9 Change History

Version	Date	Author	Description	Approved By
1.0	{{ meta.document.date }}	Thomas Weber	Initial version	{{ meta.management.ceo }}

Approved by:
Thomas Weber, CISO
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (Quarterly)

ewpage

Chapter 10

Risk Treatment Plan (RTP) – Template

Document ID: 0090
Document Type: ISMS Plan/Template
Standard Reference: ISO/IEC 27001:2022 Clause 6.1.3
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Confidential
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

10.1 1. Purpose and Scope

10.1.1 1.1 Purpose

The Risk Treatment Plan (RTP) of **AdminSend GmbH** documents all planned measures for treating identified information security risks. It serves as: - Action plan for risk treatment - Tracking tool for measure implementation - Evidence for audits and compliance - Basis for resource planning and budgeting

10.1.2 1.2 Scope

This plan encompasses all measures for treating risks within the ISMS scope (see `0020_ISMS_Scope.md`) that are treated with the "Mitigate" or "Transfer" strategy.

Excluded: - Accepted risks (see `0080_ISMS_Risk_Register_Template.md`) - Avoided risks (activity discontinued)

10.2 2. Risk Treatment Plan Table

10.2.1 2.1 Active Measures

Measure ID	Risk ID	Measure	Control Reference (Annex A)	Owner	Priority	Effort (PD)	Budget	Target Date	Status	Progress	Remarks
M-001	R-001	Procure redundant core switch	A.8.6 (Capacity management)	Anna Schmidt	High	20	€50,000	2026-06-30	Planned	0%	Budget approved, tender in progress
M-002	R-002	Implement immutable backups	A.8.13 (Information backup)	IT Operations	Very High	40	€30,000	2026-03-31	In Progress	60%	Pilot phase completed
M-003	R-003	Roll out MFA for all users	A.5.17 (Authentication information)	IAM Team	Very High	30	€15,000	2026-02-28	In Progress	80%	200 of 250 users migrated
M-004	R-004	Implement secret scanning tool	A.8.24 (Use of cryptography)	Dev Lead	Medium	15	€10,000	2026-04-30	Planned	10%	Tool evaluation: GitGuardian vs. Gitleaks
M-005	R-005	Perform VPN hardening	A.5.14 (Information transfer)	IT Operations	Medium	10	€5,000	2026-05-31	Planned	0%	Create hardening guide

[TODO: Add additional measures based on risk register]

10.2.2 2.2 Completed Measures (Archive)

Measure ID	Risk ID	Measure	Owner	Completion Date	Result	Evidence
M-010	R-020	Install patch CVE-2025-1234	IT Operations	2026-01-10	Successful	Vulnerability Scan Report

Measure ID	Risk ID	Measure	Owner	Completion Date	Result	Evidence
M-011	R-021	Correct firewall configuration	IT Operations	2026-01-15	Successful	Firewall Audit Report

[TODO: Archive completed measures]

10.3 3. Measure Prioritization

10.3.1 3.1 Prioritization Criteria

Priority Levels:

Priority	Risk Level	Compliance	Effort	Timeframe
Very High	Very High / High	Critical	Any	Immediate - 3 months
High	High / Medium	Important	Low-Medium	3-6 months
Medium	Medium	Normal	Medium	6-12 months
Low	Low	Optional	High	> 12 months

Prioritization Formula:

```
Priority = (Risk Score × 2) + Compliance Factor - Effort Factor

Compliance Factor:
- Critical (GDPR, NIS2): +10
- Important (ISO 27001): +5
- Normal: +0

Effort Factor:
- Low (< 10 PD): -0
- Medium (10-40 PD): -5
- High (> 40 PD): -10
```

10.3.2 3.2 Quick Wins

Quick Wins are measures with high benefit and low effort:

Measure ID	Measure	Risk Reduction	Effort	ROI
M-003	MFA rollout	High	Medium	High
M-005	VPN hardening	Medium	Low	Very High

Recommendation: Quick wins should be prioritized to achieve rapid security improvements.

10.4 4. Measure Details

10.4.1 4.1 Measure Description

The following details should be documented for each measure:

Measure M-002: Implement Immutable Backups

Description: Implementation of immutable backups to protect against ransomware. Backups are stored in Write-Once-Read-Many (WORM) format and cannot be deleted or modified.

Objective: - Protection against ransomware attacks on backups - Ensure recoverability in case of data loss - Compliance with GDPR Art. 32 (Security of processing)

Scope: - All production systems - Critical databases - Customer data (GDPR-relevant)

Implementation Steps: 1. Evaluate backup solution (Veeam, Commvault, AWS S3 Object Lock) 2. Pilot phase with non-critical systems (Completed) 3. Rollout to production systems (In Progress) 4. Perform restore tests 5. Documentation and training

Resources: - Owner: IT Operations - Team: 2 Backup Administrators - Effort: 40 person-days - Budget: €30,000 (licenses + hardware)

Dependencies: - No critical dependencies

Implementation Risks: - Increased storage requirements (Mitigation: Additional storage procured) - Longer backup times (Mitigation: Backup window adjusted)

Success Criteria: - All critical systems have immutable backups - Restore tests successful (RTO/RPO met) - No ransomware can delete backups

Evidence: - Backup configuration documentation - Restore test protocols - Compliance report

10.5 5. Control Mapping (Annex A)

10.5.1 5.1 Linkage to Annex A Controls

Each measure should be linked to relevant Annex A controls:

Measure ID	Annex A Control	Control Name	Implementation Status
M-001	A.8.6	Capacity management	Planned
M-002	A.8.13	Information backup	In Progress
M-003	A.5.17	Authentication information	In Progress
M-004	A.8.24	Use of cryptography	Planned
M-005	A.5.14	Information transfer	Planned

Complete Control Mapping: - See `0100_ISMS_Statement_of_Applicability_SoA_Template.md` - See `0710_Appendix_AnnexA_Mapping_Template.md`

10.5.2 5.2 Control Implementation Status

Status Definitions:

Status	Description	Criteria
Not Implemented	Control is not in place	0% implementation
Planned	Control is planned but not yet started	Measure in RTP
In Progress	Control is being implemented	1-99% implementation
Implemented	Control is fully implemented	100% implementation, evidence available
Effective	Control is implemented and demonstrably effective	Implemented + effectiveness evidence

10.6 6. Resource Planning and Budgeting

10.6.1 6.1 Resource Overview

Personnel Resources:

Team/Role	Available Capacity (PD/month)	Planned Utilization	Availability
IT Operations	40	30	75%
Security Team	20	18	90%
IAM Team	15	12	80%
Dev Team	10	5	50%

Financial Resources:

Quarter	Budget	Planned Expenses	Available
Q1 2026	€50,000	€45,000	€5,000
Q2 2026	€50,000	€55,000	-€5,000 (Overrun)
Q3 2026	€50,000	€30,000	€20,000
Q4 2026	€50,000	€20,000	€30,000

Budget Request: - Q2 2026: Additional €5,000 for M-001 (Redundant switch)

10.6.2 6.2 Capacity Planning

Bottlenecks: - Security Team: 90% utilized (critical) - IAM Team: 80% utilized (high)

Actions: - Prioritization of critical measures - External support for M-004 (Secret scanning) - Postponement of non-critical measures to Q3/Q4

10.7 7. Dependencies and Implementation Risks

10.7.1 7.1 Dependencies Between Measures

```
M-002 (Immutable Backups)
  ↓ (requires)
```

```
M-001 (Redundant Switch)
  ↓ (enables)
M-005 (VPN Hardening)
```

Critical Path: - M-002 must be completed before M-001 - M-001 is prerequisite for M-005

10.7.2 7.2 Implementation Risks

Risk	Likelihood	Impact	Mitigation
Resource bottlenecks	High	Medium	External support, prioritization
Budget overrun	Medium	Medium	Regular budget monitoring, approval process
Technical complexity	Medium	High	Pilot phases, external expertise
Resistance to change	Low	Medium	Change management, awareness

10.7.3 7.3 Change Management

Communication: - Regular updates to stakeholders - Awareness campaigns for affected users - Training for new controls

Rollback Planning: - Create rollback plan for each measure - Pilot phases before production rollout - Backup before critical changes

10.8 8. Tracking and Reporting

10.8.1 8.1 Measure Tracking

Tracking Frequency: - Weekly: Status update for critical measures - Monthly: Complete RTP review - Quarterly: Reporting to information security committee

Tracking Metrics: - Number of open measures - Number of overdue measures - Average implementation duration - Budget utilization

10.8.2 8.2 Reporting

Monthly Reporting: - Status of all active measures - Progress (% completion) - Risks and issues - Budget status

Quarterly Reporting: - Summary for information security committee - Trend analysis - Prioritization recommendations

Escalation: - Overdue measures (> 2 weeks): Escalation to CISO - Critical delays: Escalation to management

10.9 9. Effectiveness Verification

10.9.1 9.1 Evidence of Effectiveness

Effectiveness must be demonstrated for each implemented measure:

Evidence Methods: - **Technical Tests:** Vulnerability scans, penetration tests, configuration audits - **Process Audits:** Internal audits, compliance checks - **Monitoring:** SIEM alerts, log analysis, KPI tracking - **Documentation:** Policies, procedures, training records

Example M-002 (Immutable Backups): - Evidence: Restore test protocol - Frequency: Quarterly - Criteria: RTO/RPO met, backups not modifiable

10.9.2 9.2 Evidence Register

Linkage: - See `0700_Appendix_Evidence_Register.md` - Each measure has linked evidence

10.10 10. Roles and Responsibilities

10.10.1 10.1 RACI Matrix: Risk Treatment

Activity	CISO	ISMS Manager	Measure Owner	IT Operations	Budget Owner
Create RTP	A	R	C	C	I
Prioritize measures	A	R	C	C	C
Implement measures	A	C	R	R	I
Approve budget	C	I	I	I	A
Track progress	A	R	C	I	I
Verify effectiveness	A	R	C	R	I
RTP review	A	R	C	C	I

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

10.11 11. References

10.11.1 11.1 Internal Documents

- `0060_ISMS_Risk_Management_Methodology.md` - Risk Management Methodology
- `0070_ISMS_Risk_Acceptance_Criteria.md` - Risk Acceptance Criteria
- `0080_ISMS_Risk_Register_Template.md` - Risk Register
- `0100_ISMS_Statement_of_Applicability_SoA_Template.md` - SoA
- `0360_Policy_Change_and_Release_Management.md` - Change Management
- `0700_Appendix_Evidence_Register.md` - Evidence Register

10.11.2 11.2 External Standards

- **ISO/IEC 27001:2022** - Clause 6.1.3: Information security risk treatment
- **ISO/IEC 27002:2022** - Information security controls
- **ISO/IEC 27005:2022** - Information security risk management

---

10.12 Change History

Version	Date	Author	Description	Approved By
1.0	{{ meta.document.date }}	Thomas Weber	Initial version	{{ meta.management.ceo }}

Approved by:
Thomas Weber, CISO
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (Monthly)

ewpage

Chapter 11

Statement of Applicability (SoA) – Template

Document ID: 0100
Document Type: ISMS Evidence/Template
Standard Reference: ISO/IEC 27001:2022 Clause 6.1.3 d), Annex A
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Confidential
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

11.1 1. Purpose and Scope

11.1.1 1.1 Purpose

The Statement of Applicability (SoA) of **AdminSend GmbH** documents: - Which Annex A controls are applicable to the ISMS - Justification for selection or exclusion of controls - Implementation status of each control - Linkage to policies, guidelines, and evidence

The SoA is a **mandatory document** according to ISO/IEC 27001:2022 and serves as: - Evidence of systematic control selection - Basis for audits and certifications - Overview of implementation status - Link between risk analysis and controls

11.1.2 1.2 Scope

This SoA applies to the entire ISMS scope (see `0020_ISMS_Scope.md`): - All locations: {{ netbox.site.name }} and others - All IT systems and infrastructure - All business processes in scope - All information assets

11.1.3 1.3 Annex A Controls (ISO 27001:2022)

ISO/IEC 27001:2022 Annex A contains 93 controls in 4 categories: - **Organisational Controls (5.x):** 37 controls - **People Controls (6.x):** 8 controls - **Physical Controls (7.x):** 14 controls - **Technological Controls (8.x):** 34 controls

Amendment 1:2024: - Considers changes from Amendment 1:2024 - See `0710_Appendix_AnnexA_Mapping_Templ` for complete list

11.2 2. Control Selection Criteria

11.2.1 2.1 Selection Process

Controls are selected based on the following criteria:

1. Risk Analysis: - Controls to treat identified risks - See `0080_ISMS_Risk_Register_Template.md`

2. Compliance Requirements: - Legal requirements (GDPR, NIS2, etc.) - Contractual obligations - Industry standards

3. Best Practices: - Industry-standard security measures - Recommendations from security experts

4. Organizational Requirements: - Business requirements - Stakeholder expectations

11.2.2 2.2 Exclusion Criteria

Controls may be excluded when: - Not relevant to the ISMS scope - Risk is accepted and control not required - Alternative controls provide equivalent protection - Technically or organizationally not feasible (with justification)

Important: Exclusions must be justified and must not impair the organization's ability to meet security requirements.

11.3 3. Statement of Applicability (SoA) - Overview

11.3.1 3.1 Implementation Status

Status	Number of Controls	Percentage
Implemented	[TODO]	[TODO]%
In Progress	[TODO]	[TODO]%
Planned	[TODO]	[TODO]%
Not Applicable	[TODO]	[TODO]%
Total	**93**	**100%**

Target: At least 80% of applicable controls implemented by [TODO: Date]

11.3.2 3.2 Implementation by Category

Category	Applicable	Implemented	In Progress	Planned	Not Applicable
Organisational (5.x)	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
People (6.x)	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
Physical (7.x)	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]
Technological (8.x)	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

11.4 4. SoA Table: Organisational Controls (5.x)

11.4.1 4.1 Policies for Information Security (5.1-5.10)

Control ID	Control Name	Applicable	Justification (if No)	Implementation Status	Implementation Description	Policy/Procedure Document	Evidence	Owner	Remarks
A.5.1	Policies for information security	Yes	-	Implemented	ISMS policy and topic-specific policies	0010_ISMS_Policy_Information_Security_Policy	Policy documents	Thomas Weber	Annual review
A.5.2	Information security roles and responsibilities	Yes	-	Implemented	ISMS governance structure defined	0040_ISMS_Governance_Roles_and_Responsibilities	RACI matrices	Thomas Weber	
A.5.3	Segregation of duties	Yes	-	In Progress	Role separation in critical processes	0220_Policy_Access_Control_and_Identity_Management	IAM configuration	Anna Schmidt	70% implemented
A.5.4	Management responsibilities	Yes	-	Implemented	Management commitment documented	0010_ISMS_Policy_Information_Security_Policy	Management review	{{ meta.management.ceo }}	
A.5.5	Contact with authorities	Yes	-	Implemented	Contacts with authorities documented	0050_Contacts_and_Escalation.md (BCM)	Contact list	Thomas Weber	

Control ID	Control Name	Applicable	Justification (If No)	Implementation Status	Implementation Description	Policy/Procedure Document	Evidence	Owner	Remarks
A.5.6	Contact with special interest groups	Yes	-	Implemented	Membership in CERT, industry associations	[TODO: Document]	Membership evidence	Thomas Weber	-
A.5.7	Threat intelligence	Yes	-	In Progress	Threat intelligence feeds subscribed	0060_ISMS_Risk_Management_Methodology	Threat feed configuration	Security Team	MITRE ATT&CK, CERT
A.5.8	Information security in project management	Yes	-	Planned	Security in project lifecycle	0680_Policy_Security_in_Projects.md	Project checklists	PMO	Roll-out Q2 2026
A.5.9	Inventory of information and other associated assets	Yes	-	In Progress	Asset inventory maintained	0720_Appendix_Asset_and_System_Inventory.md	CMDB, NetBox	IT Operations	80% captured
A.5.10	Acceptable use of information and other associated assets	Yes	-	Implemented	Acceptable use policy	0200_Policy_Acceptable_Use_of_IT.md	Signed policies	HR	-

[TODO: Create complete table for all 37 Organisational Controls]

11.5 5. SoA Table: People Controls (6.x)

Control ID	Control Name	Applicable	Justification (if No)	Implementation Status	Implementation Description	Policy/Procedure Reference	Evidence	Owner	Remarks
A.6.1	Screening	Yes	-	Implemented	Background checks for critical roles	0520_Policy_HR_Security.md	HR process	HR	-
A.6.2	Terms and conditions of employment	Yes	-	Implemented	Security clauses in employment contracts	0530_Guideline_Employment_Onboarding_Role_Cha	Employment contracts	HR	-
A.6.3	Information security awareness, education and training	Yes	-	In Progress	Security awareness program	0120_ISMS_Training_Awareness_and_Comp	Training records	Thomas Weber	Q4 awareness training
A.6.4	Disciplinary process	Yes	-	Implemented	Disciplinary procedures for violations	0520_Policy_HR_Security.md	HR process	HR	-
A.6.5	Responsibilities after termination or change of employment	Yes	-	Implemented	Offboarding process	0530_Guideline_Onboarding_Role_Cha	Offboarding checklist	HR	-
A.6.6	Confidentiality or non-disclosure agreements	Yes	-	Implemented	NDAs for employees and third parties	0520_Policy_HR_Security.md	Signed NDAs	HR	-
A.6.7	Remote working	Yes	-	Implemented	Remote work policy	0500_Policy_Mobile_Device_and_Remote_	Remote work guidelines	Anna Schmidt	-

Control ID	Control Name	Applicable	Justification (if No)	Implementation Status	Implementation Description	Policy/Guideline Reference	Evidence	Owner	Remarks
A.6.8	Information security event reporting	Yes	-	Implemented	Incident reporting process	0400_Policy_Incident_Management.md	Incident reports	Weber	

11.6 6. SoA Table: Physical Controls (7.x)

Control ID	Control Name	Applicable	Justification (if No)	Implementation Status	Implementation Description	Policy/Guideline Reference	Evidence	Owner	Remarks
A.7.1	Physical security perimeters	Yes	-	Implemented	Access controls at {{ netbox.site.name }} location	0480_Policy_Physical_Security.md	Access logs	Facility Mgmt	
A.7.2	Physical entry	Yes	-	Implemented	Access cards, visitor management	0490_Guideline_Visitor_Access_Visitors_and_Eq	Visitor lists	Facility Mgmt	
A.7.3	Securing offices, rooms and facilities	Yes	-	Implemented	Server room secured, alarm systems	0480_Policy_Physical_Security.md	Security concept	Facility Mgmt	
A.7.4	Physical security monitoring	Yes	-	Implemented	Video surveillance, alarm systems	0480_Policy_Physical_Security.md	Monitoring logs	Facility Mgmt	GDPR-compliant
A.7.5	Protecting against physical and environmental threats	Yes	-	Implemented	Fire protection, climate control, UPS	0480_Policy_Physical_Security.md	Maintenance logs	Facility Mgmt	
A.7.6	Working in secure areas	Yes	-	Implemented	Clean desk policy, secure areas	0480_Policy_Physical_Security.md	Audit reports	Facility Mgmt	

Control ID	Control Name	Applicable	Justification (If No)	Implementation Status	Implementation Policy/Procedure	Evidence	Owner	Remarks
A.7.7	Clear desk and clear screen	Yes	-	In Progress	Clear desk policy communicated	0480_Policy_Physical_Security.md	Awareness campaign	Thal Weber	Rollout ongoing
A.7.8	Equipment siting and protection	Yes	-	Implemented	Equipment protection, theft prevention	0490_Guideline_Access_Visitors_and_Eq	Asset register	IT Operations	
A.7.9	Security of assets off-premises	Yes	-	Implemented	Laptop encryption, mobile device policy	0500_Policy_Mobile_Device_and_Remote_	MDM configuration	IT Operations	
A.7.10	Storage media	Yes	-	Implemented	Secure handling of storage media	0280_Policy_Data_Classification_and_I	Handling procedures	IT Operations	
A.7.11	Supporting utilities	Yes	-	Implemented	UPS, emergency power, climate control	0480_Policy_Physical_Security.md	Maintenance contracts	Facility Mgmt	
A.7.12	Cabling security	Yes	-	Implemented	Structured cabling, protection	0480_Policy_Physical_Security.md	Cabling plan	IT Operations	
A.7.13	Equipment maintenance	Yes	-	Implemented	Maintenance contracts, maintenance logs	0480_Policy_Physical_Security.md	Maintenance evidence	IT Operations	
A.7.14	Secure disposal or re-use of equipment	Yes	-	Implemented	Secure disposal, data wiping	0580_Policy_Retention_and_Deletion.md	Disposal evidence	IT Operations	GDPR compliant

11.7 7. SoA Table: Technological Controls (8.x)

Control ID	Control Name	Applicable	Justification (if No)	Implementation Status	Implementation Description	Policy/Procedure Document	Evidence	Owner	Remarks
A.8.1	User endpoint devices	Yes	-	Implemented	Endpoint protection (EDR/AV)	0620_Policy_Endpoint_Security.md	EDR configuration	IT Operations	-
A.8.2	Privileged access rights	Yes	-	In Progress	PAM solution being implemented	0220_Policy_Access_Control_and_Identity_Management.md	PAM system	IT Operations	Rollout Q2 2026
A.8.3	Information access restriction	Yes	-	Implemented	Access controls, RBAC	0220_Policy_Access_Control_and_Identity_Management.md	IAM configuration	IT Operations	-
A.8.4	Access to source code	Yes	-	Implemented	Git access controls, code review	0360_Policy_Secure_Development.md	Git permissions	Dev Lead	-
A.8.5	Secure authentication	Yes	-	In Progress	MFA rollout	0240_Policy_Authentication_and_Password_Management.md	MFA configuration	IT Operations	80% complete
A.8.6	Capacity management	Yes	-	In Progress	Monitoring, capacity planning	[TODO: Policy]	Monitoring dashboards	IT Operations	-
A.8.7	Protection against malware	Yes	-	Implemented	Antivirus, EDR, email filtering	0620_Policy_Endpoint_Security.md	AV/EDR reports	IT Operations	-
A.8.8	Management of technical vulnerabilities	Yes	-	In Progress	Vulnerability management process	0340_Policy_Vulnerability_and_Patch_Management.md	Scan reports	IT Operations	-

[TODO: Create complete table for all 34 Technological Controls]

11.8 8. Non-Applicable Controls

11.8.1 8.1 Excluded Controls with Justification

Control ID	Control Name	Justification for Exclusion	Alternative Measures	Approved By
[TODO]	[TODO]	[TODO: Not in scope, risk accepted, etc.]	[TODO: If available]	Thomas Weber

Important: Exclusions must be documented and approved. They must not impair the ability to meet security requirements.

11.9 9. Linkages and References

11.9.1 9.1 Linkage to ISMS Documents

Risk Analysis: - Controls are selected based on risk analysis - See `0080_ISMS_Risk_Register_Template.md`

Risk Treatment Plan: - Implementation of controls is tracked in RTP - See `0090_ISMS_Risk_Treatment_Plan_R`

Policies and Guidelines: - Each control is linked to policy/guideline - See ISMS document structure (0200-0690)

Evidence: - Evidence for control implementation - See `0700_Appendix_Evidence_Register.md`

11.9.2 9.2 Complete Annex A Mapping

For a complete overview of all 93 Annex A controls see: - `0710_Appendix_AnnexA_Mapping_Template.md`

11.10 10. Review and Update

11.10.1 10.1 Regular Review

Annually: - Complete SoA review - Review of applicability of all controls - Update of implementation status

Quarterly: - Review of implementation status - Tracking of measures from RTP

11.10.2 10.2 Triggers for Unscheduled Review

Changes to ISMS Scope: - New locations, systems, processes - See `0020_ISMS_Scope.md`

New Risks: - Significant changes in risk register - See `0080_ISMS_Risk_Register_Template.md`

New Compliance Requirements: - New laws, regulations, contracts

Audit Findings: - Internal or external audit findings

11.11 11. References

11.11.1 11.1 Internal Documents

- `0020_ISMS_Scope.md` - ISMS Scope
- `0060_ISMS_Risk_Management_Methodology.md` - Risk Management
- `0080_ISMS_Risk_Register_Template.md` - Risk Register
- `0090_ISMS_Risk_Treatment_Plan_RTP_Template.md` - Risk Treatment Plan

- `0710_Appendix_AnnexA_Mapping_Template.md` - Complete Annex A Mapping
- All Policies (0200-0680) and Guidelines (0210-0690)

11.11.2 11.2 External Standards

- **ISO/IEC 27001:2022** - Clause 6.1.3 d): Statement of Applicability
- **ISO/IEC 27001:2022** - Annex A: Information security controls
- **ISO/IEC 27001:2022/Amd 1:2024** - Amendment 1 (Annex A updates)
- **ISO/IEC 27002:2022** - Information security controls (detailed guidance)

11.12 Change History

Version	Date	Author	Description	Approved By
1.0	{{ meta.document.date }}	Thomas Weber	Initial version	{{ meta.management.ceo }}

Approved by:
Thomas Weber, CISO
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (Annually)

ewpage

Chapter 12

Information Security Objectives and Metrics

Document ID: 0110
Document Type: ISMS Foundation Document
Standard Reference: ISO/IEC 27001:2022 Clause 6.2
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

12.1 1. Information Security Objectives

12.1.1 1.1 Strategic Objectives

AdminSend GmbH defines the following strategic information security objectives:

Objective ID	Objective	Description	KPI/Metric	Target Value	Measurement Method	Owner	Frequency	Status
O-001	Ensure compliance	Compliance with all legal and contractual requirements	Number of compliance violations	0	Audit reports, incident reports	Thomas Weber	Quarterly	Active

Objective ID	Objective	Description	KPI/Metric	Target Value	Measurement Method	Owner	Frequency	Status
O-002	Minimize risks	Reduction of high and very high risks	Number of risks with score 13	< 5	Risk register	Thomas Weber	Quarterly	Active
O-003	Ensure availability	Ensure availability of critical systems	Uptime of critical systems	99.5%	Monitoring system	Anna Schmidt	Monthly	Active
O-004	Reduce incidents	Reduction of number of security incidents	Number of security incidents	< 10 per quarter	Incident management system	Thomas Weber	Quarterly	Active
O-005	Increase awareness	Increase security awareness	Training participation rate	100%	LMS, training records	Thomas Weber	Annually	Active
O-006	Patch compliance	Timely installation of critical patches	Average time to install patches (critical)	< 7 days	Vulnerability management system	IT Operations	Monthly	Active

[TODO: Add additional organization-specific objectives]

12.1.2 1.2 Operational Objectives

Objective ID	Objective	KPI/Metric	Target Value	Owner	Frequency
O-010	Complete MFA rollout	MFA activation rate	100%	IT Operations	Monthly
O-011	Vulnerability management	Average time to remediate high vulnerabilities	< 30 days	IT Operations	Monthly
O-012	Backup tests	Success rate of restore tests	100%	IT Operations	Quarterly
O-013	Phishing resilience	Phishing click rate in simulations	< 5%	Thomas Weber	Quarterly

12.2 2. Key Performance Indicators (KPIs)

12.2.1 2.1 Security KPIs

Risk Management: - Number of identified risks (by level) - Number of treated risks per quarter - Average risk remediation time - Number of accepted risks

Incident Management: - Number of security incidents (by severity) - Mean Time to Detect (MTTD) - Mean Time to Respond (MTTR) - Mean Time to Recover (MTTR)

Vulnerability Management: - Number of open vulnerabilities (by CVSS score) - Average time to install patches - Patch compliance rate

Access Management: - Number of privileged accounts - MFA activation rate - Recertification rate - Number of access violations

Awareness and Training: - Training participation rate - Phishing simulation results - Number of security incidents reported by employees

12.2.2 2.2 Compliance KPIs

- Number of audit findings (by severity)
- Average time to remediate findings
- Compliance rate with policies
- Number of compliance violations

12.2.3 2.3 Operational KPIs

- Uptime of critical systems
- Backup success rate
- Restore test success rate
- Number of change requests with security review

12.3 3. Measurement Methods and Data Sources

12.3.1 3.1 Data Sources

KPI	Data Source	Responsible	Automation
Number of incidents	Incident management system	Security Team	Yes
Risk scores	Risk register	ISMS Manager	Partial
Vulnerabilities	Vulnerability scanner	IT Operations	Yes
Uptime	Monitoring system	IT Operations	Yes
Training participation	LMS	HR / CISO	Yes
Patch compliance	Patch management system	IT Operations	Yes

12.3.2 3.2 Reporting Dashboards

Monthly Dashboard: - Incident statistics - Vulnerability status - Patch compliance - Uptime statistics

Quarterly Dashboard: - Risk overview - Audit findings status - Training statistics - Trend analyses

Annual Dashboard: - Objective achievement - Year-over-year comparison - Strategic recommendations

12.4 4. Measures for Objective Achievement

12.4.1 4.1 Linkage to Risk Treatment Plan

Each objective is linked to measures in the risk treatment plan: - See `0090_ISMS_Risk_Treatment_Plan_RTP_Templ`

Example: - **Objective O-002:** Minimize risks - **Measures:** M-001 (Redundant switch), M-002 (Immutable backups), M-003 (MFA rollout)

12.4.2 4.2 Continuous Improvement

Improvement Cycle: 1. Define objectives 2. Plan measures 3. Implement measures 4. Measure KPIs 5. Analyze results 6. Identify improvements 7. Adjust objectives

12.5 5. Review and Adjustment

12.5.1 5.1 Regular Review

Quarterly: - Review of KPI values - Analysis of deviations - Adjustment of measures

Annually: - Complete review of all objectives - Adjustment of target values - Definition of new objectives - As part of management review

12.5.2 5.2 Triggers for Unscheduled Review

- Significant changes to ISMS scope
- New compliance requirements
- Major security incidents
- Audit findings

12.6 6. References

12.6.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0080_ISMS_Risk_Register_Template.md` - Risk Register
- `0090_ISMS_Risk_Treatment_Plan_RTP_Template.md` - Risk Treatment Plan
- `0140_ISMS_Management_Review_Template.md` - Management Review

12.6.2 External Standards

- **ISO/IEC 27001:2022** - Clause 6.2: Information security objectives
- **ISO/IEC 27001:2022** - Clause 9.1: Monitoring, measurement, analysis and evaluation

---

Approved by:
Thomas Weber, CISO
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

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

ewpage

Chapter 13

Training, Awareness and Competence

Document ID: 0120
Document Type: ISMS Foundation Document
Standard Reference: ISO/IEC 27001:2022 Clauses 7.2, 7.3
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

13.1 1. Purpose and Objectives

13.1.1 1.1 Purpose

The training and awareness program of **AdminSend GmbH** ensures that: - All employees know their security responsibilities - Employees have the necessary competencies for their roles - Security awareness is continuously promoted - Compliance with ISO 27001:2022 and other requirements is ensured

13.1.2 1.2 Objectives

- **100% Training Participation:** All employees complete annual security awareness training
- **Phishing Resilience:** Click rate in phishing simulations $< 5\%$
- **Incident Reporting:** Increase security incidents reported by employees
- **Competence Building:** Specialized training for IT security roles

13.2 2. Target Groups

13.2.1 2.1 Target Group Overview

Target Group	Number	Training Need	Frequency	Responsible
All Employees	{{ meta.organization.employee_count }}	Security Awareness Basics	Annually	Thomas Weber
Admins/Privileged Users	[TODO]	Advanced Security, Privileged Access	Semi-annually	Thomas Weber
Developers/DevOps	[TODO]	Secure Coding, DevSecOps	Semi-annually	Thomas Weber
Management	[TODO]	Security Governance, Risk Management	Annually	Thomas Weber
HR	[TODO]	HR Security, Onboarding/Offboarding	Annually	Thomas Weber
Contractors/External	[TODO]	Security Basics, Compliance	At Onboarding	Thomas Weber

13.2.2 2.2 Role-Specific Requirements

IT Security Team: - ISO 27001 Lead Auditor Training - Incident Response Training - Threat Intelligence Training - Security Tool Training (SIEM, EDR, etc.)

IT Operations: - Secure Configuration Management - Patch Management - Backup and Recovery - Access Management

Developers: - OWASP Top 10 - Secure Coding Practices - Secret Management - Security Testing (SAST/DAST)

13.3 3. Training Plan

13.3.1 3.1 Mandatory Training

Training ID	Training	Target Group	Frequency	Duration	Content	Evidence	Owner	Status
T-001	Security Awareness Basics	All Employees	Annually	60 min	Phishing, passwords, clean desk, incident reporting	LMS certificate	Thomas Weber	Active

Training ID	Training	Target Group	Frequency	Duration	Content	Evidence	Owner	Status
T-002	GDPR Basics	All Employees	Annually	30 min	Data protection basics, data subject rights	LMS certificate	{{ meta.privacy.dpo }}	Active
T-003	Phishing Awareness	All Employees	Quarterly	15 min	Phishing detection, reporting	Simulation result	Thomas Weber	Active
T-004	Privileged Access Management	Admins	Semi-annually	90 min	PAM, least privilege, audit logging	LMS certificate	Thomas Weber	Active
T-005	Secure Coding	Developers	Semi-annually	120 min	OWASP Top 10, input validation, secrets	LMS certificate	Thomas Weber	Active
T-006	Incident Response	Security Team	Annually	180 min	IR process, forensics, communication	Workshop attendance	Thomas Weber	Active

[TODO: Add additional training]

13.3.2 3.2 Optional Training

Training	Target Group	Frequency	Provider	Cost
ISO 27001 Lead Auditor	Security Team	One-time	External	[TODO]
CISSP/CISM Certification	Security Team	One-time	External	[TODO]
Cloud Security (AWS/Azure)	IT Operations	As needed	External	[TODO]

Training	Target Group	Frequency	Provider	Cost
Penetration Testing	Security Team	As needed	External	[TODO]

13.3.3 3.3 Onboarding Training

New Employees: - Day 1: Security Awareness Basics (T-001) - Day 1: GDPR Basics (T-002) - Week 1: Role-specific training

External Contractors: - Before access: Security Basics - NDA signing - Access policies

13.4 4. Awareness Campaigns

13.4.1 4.1 Regular Campaigns

Monthly: - Security newsletter - Security tip of the month - Current threats and warnings

Quarterly: - Phishing simulations - Security quiz with prizes - Lunch & learn sessions

Annually: - Security Awareness Month (October) - Security Champions Program - Poster campaigns

13.4.2 4.2 Topic Focus

Quarter	Topic	Activities
Q1	Password Security	MFA rollout, password manager training
Q2	Phishing & Social Engineering	Phishing simulation, awareness videos
Q3	Mobile Security	BYOD policy, mobile device management
Q4	Incident Response	Incident reporting, lessons learned

13.4.3 4.3 Communication Channels

- **Email:** Security newsletter, alerts
- **Intranet:** Security portal, policies, FAQs
- **Posters:** Offices, break rooms
- **Teams/Slack:** Security channel
- **Workshops:** Lunch & learn, hands-on training

13.5 5. Phishing Simulations

13.5.1 5.1 Simulation Program

Frequency: Quarterly

Process: 1. Plan simulation (topic, target group) 2. Send phishing email 3. Measure click rate 4. Immediate feedback for clickers 5. Follow-up training for risk groups 6. Analyze and report results

Target Values: - Click rate < 5% - Reporting rate > 50%

Tools: - [TODO: KnowBe4, Cofense, etc.]

13.5.2 5.2 Escalation for High Click Rate

Click rate > 10%: - Additional awareness campaign - Mandatory follow-up training - Root cause analysis

Click rate > 20%: - Escalation to management - Intensified training measures - Review of awareness program

13.6 6. Effectiveness Verification

13.6.1 6.1 Measurement Methods

Quantitative Metrics: - Training participation rate - Phishing click rate - Quiz results - Number of incidents reported by employees - Number of security violations

Qualitative Metrics: - Feedback surveys - Stakeholder interviews - Observations (clean desk, screen lock)

13.6.2 6.2 Success Criteria

Metric	Target Value	Current	Status
Training participation	100%	[TODO]%	[TODO]
Phishing click rate	< 5%	[TODO]%	[TODO]
Incident reports	> 20 per quarter	[TODO]	[TODO]
Quiz success rate	> 80%	[TODO]%	[TODO]

13.6.3 6.3 Continuous Improvement

Annual Review: - Analysis of training results - Feedback evaluation - Adjustment of training content - Identification of new topics

Lessons Learned: - From security incidents - From audit findings - From phishing simulations

13.7 7. Training Records

13.7.1 7.1 Documentation

Learning Management System (LMS): - Training participation - Certificates - Quiz results - Expiration dates

Manual Records: - Workshop attendance lists - External certificates - Conference attendance

13.7.2 7.2 Retention

Retention Period: 10 years

Access: - HR: All records - CISO: All records - Managers: Records of their team - Employees: Own records

13.7.3 7.3 Audit Evidence

For audits, the following evidence is provided: - Training plan - Attendance lists - Certificates - Phishing simulation results - Awareness campaign documentation

13.8 8. Roles and Responsibilities

13.8.1 8.1 RACI Matrix: Training and Awareness

Activity	CISO	HR	Manager	Employee	External Trainer
Create training plan	R/A	C	C	I	I
Conduct training	R	C	I	I	R
Ensure participation	A	C	R	R	I
Document records	A	R	C	I	I
Verify effectiveness	R/A	C	C	I	I
Awareness campaigns	R/A	C	C	I	C
Phishing simulations	R/A	I	I	I	C

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

13.8.2 8.2 Security Champions

Program: - Volunteer employees from all departments - Multipliers for security awareness - Regular meetings and training - Recognition and incentives

Tasks: - Promote awareness in their teams - Answer security questions - Provide feedback to security team - Participate in security projects

13.9 9. Budget and Resources

13.9.1 9.1 Budget Planning

Category	Annual Budget	Remarks
LMS license	[TODO] €	E-learning platform
External training	[TODO] €	Certifications, conferences
Phishing simulation tool	[TODO] €	KnowBe4, Cofense, etc.
Awareness materials	[TODO] €	Posters, flyers, giveaways
External trainers	[TODO] €	Workshops, specialized training
Total	**[TODO] €**	

13.9.2 9.2 Time Resources

CISO/Security Team: - Training planning: 20 PD/year - Training delivery: 40 PD/year - Awareness campaigns: 30 PD/year - Phishing simulations: 20 PD/year

Employees: - Mandatory training: 2 hours/year - Optional training: As needed

13.10 10. References

13.10.1 10.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0040_ISMS_Governance_Roles_and_Responsibilities.md` - Governance
- `0110_ISMS_Security_Objectives_and_Metrics.md` - Security Objectives
- `0200_Policy_Acceptable_Use_of_IT.md` - Acceptable Use Policy
- `0520_Policy_HR_Security.md` - HR Security

13.10.2 10.2 External Standards

- **ISO/IEC 27001:2022** - Clause 7.2: Competence
- **ISO/IEC 27001:2022** - Clause 7.3: Awareness
- **ISO/IEC 27002:2022** - Control 6.3: Information security awareness, education and training

---

Approved by:
Thomas Weber, CISO
Date: {{ meta.document.approval_date }}

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

ewpage

Chapter 14

Internal Audit Program (Template)

Document ID: 0130
Document Type: ISMS Program/Template
Standard Reference: ISO/IEC 27001:2022 Clause 9.2
Owner: {{ meta.audit.manager }}
Version: 1.0
Status: Approved
Classification: Confidential
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

14.1 1. Purpose and Scope

14.1.1 1.1 Purpose

The internal audit program of **AdminSend GmbH** ensures that: - The ISMS complies with ISO 27001:2022 requirements - The ISMS is effectively implemented and maintained - Improvement opportunities are identified - Compliance with policies and guidelines is ensured

14.1.2 1.2 Scope

The audit program encompasses: - All areas within the ISMS scope (see `0020_ISMS_Scope.md`) - All Annex A controls in the SoA (see `0100_ISMS_Statement_of_Applicability_SoA_Template.md`) - All ISMS processes and documents - All locations: {{ netbox.site.name }} and others

14.2 2. Audit Approach

14.2.1 2.1 Audit Principles

Independence: - Auditors do not audit their own areas - External auditors for critical areas (optional) - Reporting line: Audit team reports to {{ meta.audit.manager }}

Risk-Based: - Audit frequency based on risk assessment - Critical areas audited more frequently - Focus on high risks and critical controls

Scope-Based: - All areas within ISMS scope are audited - Complete coverage within audit cycle (3 years)

Objective and Evidence-Based: - Audit findings based on objective evidence - Sample-based testing - Documentation of all findings

14.2.2 2.2 Audit Types

Complete ISMS Audit: - Frequency: Annually - Scope: Entire ISMS - Duration: 5-10 days

Topic Audits: - Frequency: Quarterly - Scope: Specific topics (e.g., access management, patch management) - Duration: 1-2 days

Follow-up Audits: - Frequency: As needed - Scope: Verification of corrective action implementation - Duration: 0.5-1 day

14.3 3. Annual Plan

14.3.1 3.1 Audit Annual Plan 2026

Period	Audit Topic/Scope	Audit Type	Criteria	Auditor	Auditee	Planned Duration	Status
Q1 2026	Access Management & IAM	Topic Audit	A.5.15, A.5.16, A.5.17, A.5.18, A.8.2, A.8.3	[TODO]	Anna Schmidt	2 days	Planned
Q2 2026	Vulnerability & Patch Management	Topic Audit	A.8.8, A.5.23	[TODO]	IT Operations	1 day	Planned
Q3 2026	Complete ISMS Audit	Full Audit	All Clauses, SoA	[TODO]	Thomas Weber	10 days	Planned
Q4 2026	Incident Management & Logging	Topic Audit	A.5.24, A.5.25, A.5.26, A.5.28, A.8.15, A.8.16	[TODO]	Security Team	2 days	Planned

[TODO: Complete audit plan for 2026]

14.3.2 3.2 Audit Frequency by Risk

Area	Risk Level	Audit Frequency
Privileged Access Management	High	Semi-annually

Area	Risk Level	Audit Frequency
Vulnerability Management	High	Semi-annually
Incident Management	High	Semi-annually
Backup & Recovery	Medium	Annually
Physical Security	Medium	Annually
HR Security	Low	Every 2 years

14.4 4. Audit Process

14.4.1 4.1 Audit Phases

```
1. Planning
     Define audit scope
     Appoint audit team
     Create audit plan
     Inform auditee

2. Preparation
     Request documents
     Create audit checklist
     Define samples
     Plan interviews

3. Execution
     Opening meeting
     Document review
     Interviews
     Sampling
     Observations
     Closing meeting

4. Reporting
     Document findings
     Create audit report
     Report to auditee
     Report to management

5. Follow-up
     Plan corrective actions
     Monitor implementation
     Follow-up audit
     Close findings
```

14.4.2 4.2 Audit Checklist (Example)

Audit Topic: Access Management

Check Point	Criterion	Evidence	Result	Remarks
Are access rights documented?	Policy 0220	IAM documentation	/	
Are access rights regularly recertified?	Guideline 0230	Recertification protocols	/	
Is least privilege principle implemented?	A.8.2	IAM configuration	/	
Are joiner/mover/leaver processes followed?	Guideline 0230	HR tickets, IAM logs	/	
Is MFA enabled for all users?	A.5.17	MFA configuration	/	

[TODO: Create complete checklists for all audit topics]

14.4.3 4.3 Audit Criteria

Document Review: - Are documents current and approved? - Are documents complete and consistent? - Are responsibilities defined?

Evidence Review: - Is evidence available and current? - Is evidence traceable? - Is evidence sufficient for proof?

Control Effectiveness: - Is the control implemented? - Is the control effective (sampling)? - Are there deviations or weaknesses?

Compliance: - Are policies and guidelines followed? - Are legal requirements met? - Are contractual obligations met?

14.5 5. Audit Findings

14.5.1 5.1 Finding Categories

Major Non-Conformity (Severe): - Significant violation of ISO 27001:2022 - Critical control not implemented - Systemic failure - **Example:** No risk analysis performed

Minor Non-Conformity (Minor): - Minor violation of ISO 27001:2022 - Control partially implemented - Isolated error - **Example:** Documentation incomplete

Observation: - Improvement potential - Best practice not implemented - No violation of requirements - **Example:** Process could be more efficient

Opportunity for Improvement: - Recommendation for improvement - No deviation - **Example:** Automation possible

14.5.2 5.2 Finding Documentation

For each finding: - Finding ID (e.g., F-2026-Q1-001) - Category (Major/Minor/Observation) - Description - Affected area/control - Evidence - Impact - Recommended corrective action - Responsible

person - Deadline

14.5.3 5.3 Corrective Actions

Process: 1. Auditee plans corrective action 2. CISO approves action and deadline 3. Auditee implements action 4. Auditor verifies implementation (follow-up) 5. Finding is closed

Deadlines: - Major Non-Conformity: 30 days - Minor Non-Conformity: 90 days - Observation: 180 days

14.6 6. Audit Report

14.6.1 6.1 Report Structure

Executive Summary: - Audit scope and objective - Audit date and team - Summary of results - Overall assessment

Audit Details: - Audit methodology - Audited areas and controls - Samples - Interviews

Findings: - List of all findings (by category) - Detailed description of each finding - Recommended corrective actions

Positive Observations: - Best practices - Well-implemented controls - Improvements since last audit

Conclusion: - Overall assessment of ISMS - Recommendations - Next steps

14.6.2 6.2 Report Distribution

Recipients: - Auditee - CISO - Management - Information security committee

Confidentiality: - Audit reports are confidential - Access only for authorized persons

14.7 7. Auditor Qualification

14.7.1 7.1 Auditor Requirements

Technical Qualification: - Knowledge of ISO 27001:2022 - Knowledge of ISO 27002:2022 - Knowledge of audit methodology - Industry knowledge

Certifications (recommended): - ISO 27001 Lead Auditor - CISA (Certified Information Systems Auditor) - CISM (Certified Information Security Manager)

Soft Skills: - Communication skills - Objectivity - Analytical thinking - Documentation skills

14.7.2 7.2 Auditor Training

Initial Training: - ISO 27001:2022 training - Audit methodology training - Shadowing experienced auditors

Continuous Education: - Annual refresher - Participation in auditor conferences - Exchange with other auditors

14.8 8. Audit Metrics

14.8.1 8.1 KPIs

Metric	Target Value	Current	Status
Audit plan fulfillment	100%	[TODO]%	[TODO]
Average time to remediate (Major)	< 30 days	[TODO] days	[TODO]
Average time to remediate (Minor)	< 90 days	[TODO] days	[TODO]
Number of open findings	< 5	[TODO]	[TODO]
Recurring findings	0	[TODO]	[TODO]

14.8.2 8.2 Trend Analysis

Annual Review: - Number of findings per year (trend) - Most common finding categories - Areas with most findings - Improvements since previous year

14.9 9. Roles and Responsibilities

14.9.1 9.1 RACI Matrix: Audit Process

Activity	Audit Manager	Auditor	Auditee	CISO	Management
Create audit program	R/A	C	C	C	I
Plan audit	R	R	C	I	I
Conduct audit	A	R	C	I	I
Document findings	A	R	C	I	I
Create audit report	R/A	R	C	I	I
Plan corrective actions	C	C	R/A	C	I
Conduct follow-up	A	R	C	I	I
Review audit program	R/A	C	C	C	C

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

14.10 10. References

14.10.1 10.1 Internal Documents

- `0020_ISMS_Scope.md` - ISMS Scope
- `0100_ISMS_Statement_of_Applicability_SoA_Template.md` - SoA
- `0140_ISMS_Management_Review_Template.md` - Management Review
- `0150_ISMS_Non_Conformities_and_Corrective_Actions.md` - Non-conformities
- All Policies (0200-0680) and Guidelines (0210-0690)

14.10.2 10.2 External Standards

- **ISO/IEC 27001:2022** - Clause 9.2: Internal audit
- **ISO 19011:2018** - Guidelines for auditing management systems

- **ISO/IEC 27007:2020** - Guidelines for information security management systems auditing

---

Approved by:
{{ meta.audit.manager }}, Audit Manager
Thomas Weber, CISO
Date: {{ meta.document.approval_date }}

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

ewpage

Chapter 15

Management Review (Template)

Document ID: 0140
Document Type: ISMS Evidence/Template
Standard Reference: ISO/IEC 27001:2022 Clause 9.3
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Confidential
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

15.1 1. Management Review Overview

15.1.1 1.1 Participants and Period

Review Date: [TODO: Date]
Review Period: [TODO: e.g., 01.01.2026 - 31.12.2026]
Next Review: [TODO: Date]

Participants:

Name	Role	Present
{{ meta.management.ceo }}	Management (Chair)	/
Thomas Weber	CISO	/
Anna Schmidt	CIO	/
[TODO]	CFO	/
[TODO]	Department Representatives	/
{{ meta.audit.manager }}	Internal Audit (Advisory)	/

15.1.2 1.2 Scope

This management review encompasses: - Entire ISMS in scope (see `0020_ISMS_Scope.md`) - All locations: {{ netbox.site.name }} and others - Review period: [TODO]

15.2 2. Inputs (Clause 9.3.2)

15.2.1 2.1 Status of Actions from Previous Review

Actions from last review ([TODO: Date]):

Action	Responsible	Deadline	Status	Remarks
[TODO]	[TODO]	[TODO]	Completed / In Progress / Open	[TODO]

Summary: - Completed: [TODO] of [TODO] - In Progress: [TODO] - Open/Overdue: [TODO]

15.2.2 2.2 Changes in External and Internal Issues

External Changes: - **Regulatory Changes:** [TODO: e.g., NIS2 implementation, GDPR updates] - **Threat Landscape:** [TODO: e.g., New ransomware variants, APT activities] - **Market Development:** [TODO: e.g., New competitors, customer requirements] - **Technology Trends:** [TODO: e.g., Cloud migration, AI adoption]

Internal Changes: - **Organizational:** [TODO: e.g., Mergers, acquisitions, restructuring] - **Personnel:** [TODO: e.g., New CISO, team expansion] - **Technological:** [TODO: e.g., New systems, cloud migration] - **Processes:** [TODO: e.g., DevOps introduction, agile transformation]

Impact on ISMS: - Scope changes required: Yes / No - Risk analysis update required: Yes / No - Policy updates required: Yes / No

15.2.3 2.3 Feedback on Information Security Performance

KPI Development:

KPI	Target Value	Current	Previous Year	Trend	Status
Number of security incidents	< 10/quarter	[TODO]	[TODO]	$\uparrow$ / $\rightarrow$ / $\downarrow$	/
Risks with score 13	< 5	[TODO]	[TODO]	$\uparrow$ / $\rightarrow$ / $\downarrow$	/
Uptime of critical systems	99.5%	[TODO]%	[TODO]%	$\uparrow$ / $\rightarrow$ / $\downarrow$	/

KPI	Target Value	Current	Previous Year	Trend	Status
Patch compliance (critical)	< 7 days	[TODO] days	[TODO] days	↑ / → / ↓	/
Training participation	100%	[TODO]%	[TODO]%	↑ / → / ↓	/
Phishing click rate	< 5%	[TODO]%	[TODO]%	↑ / → / ↓	/

Summary: - Objectives achieved: [TODO] of [TODO] - Improvements: [TODO] - Deteriorations: [TODO]

Stakeholder Feedback: - Customers: [TODO] - Employees: [TODO] - Regulatory authorities: [TODO] - Suppliers: [TODO]

15.2.4 2.4 Results of Internal and External Audits

Internal Audits:

Audit Date	Scope	Findings (Major/Minor/Obs)	Status	Remarks
[TODO]	Access Management	0 / 2 / 3	Completed	All findings resolved
[TODO]	Vulnerability Management	1 / 1 / 2	In Progress	Major finding being addressed
[TODO]	Complete ISMS	0 / 5 / 8	Completed	Improvements implemented

External Audits:

Audit Date	Auditor	Scope	Result	Certificate	Remarks
[TODO]	[TODO: Certification body]	ISO 27001:2022	Passed	Valid until [TODO]	Recertification successful

Summary: - Open major findings: [TODO] - Open minor findings: [TODO] - Average remediation time: [TODO] days

15.2.5 2.5 Feedback from Interested Parties

Customers: - Security requirements: [TODO] - Satisfaction: [TODO] - Incidents with customer impact: [TODO]

Regulatory Authorities: - Reportable incidents: [TODO] - Compliance status: [TODO]

Suppliers: - Third-party risks: [TODO] - Security incidents at suppliers: [TODO]

15.2.6 2.6 Results of Risk Assessment

Risk Overview:

Risk Level	Number of Risks	Previous Year	Trend
Very High	[TODO]	[TODO]	↑ / → / ↓
High	[TODO]	[TODO]	↑ / → / ↓
Medium	[TODO]	[TODO]	↑ / → / ↓
Low	[TODO]	[TODO]	↑ / → / ↓

Top 5 Risks:

Risk ID	Description	Score	Treatment	Status
R-001	[TODO]	[TODO]	[TODO]	[TODO]
R-002	[TODO]	[TODO]	[TODO]	[TODO]
R-003	[TODO]	[TODO]	[TODO]	[TODO]
R-004	[TODO]	[TODO]	[TODO]	[TODO]
R-005	[TODO]	[TODO]	[TODO]	[TODO]

New Risks: - [TODO: List of new risks since last review]

Closed Risks: - [TODO: List of closed risks]

15.2.7 2.7 Opportunities for Continuous Improvement

Identified Improvement Opportunities:

ID	Area	Improvement	Benefit	Effort	Priority
I-001	[TODO]	[TODO]	[TODO]	[TODO]	High / Medium / Low
I-002	[TODO]	[TODO]	[TODO]	[TODO]	High / Medium / Low

Lessons Learned: - From security incidents: [TODO] - From audits: [TODO] - From projects: [TODO]

15.2.8 2.8 Relevant Changes

ISMS Scope: - Changes: [TODO: New locations, systems, processes] - Impact: [TODO]

Technology: - New systems: [TODO] - Cloud migration: [TODO] - Technology refresh: [TODO]

Suppliers: - New critical suppliers: [TODO] - Terminated supplier relationships: [TODO]

Personnel: - New key personnel: [TODO] - Departures: [TODO]

15.2.9 2.9 Incidents and Lessons Learned

Security Incidents:

Incident ID	Date	Severity	Description	Impact	Lessons Learned	Status
INC-001	[TODO]	High	[TODO]	[TODO]	[TODO]	Closed
INC-002	[TODO]	Medium	[TODO]	[TODO]	[TODO]	Closed

Summary: - Number of incidents: [TODO] - Major incidents: [TODO] - MTTD (Mean Time to Detect): [TODO] - MTTR (Mean Time to Respond): [TODO]

Implemented Improvements: - [TODO: Measures from lessons learned]

15.2.10 2.10 Resources

Budget: - Planned budget: [TODO] € - Actual expenses: [TODO] € - Variance: [TODO] € ([TODO]%)

Personnel: - Planned FTE: [TODO] - Actual FTE: [TODO] - Bottlenecks: [TODO]

External Support: - Consultants: [TODO] - Managed services: [TODO] - Training: [TODO]

15.3 3. Outputs / Decisions (Clause 9.3.3)

15.3.1 3.1 Adjustments to ISMS Policy and Objectives

ISMS Policy: - Changes required: Yes / No - Description: [TODO] - Responsible: Thomas Weber - Deadline: [TODO]

Security Objectives: - New objectives: [TODO] - Adjustment of existing objectives: [TODO] - Responsible: Thomas Weber - Deadline: [TODO]

15.3.2 3.2 Resources and Investments

Approved Investments:

Investment	Description	Budget	Responsible	Deadline	Priority
[TODO]	[TODO]	[TODO] €	[TODO]	[TODO]	High / Medium / Low

Personnel Resources: - Additional FTE: [TODO] - External support: [TODO] - Training budget: [TODO] €

15.3.3 3.3 Improvement Measures

Approved Measures:

Measure ID	Measure	Objective	Responsible	Deadline	Budget	Status
M-001	[TODO]	[TODO]	[TODO]	[TODO]	[TODO] €	Approved
M-002	[TODO]	[TODO]	[TODO]	[TODO]	[TODO] €	Approved

15.3.4 3.4 Accepted Risks

Risk Acceptance by Management:

Risk ID	Description	Score	Justification	Valid Until	Compensating Measures
R-010	[TODO]	[TODO]	[TODO]	[TODO]	[TODO]

15.3.5 3.5 Scope Changes

Approved Scope Changes: - [TODO: New locations, systems, processes] - Impact on risk analysis: [TODO] - Impact on SoA: [TODO] - Responsible: Thomas Weber - Deadline: [TODO]

15.3.6 3.6 Strategic Decisions

Strategic Direction: - [TODO: e.g., Cloud-first strategy, zero-trust architecture]

Compliance Strategy: - [TODO: e.g., NIS2 preparation, additional certifications]

Security Culture: - [TODO: e.g., Security Champions Program, awareness campaigns]

15.4 4. Summary and Assessment

15.4.1 4.1 Overall Assessment of ISMS

Suitability: - The ISMS is suitable for the organization: Yes / No / Partially - Justification: [TODO]

Adequacy: - The ISMS is adequate for the risks: Yes / No / Partially - Justification: [TODO]

Effectiveness: - The ISMS is effective: Yes / No / Partially - Justification: [TODO]

Overall Assessment: - [TODO: Summary assessment by management]

15.4.2 4.2 Next Steps

1. [TODO: Action 1]
2. [TODO: Action 2]
3. [TODO: Action 3]

Next Management Review: [TODO: Date]

15.5 5. Appendices

15.5.1 5.1 Supporting Documents

- Risk Register (`0080_ISMS_Risk_Register_Template.md`)
- Risk Treatment Plan (`0090_ISMS_Risk_Treatment_Plan_RTP_Template.md`)
- Audit Reports (`0130_ISMS_Internal_Audit_Program.md`)
- KPI Dashboard (`0110_ISMS_Security_Objectives_and_Metrics.md`)
- Incident Reports (`0400_Policy_Incident_Management.md`)

15.5.2 5.2 Presentations

- [TODO: Link to management review presentation]

15.6 6. References

15.6.1 6.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0020_ISMS_Scope.md` - ISMS Scope
- `0080_ISMS_Risk_Register_Template.md` - Risk Register
- `0090_ISMS_Risk_Treatment_Plan_RTP_Template.md` - Risk Treatment Plan
- `0110_ISMS_Security_Objectives_and_Metrics.md` - Security Objectives
- `0130_ISMS_Internal_Audit_Program.md` - Internal Audit Program

15.6.2 6.2 External Standards

- **ISO/IEC 27001:2022** - Clause 9.3: Management review
- **ISO/IEC 27002:2022** - Information security controls

15.7 Change History

Version	Date	Author	Description	Approved By
1.0	{{ meta.document.date }}	Thomas Wabel	Initial version	{{ meta.management.ceo }}

Recorded by:
Thomas Weber, CISO
Date: [TODO]

Approved by:
{{ meta.management.ceo }}, Management
Date: [TODO]

Next Review: [TODO: Date] (Annually)

ewpage

Chapter 16

Non-Conformities and Corrective Actions

Document ID: 0150
Document Type: ISMS Process/Template
Standard Reference: ISO/IEC 27001:2022 Clause 10.1
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

16.1 1. Purpose and Objective

16.1.1 1.1 Purpose

This document defines the process for systematic treatment of non-conformities in the ISMS of **AdminSend GmbH**. It ensures that: - Deviations from requirements are identified and documented - Root causes are analyzed and addressed - Corrective actions are effectively implemented - Recurrence is prevented

16.1.2 1.2 Types of Non-Conformities

Audit Findings: - Major non-conformities (severe) - Minor non-conformities (minor) - Observations

Security Incidents: - Security incidents with root cause in process/control weaknesses

Policy Violations: - Violations of ISMS policies and guidelines

Compliance Violations: - Violations of legal or contractual requirements

16.2 2. Process

16.2.1 2.1 Process Overview

```
1. Capture
     Identify non-conformity
     Create ticket/finding
     Categorize and prioritize

2. Root Cause Analysis
     Perform root cause analysis
     Identify contributing factors
     Recognize systemic causes

3. Define Corrective Action
     Immediate action (containment)
     Corrective action
     Preventive action

4. Implementation
     Implement action
     Track progress
     Document

5. Effectiveness Verification
     Verify effectiveness
     Conduct follow-up
     Document lessons learned

6. Closure
     Close finding
     Archive documentation
     Communication
```

16.2.2 2.2 Step 1: Capture

Identification: - Through audits (internal/external) - Through security incidents - Through monitoring and KPIs - Through employee reports - Through management reviews

Documentation: - Assign finding ID (e.g., F-2026-001) - Description of non-conformity - Affected area/control - Evidence - Categorization (Major/Minor/Observation) - Priority (High/Medium/Low)

Responsible: Auditor, ISMS Manager, or Reporter

16.2.3 2.3 Step 2: Root Cause Analysis

Root Cause Analysis (RCA): - **5-Why Method:** Why did this happen? (ask 5 times) - **Fishbone Diagram:** Cause categories (People, Process, Technology, Environment) - **Fault Tree Analysis:** Logical analysis of failure causes

To Identify: - Immediate cause - Root cause - Contributing factors - Systemic causes

Documentation: - RCA method - Identified causes - Contributing factors

Responsible: Finding owner, supported by ISMS Manager

16.2.4 2.4 Step 3: Define Corrective Action

Immediate Action: - Containment of problem - Damage limitation - Temporary solution

Corrective Action: - Address root cause - Permanent solution - Process/control improvement

Preventive Action: - Prevent recurrence - Prevent similar problems - Systemic improvements

Documentation: - Description of action - Responsible person - Deadline - Resources/budget - Success criteria

Responsible: Finding owner, approved by CISO

16.2.5 2.5 Step 4: Implementation

Implementation: - Implement action according to plan - Document progress - Inform stakeholders

Tracking: - Regular status updates - Escalation for delays - Adjustment for problems

Documentation: - Implementation steps - Deviations from plan - Lessons learned

Responsible: Finding owner

16.2.6 2.6 Step 5: Effectiveness Verification

Verification: - Is the action implemented? - Is the non-conformity resolved? - Is the root cause eliminated?

Validation: - Is the action effective? - Does the problem still occur? - Are there unintended side effects?

Methods: - Follow-up audit - Sampling - Monitoring - Interviews

Documentation: - Effectiveness verification performed on - Method - Result - Evidence

Responsible: Auditor or ISMS Manager

16.2.7 2.7 Step 6: Closure

Closure Criteria: - Action fully implemented - Effectiveness demonstrated - Documentation complete - Lessons learned documented

Closure Activities: - Set finding status to “Closed” - Archive documentation - Inform stakeholders - Communicate lessons learned

Responsible: ISMS Manager

16.3 3. Non-Conformities Register

16.3.1 3.1 Active Non-Conformities

Finding ID	Source	Category	Description	Root Cause	Corrective Action	Owner	Due	Status	Effectiveness Verified
F-2026-001	Audit	Minor	Documentation incomplete	Process not defined	Document process	[TODO]	2026-03-31	In Progress	-
F-2026-002	Incident	Major	Unpatched vulnerability exploited	Patch process insufficient	Improve patch process	IT Operations	2026-02-28	In Progress	-
F-2026-003	Monitoring	Observation	MFA activation < 100%	Awareness insufficient	MFA campaign	Thomas Weber	2026-04-30	Planned	-

[TODO: Add active non-conformities]

16.3.2 3.2 Closed Non-Conformities (Archive)

Finding ID	Source	Category	Description	Corrective Action	Closure Date	Effectiveness Confirmed
F-2025-050	Audit	Minor	Backup tests not documented	Establish backup test process	2026-01-15	Yes
F-2025-051	Incident	Major	Phishing incident	Security awareness training	2026-01-20	Yes

[TODO: Archive closed non-conformities]

16.4 4. Prioritization and Deadlines

16.4.1 4.1 Prioritization

Category	Priority	Deadline	Escalation
Major Non-Conformity	Very High	30 days	Immediately to CISO and management
Minor Non-Conformity	High	90 days	To CISO if delayed
Observation	Medium	180 days	To ISMS Manager if delayed

Category	Priority	Deadline	Escalation
Opportunity for Improvement	Low	As available	None

16.4.2 4.2 Escalation

Overdue Actions: - > 2 weeks overdue: Reminder to owner - > 4 weeks overdue: Escalation to CISO - > 8 weeks overdue: Escalation to management

Critical Non-Conformities: - Major non-conformities: Immediate escalation - Compliance violations: Immediate escalation - Recurring non-conformities: Escalation to management

16.5 5. Root Cause Analysis Methods

16.5.1 5.1 5-Why Method

Example: 1. **Why** did the non-conformity occur? → Unpatched vulnerability was exploited 2. **Why** was the vulnerability unpatched? → Patch was not installed in time 3. **Why** was the patch not installed in time? → Patch process did not prioritize patch 4. **Why** did the process not prioritize the patch? → CVSS score was not considered 5. **Why** was CVSS score not considered? → Process only considers vendor severity

Root Cause: Patch prioritization not based on CVSS score

Corrective Action: Extend patch process with CVSS-based prioritization

16.5.2 5.2 Fishbone Diagram (Ishikawa)

Categories: - **People:** Lack of training, errors, negligence - **Process:** Insufficient processes, missing documentation - **Technology:** Missing tools, misconfiguration, bugs - **Environment:** Organizational factors, resource shortage

16.6 6. Effectiveness Verification

16.6.1 6.1 Methods

Audit: - Follow-up audit - Sample testing - Document review

Monitoring: - KPI tracking - Incident tracking - Compliance monitoring

Testing: - Penetration tests - Vulnerability scans - Configuration audits

Interviews: - Questioning affected persons - Feedback collection

16.6.2 6.2 Success Criteria

Action is effective when: - Non-conformity no longer occurs - Root cause is eliminated - KPIs have improved - No new problems have emerged - Stakeholders are satisfied

16.7 7. Lessons Learned

16.7.1 7.1 Documentation

For each closed non-conformity: - What did we learn? - What worked well? - What could be improved? - Which actions are transferable?

16.7.2 7.2 Communication

Target Groups: - Affected teams - ISMS committee - Management - All employees (for relevant lessons learned)

Channels: - Lessons learned database - Security newsletter - Team meetings - Awareness campaigns

16.8 8. Roles and Responsibilities

16.8.1 8.1 RACI Matrix: Non-Conformities Process

Activity	CISO	ISMS Manager	Finding Owner	Auditor	Management
Capture non-conformity	A	R	C	R	I
Root cause analysis	A	C	R	C	I
Define action	A	C	R	C	I
Approve action	A	C	I	I	C
Implement action	A	C	R	I	I
Verify effectiveness	A	R	C	R	I
Close finding	A	R	C	C	I

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

16.9 9. Metrics and Reporting

16.9.1 9.1 KPIs

Metric	Target Value	Current	Status
Open major findings	0	[TODO]	/
Open minor findings	< 5	[TODO]	/
Average remediation time (Major)	< 30 days	[TODO] days	/
Average remediation time (Minor)	< 90 days	[TODO] days	/
Overdue findings	0	[TODO]	/
Recurring findings	0	[TODO]	/

16.9.2 9.2 Reporting

Monthly: - Status of all open findings - Overdue findings - Newly added findings

Quarterly: - Trend analysis - Most common causes - Effectiveness of actions

Annually: - Complete review in management review - Lessons learned summary

16.10 10. References

16.10.1 10.1 Internal Documents

- `0130_ISMS_Internal_Audit_Program.md` - Internal Audit Program
- `0140_ISMS_Management_Review_Template.md` - Management Review
- `0160_ISMS_Continuous_Improvement.md` - Continuous Improvement
- `0400_Policy_Incident_Management.md` - Incident Management

16.10.2 10.2 External Standards

- **ISO/IEC 27001:2022** - Clause 10.1: Nonconformity and corrective action
- **ISO 9001:2015** - Clause 10.2: Nonconformity and corrective action
- **ISO 19011:2018** - Guidelines for auditing management systems

---

Approved by:
Thomas Weber, CISO
Date: {{ meta.document.approval_date }}

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

ewpage

Chapter 17

Continuous Improvement (CI) in the ISMS

Document ID: 0160
Document Type: ISMS Foundation Document
Standard Reference: ISO/IEC 27001:2022 Clause 10.2
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

17.1 1. Purpose and Objectives

17.1.1 1.1 Purpose

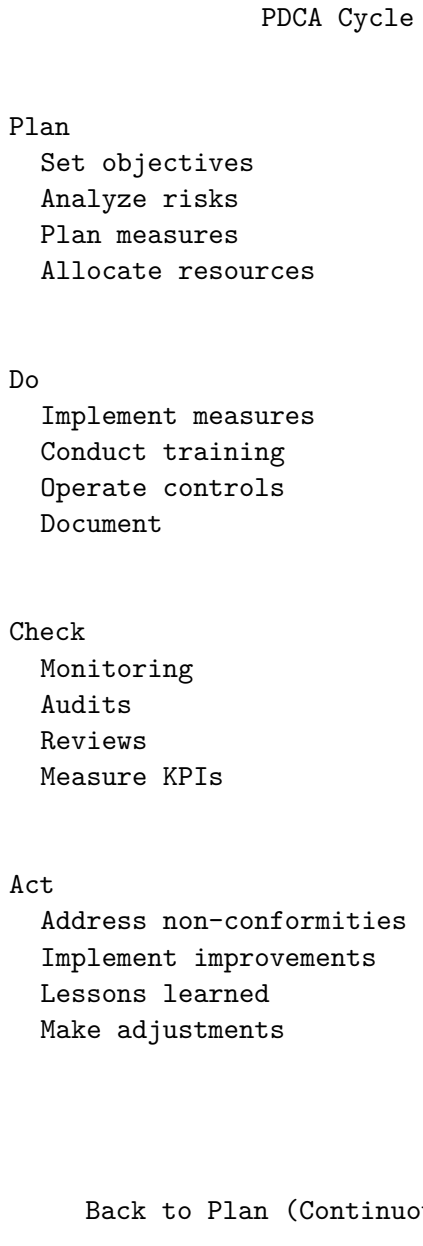
The continuous improvement (CI) program of **AdminSend GmbH** ensures that: - The ISMS is continuously improved - Improvement opportunities are systematically identified - Improvement measures are prioritized and implemented - The suitability, adequacy, and effectiveness of the ISMS are maintained

17.1.2 1.2 Objectives

- **Continuous Improvement:** At least 10 improvement measures per year
- **Lessons Learned:** Systematic evaluation of all incidents and audits
- **Innovation:** Use of new technologies and best practices
- **Efficiency:** Optimization of processes and controls

17.1.3 1.3 PDCA Cycle

The ISMS follows the PDCA cycle (Plan-Do-Check-Act):



17.2 2. Sources for Improvements

17.2.1 2.1 Audits and Findings

Internal Audits: - Audit findings (Major/Minor/Observations) - Opportunities for improvement - Best practices from other areas

External Audits: - Certification audits - Customer audits - Regulatory audits

See: `0130_ISMS_Internal_Audit_Program.md`

17.2.2 2.2 Incidents and Postmortems

Security Incidents: - Root cause analysis - Lessons learned - Preventive measures

Near Misses: - Near-miss incidents - Early warning indicators - Proactive measures

See: `0400_Policy_Incident_Management.md`

17.2.3 2.3 Risk Assessments

Risk Analysis: - New risks - Changed risk assessments - Emerging threats

Risk Treatment: - Effectiveness of measures - New treatment options - Optimization potential

See: `0080_ISMS_Risk_Register_Template.md`

17.2.4 2.4 KPIs and Monitoring

Performance Metrics: - KPI trends - Deviations from target values - Benchmarking

Monitoring Data: - SIEM alerts - Vulnerability scans - Log analysis

See: `0110_ISMS_Security_Objectives_and_Metrics.md`

17.2.5 2.5 Changes in Context

External Changes: - New threats - New technologies - New regulations - Industry trends

Internal Changes: - Organizational changes - New systems/processes - Strategic direction

See: `0030_ISMS_Context_and_Interested_Parties.md`

17.2.6 2.6 Stakeholder Feedback

Customers: - Security requirements - Satisfaction surveys - Complaints

Employees: - Process feedback - Improvement suggestions - Usability issues

Management: - Strategic directives - Resource decisions

17.2.7 2.7 Best Practices and Innovation

External Sources: - Industry standards (NIST, CIS, etc.) - Security conferences - Threat intelligence - Peer exchange

Internal Innovation: - Proof of concepts - Pilot projects - Technology evaluations

17.3 3. CI Backlog

17.3.1 3.1 Improvement Suggestions

Item ID	Title	Source	Description	Benefit	Effort	Owner	Priority	Status
CI-001	SIEM automation	Monitoring	Automatic response playbooks	Faster incident response	40 PD	Security Team	High	Planned

Item ID	Title	Source	Description	Benefit	Effort	Owner	Priority	Status
CI-002	Zero-trust architecture	Best Practice	Implement zero-trust principles	Improved segmentation	200 PD	Anna Schmidt	Medium	Evaluation
CI-003	Security Champions Program	Awareness	Multipliers in all teams	Higher security awareness	20 PD	Thomas Weber	High	In Progress
CI-004	Immutable infrastructure	DevOps	Infrastructure as Code with immutability	Better compliance, less drift	80 PD	DevOps	Medium	Planned

[TODO: Add additional improvement suggestions]

17.3.2 3.2 Prioritization

Prioritization Criteria:

Criterion	Weight	Rating (1-5)
Risk reduction	40%	How much is risk reduced?
Compliance benefit	20%	Improves compliance?
Efficiency gain	20%	Saves time/resources?
Effort	10%	How high is the effort? (inverted)
Strategic alignment	10%	Fits strategy?

Prioritization Formula:

```
Priority = (Risk Reduction × 0.4) + (Compliance × 0.2) +
           (Efficiency × 0.2) + ((6 - Effort) × 0.1) +
           (Strategy × 0.1)
```

Priority Levels: - **Very High (4.0-5.0):** Implement immediately - **High (3.0-3.9):** Within 6 months - **Medium (2.0-2.9):** Within 12 months - **Low (< 2.0):** As available

17.4 4. Improvement Process

17.4.1 4.1 Process Steps

```
1. Identification
     Recognize improvement potential
     Create description
     Add to backlog
```

```
2. Assessment
     Assess benefit
     Estimate effort
     Prioritize
     Obtain approval

3. Planning
     Detailed planning
     Allocate resources
     Create timeline
     Inform stakeholders

4. Implementation
     Implementation
     Testing
     Documentation
     Training

5. Review
     Verify effectiveness
     Lessons learned
     Documentation
     Communication
```

17.4.2 4.2 Approval Process

Small Improvements (< 10 PD, < €5,000): - Approval by CISO

Medium Improvements (10-40 PD, €5,000-25,000): - Approval by CISO and CIO

Large Improvements (> 40 PD, > €25,000): - Approval by management - Presentation to information security committee

17.5 5. Improvement Categories

17.5.1 5.1 Process Improvements

Objective: Efficiency increase, error reduction

Examples: - Automation of manual processes - Simplification of complex processes - Tool integration - Standardization

17.5.2 5.2 Control Improvements

Objective: Increase effectiveness

Examples: - New security controls - Improvement of existing controls - Control automation - Monitoring extensions

17.5.3 5.3 Technology Improvements

Objective: Modernization, innovation

Examples: - New security tools - Cloud migration - Zero-trust architecture - AI/ML-based security

17.5.4 5.4 Awareness Improvements

Objective: Increase security awareness

Examples: - New training formats - Gamification - Security champions - Awareness campaigns

17.5.5 5.5 Documentation Improvements

Objective: Clarity, completeness

Examples: - Update outdated documents - New templates - Better structuring - Automated documentation

17.6 6. Lessons Learned

17.6.1 6.1 Lessons Learned Process

After each incident/audit/project: 1. Conduct lessons learned session 2. Document findings 3. Derive improvement measures 4. Add to CI backlog 5. Communicate

17.6.2 6.2 Lessons Learned Database

Structure: - Date and context - What happened? - What did we learn? - What worked well? - What could be improved? - Derived measures - Status of measures

Access: - All employees (read) - ISMS team (write)

17.6.3 6.3 Communication

Target Groups: - Affected teams - ISMS committee - Management - All employees (for relevant lessons learned)

Channels: - Lessons learned database - Security newsletter - Team meetings - Awareness campaigns

17.7 7. Innovation and Best Practices

17.7.1 7.1 Technology Radar

Observation of new technologies: - Emerging security technologies - Cloud security - Zero trust - AI/ML in security - DevSecOps

Assessment: - Adopt (Use) - Trial (Try) - Assess (Evaluate) - Hold (Wait)

17.7.2 7.2 Proof of Concepts (PoCs)

Process: 1. Identify technology 2. Define PoC scope 3. Conduct PoC 4. Evaluate 5. Decision: Adopt / Reject

Budget: - Annual PoC budget: [TODO] €

17.7.3 7.3 Benchmarking

Comparison with: - Industry standards - Peer organizations - Best practices

Sources: - NIST Cybersecurity Framework - CIS Controls - SANS Top 20 - Gartner/Forrester reports

17.8 8. Metrics and Reporting

17.8.1 8.1 CI KPIs

Metric	Target Value	Current	Status
Number of improvement measures per year	10	[TODO]	/
Average implementation time	< 90 days	[TODO] days	/
Implemented improvements	80%	[TODO]%	/
Lessons learned documented	100%	[TODO]%	/
PoCs conducted	3 per year	[TODO]	/

17.8.2 8.2 Reporting

Quarterly: - Status of CI backlog - Implemented improvements - Lessons learned summary

Annually: - Complete CI report in management review - Trend analysis - Success stories

17.9 9. Roles and Responsibilities

17.9.1 9.1 RACI Matrix: Continuous Improvement

Activity	CISO	ISMS Manager	Improvement Owner	Teams	Management
Identify improvements	A	R	R	R	I
Assess improvements	A	R	C	C	I
Prioritize improvements	A	R	C	C	C
Approve improvements	A	C	I	I	C
Implement improvements	A	C	R	R	I

Activity	CISO	ISMS Manager	Improvement Owner	Teams	Management
Verify effectiveness	A	R	C	C	I
Document lessons learned	A	R	R	C	I

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

17.10 10. References

17.10.1 10.1 Internal Documents

- `0110_ISMS_Security_Objectives_and_Metrics.md` - Security Objectives
- `0130_ISMS_Internal_Audit_Program.md` - Internal Audit Program
- `0140_ISMS_Management_Review_Template.md` - Management Review
- `0150_ISMS_Non_Conformities_and_Corrective_Actions.md` - Non-conformities
- `0400_Policy_Incident_Management.md` - Incident Management

17.10.2 10.2 External Standards

- **ISO/IEC 27001:2022** - Clause 10.2: Continual improvement
- **ISO 9001:2015** - Clause 10.3: Continual improvement
- **NIST Cybersecurity Framework** - Continuous improvement practices

---

Approved by:
Thomas Weber, CISO
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

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

ewpage

Chapter 18

Policy: Acceptable Use of IT

Document ID: 0200
Document Type: Policy (Abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.5.10 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

18.1 1. Purpose

This policy defines the principles for acceptable use of IT resources at **AdminSend GmbH**. It ensures that IT systems, applications, and information are used exclusively for business purposes and in compliance with legal and regulatory requirements.

18.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Systems:** All IT systems, networks, applications, email, internet, cloud services
- **Persons:** All employees, contractors, temporary workers, interns, and third parties with access to IT resources
- **Devices:** Company-owned and private devices (BYOD) accessing company resources
- **Locations:** {{ netbox.site.name }} and all operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

18.3 3. Principles (Policy Statements)

18.3.1 3.1 Business Use

IT resources of the organization are provided primarily for business purposes. Personal use is permitted only to the extent that it does not interfere with business use and complies with security policies.

18.3.2 3.2 Responsible Use

Users are required to use IT resources responsibly, efficiently, and in accordance with all applicable policies. Misuse, waste, or damage to IT resources is prohibited.

18.3.3 3.3 Prohibited Activities

The following activities are expressly prohibited: - Accessing, storing, or distributing illegal, offensive, or inappropriate content - Circumventing security controls or unauthorized access to systems - Installing unauthorized software or modifying system configurations - Using IT resources for commercial purposes outside business activities - Sending spam, phishing, or other malicious communications

18.3.4 3.4 Privacy and Confidentiality

Users must maintain the confidentiality of company information and must not share or publish confidential information without authorization.

18.3.5 3.5 Monitoring and Surveillance

The organization reserves the right to monitor the use of IT resources to ensure security, compliance, and proper use. Users have no expectation of privacy when using company resources.

18.3.6 3.6 Personal Responsibility

Users are personally responsible for all activities performed under their credentials. Credentials must not be shared.

18.4 4. Roles and Responsibilities

18.4.1 RACI Matrix: Acceptable Use of IT

Activity	CISO	IT Operations	HR	Employee	Legal/Compliance
Policy creation	R/A	C	C	I	C
Policy communication	R	C	R	I	I
Training and awareness	C	C	R	R	I
Monitoring and surveillance	A	R	I	I	C
Investigate violations	R	C	R	I	C
Enforce sanctions	C	I	R/A	I	C

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

18.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **Implementation Responsible:** IT Operations, HR
- **Control/Audit Authority:** ISMS, Internal Audit, Legal/Compliance

18.5 5. Derivatives (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

18.5.1 Related Guidelines

- **0210_Guideline_Acceptable_Use_of_IT.md** - Detailed implementation guideline
- `0220_Policy_Access_Control_and_Identity_Management.md` - Access Control Policy
- `0500_Policy_Mobile_Device_and_Remote_Work.md` - Mobile Device Policy
- `0660_Policy_Information_Transfer_and_Communication.md` - Communication Policy

18.5.2 Related Standards/Baselines

- Email usage guidelines
- Internet usage guidelines
- BYOD guidelines (Bring Your Own Device)
- Social media guidelines

18.5.3 Related Processes

- User onboarding/offboarding
- Incident response for policy violations
- HR disciplinary procedures

18.6 6. Compliance, Monitoring and Enforcement

18.6.1 Metrics and KPIs

- Number of policy violations per quarter
- Training participation rate (Target: 100% annually)
- Number of blocked inappropriate accesses
- Average time to investigate violations
- Repeat offender rate

18.6.2 Evidence

- Training records and confirmations
- Monitoring logs and audit trails
- Incident reports for violations
- Disciplinary action documentation
- Awareness campaign metrics

18.6.3 Consequences for Violations

Violations of this policy will be handled according to applicable HR and compliance processes: - **Minor Violations:** Warning, retraining, monitoring - **Medium Violations:** Written warning, temporary access restrictions - **Severe Violations:** Employment consequences up to termination, legal action - **Intentional Violations:** Immediate suspension, termination, criminal prosecution

18.7 7. Exceptions

Exceptions to this policy are only permitted in justified cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and, if applicable, HR
- **Documentation:** All exceptions are documented and regularly reviewed
- **Time Limit:** Exceptions are generally time-limited

18.8 8. References

18.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0210_Guideline_Acceptable_Use_of_IT.md` - Detailed Guideline
- `0400_Policy_Incident_Management.md` - Incident Management Policy
- `0530_Guideline_HR_Onboarding_Role_Change_Offboarding.md` - HR Security Guideline

18.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.5.10** - Acceptable use of information and other associated assets
- **ISO/IEC 27002:2022** - Information security controls
- **GDPR (EU 2016/679)** - General Data Protection Regulation
- Employment law requirements for IT use

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 19

Guideline: Acceptable Use of IT

Document ID: 0210
Document Type: Guideline (detailed)
Related Policy: 0200_Policy_Acceptable_Use_of_IT.md
Standard Reference: ISO/IEC 27001:2022 Annex A.5.10
Owner: {{ meta.it_operations.manager }}
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

19.1 1. Purpose and Scope

This guideline implements the `0200_Policy_Acceptable_Use_of_IT.md` and defines detailed rules, procedures, and technical controls for the acceptable use of IT resources at **AdminSend GmbH**.

Scope: - All employees, contractors, and third parties with access to IT resources - All IT systems, networks, applications, and devices - Locations: {{ netbox.site.name }} and all operational sites

19.2 2. Detailed Usage Rules

19.2.1 2.1 Email Usage

Permitted Use: - Business communication with customers, partners, and colleagues - Limited personal use (max. 10 emails per day, no large attachments) - Registration for business online services

Prohibited Activities: - Sending spam, chain letters, or unsolicited mass emails - Sending confidential information without encryption - Using personal email accounts for business communication - Opening suspicious attachments or links (see phishing awareness) - Automatic forwarding of business emails to external addresses

Technical Controls: - Email filtering and anti-spam systems - DLP (Data Loss Prevention) for outgoing emails - Email archiving for compliance (retention: {{ meta.retention.email_years }} years) - Encryption for confidential emails (S/MIME or PGP)

19.2.2 2.2 Internet Usage

Permitted Use: - Research for business purposes - Access to approved cloud services and SaaS applications - Limited personal use during breaks (max. 30 minutes per day) - Access to professional portals, documentation, and training resources

Prohibited Activities: - Access to illegal, pornographic, or violence-glorifying content - Downloading unapproved software or files - Streaming videos/music during work hours (except for business purposes) - Using anonymization services (VPN, proxy) without approval - Online shopping, gambling, or private business activities

Technical Controls: - Web filtering and URL categorization - Blocking known malware and phishing sites - Bandwidth management for streaming services - Logging and monitoring of internet usage - SSL inspection for encrypted traffic (with data protection compliance)

19.2.3 2.3 Software Installation and Usage

Permitted Activities: - Using approved software from the software catalog - Software installation by IT operations or via self-service portal - Using browser extensions from approved whitelist

Prohibited Activities: - Installing unapproved software (shadow IT) - Using pirated or unlicensed software - Installing peer-to-peer software (torrents, file sharing) - Disabling or bypassing security software (antivirus, EDR) - Changing system configurations without approval

Technical Controls: - Application whitelisting (only approved software can execute) - Software Asset Management (SAM) for license compliance - Endpoint protection (antivirus, EDR) with tamper protection - Regular software inventory - Patch management for approved software

19.2.4 2.4 Data Handling and Storage

Permitted Activities: - Storing business data on approved network drives and cloud storage - Using {{ meta.cloud.storage_service }} for file storage - Encrypting confidential data according to classification

Prohibited Activities: - Storing business data on personal cloud services (Dropbox, personal Google Drive) - Storing confidential data on local hard drives without encryption - Sharing access credentials or passwords - Exfiltrating large amounts of data without approval

Technical Controls: - DLP (Data Loss Prevention) for data transfer monitoring - Hard drive encryption (BitLocker, FileVault) - Cloud Access Security Broker (CASB) for cloud service monitoring - Network segmentation for sensitive data - Backup and retention per `0420_Policy_Backup_und_Wiederherstellung.md`

19.2.5 2.5 Mobile Devices and BYOD

Permitted Activities: - Using company-owned mobile devices for business purposes - BYOD (Bring Your Own Device) after registration and MDM enrollment - Accessing approved enterprise applications via mobile apps

Prohibited Activities: - Jailbreaking or rooting devices - Installing unapproved apps on BYOD devices with enterprise access - Storing confidential data on personal devices without container - Using insecure WiFi networks without VPN

Technical Controls: - Mobile Device Management (MDM) for all devices with enterprise access - Containerization for business data on BYOD devices - Remote wipe in case of loss or theft - Enforced encryption and PIN/biometrics - Compliance checks (OS version, jailbreak detection)

Details: See `0500_Policy_Mobile_Device_und_Remote_Work.md`

19.2.6 2.6 Social Media and External Communication

Permitted Activities: - Using social media for marketing and corporate communication (authorized accounts) - Professional use of LinkedIn, Xing for networking - Participation in professional forums and communities (with disclaimer)

Prohibited Activities: - Publishing confidential company information - Negative statements about company, customers, or colleagues - Pretending to represent official company opinion without authorization - Using company logos without approval

Guidelines: - Social media guidelines for employees - Approval process for official company accounts - Training on social engineering and phishing via social media

19.2.7 2.7 Remote Work and VPN Usage

Permitted Activities: - Remote access via approved VPN connections - Using remote desktop (RDP, Citrix) for system access - Working from home office after approval

Prohibited Activities: - Using insecure networks without VPN - Sharing VPN credentials - Working in public areas with screen visibility (shoulder surfing) - Using personal devices without MDM enrollment

Technical Controls: - VPN with multi-factor authentication (MFA) - Zero Trust Network Access (ZTNA) for granular access control - Endpoint compliance checks before VPN access - Session timeouts and idle disconnects

Details: See `0500_Policy_Mobile_Device_und_Remote_Work.md`

19.3 3. Monitoring and Surveillance

19.3.1 3.1 Monitoring Scope

The organization monitors the following activities to ensure security and compliance:

- **Email Traffic:** Metadata (sender, recipient, subject), DLP scans
- **Internet Usage:** Visited URLs, categories, bandwidth usage
- **File Transfers:** Uploads/downloads, cloud service usage
- **System Access:** Login activities, privileged access
- **Application Usage:** Used applications, usage duration

19.3.2 3.2 Data Protection and Privacy

Principles: - Monitoring is purpose-bound for security and compliance - No indiscriminate monitoring of individual employees - Monitoring data is only analyzed with justified suspicion - Compliance with GDPR and works council agreements

Transparency: - Employees are informed about monitoring measures (onboarding, training) - Works council is involved in monitoring measures - Data protection officer reviews monitoring concepts

19.3.3 3.3 Incident Response for Violations

Process: 1. **Detection:** Automatic alerts for policy violations (DLP, web filter, SIEM) 2. **Triage:** IT security reviews alert and assesses severity 3. **Investigation:** With justified suspicion: detailed analysis, HR involvement 4. **Measures:** Depending on severity: warning, training, disciplinary action 5. **Documentation:** Incident report, lessons learned

Escalation: - Minor violations: IT operations informs supervisor - Medium violations: CISO and HR are involved - Severe violations: Management, legal, possibly law enforcement

19.4 4. Training and Awareness

19.4.1 4.1 Mandatory Training

Onboarding: - Acceptable Use Policy training (1 hour) - Phishing awareness training - Data protection basics

Annual Refresher: - Acceptable Use Policy refresher (30 minutes) - Current threats and best practices - Quiz for knowledge verification (passing threshold: 80%)

19.4.2 4.2 Awareness Campaigns

Regular Measures: - Monthly security newsletters - Phishing simulations (quarterly) - Posters and infographics on security topics - Lunch & Learn sessions on current topics

19.4.3 4.3 Documentation

Evidence: - Training participation tracking in LMS (Learning Management System) - Policy acknowledgment confirmations (annual) - Quiz results and certificates - Phishing simulation results

19.5 5. Exceptions and Special Cases

19.5.1 5.1 Exception Process

Request: - Form: Exception request with justification and risk assessment - Approval: CISO (for technical exceptions), HR (for usage exceptions) - Time limit: Max. 12 months, then re-evaluation

Examples of Exceptions: - Installing special software for projects - Extended internet access for research - Using personal devices without MDM (temporary)

Documentation: See `0640_Policy_Ausnahmen_und_Risk_Waivers.md`

19.5.2 5.2 Privileged Users

Administrators and IT Operations: - Extended rights for system administration - Additional training and background checks - Increased monitoring of privileged activities - Four-eyes principle for critical changes

Details: See `0230_Richtlinie_IAM_Joiner_Mover_Leaver_und_Zugriffsantraege.md`

19.6 6. Technical Implementation

19.6.1 6.1 Technology Stack

Security Tools: - **Web Filter:** {{ meta.security.web_filter }} (e.g., Cisco Umbrella, Zscaler) - **Email Security:** {{ meta.security.email_gateway }} (e.g., Proofpoint, Mimecast) - **DLP:** {{ meta.security.dlp_solution }} (e.g., Microsoft Purview, Symantec DLP) - **Endpoint Protection:** {{ meta.security.edr_solution }} (e.g., CrowdStrike, SentinelOne) - **CASB:** {{ meta.security.casb_solution }} (e.g., Microsoft Defender for Cloud Apps)

Monitoring and Logging: - **SIEM:** {{ meta.security.siem_solution }} (e.g., Splunk, Microsoft Sentinel) - **Log Retention:** {{ meta.retention.log_years }} years for security logs - **Alerting:** Automatic alerts for critical violations

19.6.2 6.2 Configuration Examples

Web Filter Categories (blocked): - Adult Content, Gambling, Illegal Drugs - Malware, Phishing, Command & Control - Anonymizers, Proxy Avoidance - Peer-to-Peer, File Sharing (except approved services)

DLP Rules: - Blocking credit card numbers in emails - Warning when sending documents with "Confidential" classification - Blocking uploads to unapproved cloud services - Detection of PII (Personally Identifiable Information) in file transfers

Application Whitelisting: - Only signed applications from approved catalog - Blocking PowerShell/CMD for standard users - Exceptions for developers and administrators

19.7 7. Compliance and Audit

19.7.1 7.1 Key Performance Indicators (KPIs)

Metric	Target Value	Measurement
Training Participation	100% annually	LMS reports
Policy Violations	< 5 per month	SIEM alerts
Phishing Click Rate	$< 5\%$	Simulation results
Unapproved Software	0 installations	Software inventory
DLP Incidents	< 10 per month	DLP reports

19.7.2 7.2 Audit Evidence

Documentation: - Policy documents and version history - Training evidence and confirmations - Monitoring logs and incident reports - Exception register - Audit trails for access and changes

Audit Frequency: - Internal audits: Annually - External audits: For ISO 27001 certification - Ad-hoc audits: In case of suspected violations

19.8 8. Review and Updates

Review Cycle: - Annual review by CISO and IT operations - Ad-hoc updates for new threats or technologies - Involvement of HR and legal for changes

Change Management: - Changes are managed through change process - Communication to all employees for significant changes - Update of training materials

19.9 9. References

19.9.1 Internal Documents

- `0200_Policy_Acceptable_Use_of_IT.md` - Parent policy
- `0220_Policy_Zugriffssteuerung_und_Identitaetsmanagement.md` - Access control
- `0320_Policy_Logging_und_Monitoring.md` - Logging policy
- `0400_Policy_Incident_Management.md` - Incident management
- `0500_Policy_Mobile_Device_und_Remote_Work.md` - Mobile device policy
- `0640_Policy_Ausnahmen_und_Risk_Waivers.md` - Exception process

19.9.2 External Standards

- **ISO/IEC 27001:2022 Annex A.5.10** - Acceptable use of information
- **ISO/IEC 27002:2022** - Information security controls
- **GDPR (EU 2016/679)** - General Data Protection Regulation
- **Works Constitution Act (BetrVG)** - Co-determination in monitoring

---

Approved by:
Thomas Weber, CISO
Date: {{ meta.document.approval_date }}

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

ewpage

Chapter 20

Policy: Access Control and Identity Management

Document ID: 0220
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.5.15-A.5.18 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

20.1 1. Purpose

This policy defines the principles for access control and identity management (IAM) at **AdminSend GmbH**. It ensures that access to information and IT systems is granted exclusively to authorized persons based on the need-to-know principle and least privilege.

20.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Systems:** All IT systems, applications, databases, networks, cloud services
- **Persons:** All employees, contractors, suppliers, and third parties with access to IT resources
- **Access Methods:** Local access, remote access, privileged access, API access
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Ausnahmen_und_`

20.3 3. Principles (Policy Statements)

20.3.1 3.1 Least Privilege

Users receive only the minimum access rights required to fulfill their duties. Privileged access is granted restrictively and reviewed regularly.

20.3.2 3.2 Need-to-Know Principle

Access to information is only granted when there is a business necessity. Access is granted based on roles and responsibilities.

20.3.3 3.3 Identity Lifecycle (Joiner-Mover-Leaver)

Identities are managed throughout their entire lifecycle: - **Joiner:** Access rights are granted upon entry based on role and function - **Mover:** Access rights are adjusted during role changes (revoke old rights, grant new ones) - **Leaver:** All access rights are immediately revoked upon departure

20.3.4 3.4 Role-Based Access Control (RBAC)

Access rights are primarily granted through roles and groups, not through individual permissions. Role models are regularly reviewed and updated.

20.3.5 3.5 Segregation of Duties

Critical functions are divided so that no single person can perform all steps of a sensitive process. This prevents fraud and errors.

20.3.6 3.6 Regular Recertification

Access rights are regularly reviewed and recertified (at least annually). Rights that are no longer needed are revoked.

20.3.7 3.7 Privileged Access Management (PAM)

Privileged accounts (administrators, root, service accounts) are subject to special controls: - Separate accounts for privileged activities - Just-in-Time (JIT) access where possible - Comprehensive logging and monitoring

20.3.8 3.8 Access Approval and Documentation

All access grants must be approved and documented by the resource owner. Access decisions are traceable and auditable.

20.4 4. Roles and Responsibilities

20.4.1 RACI Matrix: Access Control and IAM

Activity	CISO	IT Operations	Resource Owner	HR	Employee
Policy Creation	R/A	C	C	C	I

Activity	CISO	IT Operations	Resource Owner	HR	Employee
IAM System Operations	C	R/A	I	I	I
Request Access	I	I	C	I	R
Approve Access	C	I	R/A	C	I
Provision Access	I	R	I	I	I
Recertification	C	C	R/A	C	I
Revoke Access (Leaver)	C	R	I	R/A	I
Monitoring and Audits	R/A	C	C	I	I

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

20.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **IAM Manager:** {{ meta.it.iam_manager }}
- **Resource Owners:** Department heads, system owners
- **Implementation Responsible:** IT operations, HR
- **Control/Audit Function:** ISMS, internal audit

20.5 5. Derivations (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

20.5.1 Related Guidelines

- **0230_Richtlinie_IAM_Joiner_Mover_Leaver_und_Zugriffsantraege.md** - Detailed IAM guideline
- `0240_Policy_Authentisierung_und_Passwoerter.md` - Authentication policy
- `0520_Policy_HR_Security.md` - HR security policy
- `0640_Policy_Ausnahmen_und_Risk_Waivers.md` - Exception policy

20.5.2 Related Standards/Baselines

- Role model and RBAC matrix
- Privileged Access Management (PAM) standard
- Recertification process
- Service account management

20.5.3 Related Processes

- Joiner-Mover-Leaver process
- Access approval process
- Recertification process
- Incident response for unauthorized access

20.6 6. Compliance, Monitoring, and Enforcement

20.6.1 Metrics and KPIs

- Number of open access requests and average processing time
- Recertification rate (target: 100% annually)
- Number of non-recertified accounts
- Number of privileged accounts and their usage frequency
- Number of least privilege violations
- Average time to deactivate leaver accounts (target: < 1 day)

20.6.2 Evidence and Proof

- IAM system logs and audit trails
- Access approvals and requests
- Recertification evidence
- Joiner-Mover-Leaver documentation
- Privileged access logs
- Audit reports on access rights

20.6.3 Consequences for Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Unauthorized access grants:** Immediate suspension, investigation, possible disciplinary action - **Non-recertified accounts:** Automatic deactivation after deadline - **Abuse of privileged access:** Immediate suspension, employment law consequences - **Sharing of credentials:** Warning up to termination

20.7 7. Exceptions

Exceptions to this policy are only permitted in justified exceptional cases:

- **Exception Process:** See `0640_Policy_Ausnahmen_und_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and resource owner
- **Documentation:** All exceptions are documented in the risk register
- **Time Limit:** Exceptions are generally time-limited and regularly reviewed

20.8 8. References

20.8.1 Internal Documents

- `0010_ISMS_Informationssicherheitsleitlinie.md` - ISMS policy
- `0230_Richtlinie_IAM_Joiner_Mover_Leaver_und_Zugriffsantraege.md` - Detailed IAM guideline
- `0080_ISMS_Risikoregister_Template.md` - Risk register
- `0530_Richtlinie_HR_Onboarding_Rollenwechsel_Offboarding.md` - HR security guideline

20.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.5.15** - Identity management

- **ISO/IEC 27001:2022 Annex A.5.16** - Access rights
- **ISO/IEC 27001:2022 Annex A.5.17** - Authentication information
- **ISO/IEC 27001:2022 Annex A.5.18** - Access rights review
- **ISO/IEC 27002:2022** - Information security controls
- **NIST SP 800-63** - Digital Identity Guidelines

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 21

Guideline: IAM - Joiner, Mover, Leaver and Access Requests

Document ID: 0230
Document Type: Guideline (detailed)
Related Policy: 0220_Policy_Access_Control_and_Identity_Management.md
Standard Reference: ISO/IEC 27001:2022 Annex A.5.15, A.5.16, A.5.18
Owner: {{ meta.it_operations.manager }}
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

21.1 1. Purpose and Scope

This guideline implements the `0220_Policy_Access_Control_and_Identity_Management.md` and defines detailed processes for: - **Joiner:** Onboarding new employees and access provisioning - **Mover:** Role changes and access adjustments - **Leaver:** Offboarding and access revocation - **Access Requests:** Process for ad-hoc access requests

Scope: All employees, contractors, and third parties at **AdminSend GmbH**

21.2 2. Joiner Process (Onboarding)

21.2.1 2.1 Process Overview

Trigger: HR creates new employee in HR system ({{ meta.hr.system }})

Timeline: - **Standard Accounts:** Provisioning by 1 day before start date - **Special Access:** Provisioning by 3 days before start date - **External Contractors:** Provisioning after contract signing

21.2.2 2.2 Detailed Workflow

Phase 1: HR Initiation (T-5 days) 1. HR creates employee record in {{ meta.hr.system }} 2. HR defines: - Department, role, location - Supervisor, cost center - Start date, contract type (permanent, temporary, internship) 3. Automatic notification to IT operations

Phase 2: IT Provisioning (T-3 days) 1. **Account Creation:** - Active Directory / Azure AD account - Email mailbox ({{ meta.email.system }}) - Username per schema: `{{ meta.naming.user_format }}` (e.g., firstname.lastname) - Initial password (temporary, must be changed at first login)

2. **Basic Access (automatic via role model):**
   - Access to intranet and collaboration tools
   - Standard applications for department
   - Network drives according to department membership
   - VPN access (if remote work)
3. **Hardware Provisioning:**
   - Laptop/desktop per role (see hardware catalog)
   - Mobile device (if required)
   - Peripherals (monitor, keyboard, mouse)
   - Asset tagging and inventory

Phase 3: Special Access (T-2 days) 1. Supervisor requests special access via self-service portal 2. Approval by resource owner 3. Provisioning by IT operations or automated

Phase 4: Onboarding Day (T-0) 1. **Welcome Email:** - Credentials (initial password) - Links to training and policies - IT support contact information 2. **First Login:** - Password change enforced - MFA registration (authenticator app, hardware token) - Acceptable Use Policy confirmation 3. **IT Orientation:** - Device usage, VPN access - Password manager training - Phishing awareness basics

21.2.3 2.3 Role-Based Access (RBAC)

Standard Roles:

Role	Description	Automatic Access
Employee_Standard	All employees	Intranet, email, Office 365, VPN
Employee_Developer	Developers	+ Git, CI/CD, dev environments
Employee_Finance	Finance department	+ ERP, accounting software
Employee_HR	Human resources	+ HR system, applicant management
Employee_Sales	Sales	+ CRM, quotation system
Contractor_Standard	External contractors	Basic access, time-limited
Contractor_Developer	External developers	+ Dev access, time-limited

Privileged Roles: - `Admin_System`: System administrators (Windows, Linux) - `Admin_Network`: Network administrators - `Admin_Security`: Security team - `Admin_Database`: Database administrators

21.2.4 2.4 External Contractors and Third Parties

Special Considerations: - **Contract Review:** IT access only after contract signing and NDA - **Time Limitation:** Accounts automatically deactivated after contract end - **Restricted Access:** Only project-related resources - **Sponsorship:** Every external account requires internal sponsor - **Recertification:** Quarterly review by sponsor

21.3 3. Mover Process (Role Change)

21.3.1 3.1 Process Overview

Trigger: HR updates employee data (department change, promotion, new role)

Timeline: Access adjustment within 2 business days after HR change

21.3.2 3.2 Detailed Workflow

Phase 1: HR Change 1. HR updates employee record in {{ meta.hr.system }} 2. Changes: Department, role, supervisor, location 3. Automatic notification to IT operations and previous/new supervisors

Phase 2: Access Review 1. **Previous Supervisor:** Confirms revocation of no longer needed access 2. **New Supervisor:** Requests new required access 3. **IT Operations:** Reviews current access and plans changes

Phase 3: Access Adjustment 1. **Revoke Old Access:** - Removal from old department groups - Revocation of department-specific application access - Archiving old emails (if mailbox change) 2. **Provision New Access:** - Addition to new department groups - Provisioning new application access - Adjustment of network drives and permissions

Phase 4: Documentation 1. Update CMDB and asset management 2. Documentation of access changes 3. Notification to employee about changes

21.3.3 3.3 Promotions and Privilege Elevation

Additional Checks for Privilege Elevation: - **Approval:** CISO approval for privileged roles - **Background Check:** Extended verification for admin rights - **Training:** Additional security training for privileged users - **Monitoring:** Increased monitoring of privileged activities

21.4 4. Leaver Process (Offboarding)

21.4.1 4.1 Process Overview

Trigger: HR marks employee as leaving in {{ meta.hr.system }}

Timeline: - **Planned Departure:** Deactivation on last working day - **Unplanned Departure:** Immediate deactivation (e.g., termination, emergency)

21.4.2 4.2 Detailed Workflow

Phase 1: Preparation (T-14 days) 1. HR informs IT operations about departure date 2. **Knowledge Transfer:** - Supervisor identifies critical access and information - Handover to suc-

cessor or team - Documentation of passwords for shared accounts (in password manager) 3. **Data Backup:** - Backup of personal drives - Email mailbox archiving - Handover of project-relevant files

Phase 2: Last Working Day (T-0) 1. **Account Deactivation (End of Business Day):** - Active Directory / Azure AD account deactivated - Email forwarding to supervisor (temporary, 30 days) - VPN access blocked - All application access revoked 2. **Hardware Return:** - Laptop, mobile device, peripherals - Access cards, keys - Asset inventory updated 3. **Exit Interview:** - Return of all company property - Reminder of confidentiality obligations - Confirmation of data return

Phase 3: Post-Offboarding (T+30 days) 1. **Account Deletion:** - After 30 days: Final account deletion - Email archiving per retention policy ({{ meta.retention.email_years }} years) - Deletion of personal data (GDPR compliant) 2. **License Release:** - Return of software licenses - Update license management 3. **Documentation:** - Offboarding checklist completed - Audit trail for compliance

21.4.3 4.3 Emergency Offboarding

Immediate Deactivation for: - Termination for cause - Security incidents or suspected abuse - Court orders

Process: 1. **Immediate Suspension (within 1 hour):** - All accounts deactivated - VPN and remote access blocked - Access cards deactivated - Mobile devices remotely wiped (if MDM) 2. **Forensics:** - Backup of logs and activities - Analysis in case of suspected data abuse - Involvement of legal and HR 3. **Communication:** - Information to supervisor and security team - Documentation for legal purposes

21.5 5. Access Requests

21.5.1 5.1 Self-Service Portal

Access: {{ meta.iam.portal_url }}

Functions: - Request new access (applications, network drives, groups) - Overview of own access - Status tracking of requests - Recertification of own access

21.5.2 5.2 Request Workflow

Step 1: Request Submission 1. Employee submits request via self-service portal 2. **Required Information:** - Resource/application - Business justification - Required permission level - Time period (permanent or time-limited)

Step 2: Approval 1. **Supervisor:** Reviews business necessity (1st approval) 2. **Resource Owner:** Reviews technical authorization (2nd approval) 3. **CISO:** Additional approval for privileged access 4. **Automatic Approval:** For standard access per role model

Step 3: Provisioning 1. **Automatic:** For standard applications (within 15 minutes) 2. **Manual:** For special access (within 1 business day) 3. **Notification:** Email to requester upon completion

Step 4: Documentation 1. Audit trail in IAM system 2. CMDB update 3. Compliance reporting

21.5.3 5.3 Time-Limited Access

Use Cases: - Project-related access - Substitutions (vacation, illness) - External contractors - Test and development access

Automatic Deactivation: - System automatically deactivates access after expiration date - Notification to user 7 days before expiration - Extension only through new request

21.6 6. Recertification

21.6.1 6.1 Regular Access Reviews

Frequency: - **Standard Users:** Annual recertification - **Privileged Users:** Quarterly recertification - **External Contractors:** Quarterly recertification - **Critical Systems:** Monthly recertification

21.6.2 6.2 Recertification Process

Step 1: Automatic Campaign 1. IAM system starts recertification campaign 2. Email to supervisors with list of employee access 3. Deadline: 14 days for confirmation

Step 2: Review by Supervisors 1. Supervisor reviews each access: - **Confirm:** Access still required - **Revoke:** Access no longer needed - **Escalate:** Uncertainty, query to resource owner 2. Documentation of decision

Step 3: Automatic Enforcement 1. Confirmed access remains active 2. Unconfirmed access is automatically revoked after deadline 3. Escalated cases are forwarded to CISO

Step 4: Reporting 1. Compliance report for audit 2. Identification of access anomalies 3. Optimization of role model

21.6.3 6.3 Privileged Access

Additional Controls: - **Four-Eyes Principle:** Two approvals required - **Just-in-Time (JIT) Access:** Privileges only when needed, time-limited - **Privileged Access Management (PAM):** Management via PAM system ({{ meta.security.pam_solution }}) - **Session Recording:** Recording of privileged sessions for audit

21.7 7. Technical Implementation

21.7.1 7.1 IAM Technology Stack

Systems: - **Identity Provider:** {{ meta.iam.idp }} (e.g., Azure AD, Okta) - **HR System:** {{ meta.hr.system }} (e.g., SAP SuccessFactors, Workday) - **IAM Portal:** {{ meta.iam.portal }} (e.g., SailPoint, Saviynt) - **PAM System:** {{ meta.security.pam_solution }} (e.g., CyberArk, BeyondTrust) - **CMDB:** {{ meta.itsm.cmdb }} (e.g., ServiceNow, Jira Service Management)

Integration: - HR system → IAM system (automatic synchronization) - IAM system → Active Directory / Azure AD (provisioning) - IAM system → Applications (SCIM, SAML, API)

21.7.2 7.2 Automation

Automated Processes: - Account creation for joiner (within 1 hour after HR entry) - Role-based access provisioning (RBAC) - Account deactivation for leaver (on last working day) - Time-limited access (automatic deactivation) - Recertification campaigns (automatic start)

Manual Processes: - Special access outside role model - Privileged access (after approval) - Emergency offboarding (immediate suspension)

21.8 8. Compliance and Audit

21.8.1 8.1 Key Performance Indicators (KPIs)

Metric	Target Value	Measurement
Joiner Provisioning	< 1 day	IAM system
Leaver Deactivation	100% on last day	IAM system
Access Requests (Processing Time)	< 1 business day	IAM system
Recertification (Completion Rate)	$> 95\%$	IAM system
Orphaned Accounts	0	Quarterly review

21.8.2 8.2 Audit Evidence

Documentation: - Joiner/Mover/Leaver logs (audit trail) - Access requests and approvals - Recertification reports - Privileged access and approvals - Emergency offboarding documentation

Audit Frequency: - Internal audits: Quarterly - External audits: Annually (ISO 27001) - Ad-hoc audits: For security incidents

21.9 9. References

21.9.1 Internal Documents

- `0220_Policy_Access_Control_and_Identity_Management.md` - Parent policy
- `0250_Richtlinie_MFA_Passwortregeln_und_Session_Management.md` - Authentication
- `0530_Richtlinie_HR_Onboarding_Rollenwechsel_Offboarding.md` - HR security
- `0640_Policy_Ausnahmen_und_Risk_Waivers.md` - Exception process

21.9.2 External Standards

- **ISO/IEC 27001:2022 Annex A.5.15** - Access control
- **ISO/IEC 27001:2022 Annex A.5.16** - Identity management
- **ISO/IEC 27001:2022 Annex A.5.18** - Access rights
- **NIST SP 800-63** - Digital Identity Guidelines

Approved by:
Thomas Weber, CISO
Date: {{ meta.document.approval_date }}

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

ewpage

Chapter 22

Policy: Authentication and Passwords

Document ID: 0240
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.5.17, A.5.18 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

22.1 1. Purpose

This policy defines the principles for authentication and password management at **AdminSend GmbH**. It ensures that user identity is securely verified and authentication information is appropriately protected.

22.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Systems:** All IT systems, applications, databases, networks, cloud services
- **Persons:** All employees, contractors, suppliers, and third parties with access to IT resources
- **Authentication Methods:** Passwords, multi-factor authentication (MFA), biometric methods, tokens
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Ausnahmen_und_`

22.3 3. Principles (Policy Statements)

22.3.1 3.1 Strong Authentication

All access to IT systems and applications requires secure authentication. The strength of authentication is based on the protection requirements of the resource and the risk.

22.3.2 3.2 Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) is mandatory for access to critical systems, privileged accounts, and remote access. MFA combines at least two independent factors: - Knowledge (password, PIN) - Possession (token, smartphone, smartcard) - Biometrics (fingerprint, facial recognition)

22.3.3 3.3 Password Requirements

Passwords must meet the following minimum requirements: - Sufficient length and complexity (details in guideline) - No reuse of old passwords - No sharing or writing down - Regular change when compromise is suspected

22.3.4 3.4 Passwordless Authentication

The organization promotes the use of passwordless authentication methods (e.g., FIDO2, Windows Hello, biometric methods) where technically feasible and secure.

22.3.5 3.5 Session Management

Authenticated sessions are protected by appropriate measures: - Automatic lockout on inactivity - Secure session tokens - Logout functionality - No concurrent sessions for privileged accounts

22.3.6 3.6 Protection of Authentication Information

Passwords and other authentication information are stored securely: - Encrypted or hashed storage (no plaintext passwords) - Secure transmission (TLS/SSL) - Protection against brute-force attacks (account lockout, rate limiting)

22.3.7 3.7 Privileged Accounts

Privileged accounts (administrators, root, service accounts) are subject to stricter authentication requirements: - Mandatory MFA - Separate accounts for privileged activities - Just-in-Time (JIT) access where possible - Comprehensive logging

22.3.8 3.8 Password Reset and Account Recovery

Password reset and account recovery processes must be securely designed and verify user identity before granting access.

22.4 4. Roles and Responsibilities

22.4.1 RACI Matrix: Authentication and Passwords

Activity	CISO	IT Operations	Employee	IAM Team	Security Operations
Policy Creation	R/A	C	I	C	C
MFA Implementation	A	R	I	R	C
Password Reset	I	R	R	R	I
Session Monitoring	C	C	I	C	R/A
Brute-Force Protection	A	R	I	C	R
Incident Response	R/A	C	I	C	R

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

22.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **IAM Manager:** {{ meta.it.iam_manager }}
- **Implementation Responsible:** IT operations, IAM team
- **Control/Audit Function:** ISMS, internal audit, security operations

22.5 5. Derivations (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

22.5.1 Related Guidelines

- **0250_Richtlinie_MFA_Passwortregeln_und_Session_Management.md** - Detailed implementation guideline
- `0220_Policy_Zugriffssteuerung_und_Identitaetsmanagement.md` - Access control policy
- `0260_Policy_Kryptografie_und_Schluesselmanagement.md` - Cryptography policy
- `0400_Policy_Incident_Management.md` - Incident management policy

22.5.2 Related Standards/Baselines

- Password complexity requirements
- MFA implementation standard
- Session timeout configurations
- Privileged Access Management (PAM) standard

22.5.3 Related Processes

- Password reset process
- Account recovery process

- MFA enrollment process
- Incident response for authentication incidents

22.6 6. Compliance, Monitoring, and Enforcement

22.6.1 Metrics and KPIs

- MFA adoption rate (target: 100% for critical systems)
- Number of password reset requests per month
- Number of failed authentication attempts
- Number of account lockouts
- Average password strength (entropy)
- Number of compromised accounts

22.6.2 Evidence and Proof

- Authentication logs and audit trails
- MFA enrollment status
- Password policy compliance reports
- Brute-force detection logs
- Incident reports for authentication incidents
- Penetration test results

22.6.3 Consequences for Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Weak passwords:** Forced password change, retraining - **Password sharing:** Warning up to termination - **MFA bypass:** Immediate suspension, investigation - **Repeated violations:** Employment law consequences

22.7 7. Exceptions

Exceptions to this policy are only permitted in justified exceptional cases:

- **Exception Process:** See `0640_Policy_Ausnahmen_und_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO
- **Documentation:** All exceptions are documented in the risk register
- **Time Limit:** Exceptions are generally time-limited and regularly reviewed
- **Compensating Controls:** Exceptions require alternative security measures

22.8 8. References

22.8.1 Internal Documents

- `0010_ISMS_Informationssicherheitsleitlinie.md` - ISMS policy
- `0250_Richtlinie_MFA_Passwortregeln_und_Session_Management.md` - Detailed guideline
- `0220_Policy_Zugriffssteuerung_und_Identitaetsmanagement.md` - Access control policy
- `0080_ISMS_Risikoregister_Template.md` - Risk register

22.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.5.17** - Authentication information
- **ISO/IEC 27001:2022 Annex A.5.18** - Access rights review
- **ISO/IEC 27002:2022** - Information security controls
- **NIST SP 800-63B** - Digital Identity Guidelines: Authentication and Lifecycle Management
- **NIST SP 800-63-3** - Digital Identity Guidelines
- **BSI TR-02102** - Cryptographic Procedures: Recommendations and Key Lengths

---

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 23

Guideline: MFA, Password Rules and Session Management

Document ID: 0250
Document Type: Guideline (detailed)
Related Policy: 0240_Policy_Authentication_and_Passwords.md
Standard Reference: ISO/IEC 27001:2022 Annex A.5.17, A.5.18
Owner: {{ meta.it_operations.manager }}
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

23.1 1. Purpose and Scope

This guideline implements the `0240_Policy_Authentication_and_Passwords.md` and defines detailed rules for: - Multi-factor authentication (MFA) - Password policies and complexity requirements - Session management and timeouts - Authentication methods and technologies

Scope: All systems, applications, and users at **AdminSend GmbH**

23.2 2. Multi-Factor Authentication (MFA)

23.2.1 2.1 MFA Requirements

Mandatory for: - All remote access (VPN, remote desktop) - All privileged accounts (administrators, root) - Access to critical systems (production, financial systems) - Cloud services and SaaS applications - Email access from external devices - Access to confidential data

Optional for: - Local logins in the office (can be enforced via conditional access) - Non-critical internal applications

23.2.2 2.2 MFA Methods

Supported Factors:

Method	Type	Security Level	Use Case
Authenticator App (TOTP)	Possession	High	Standard for all users
Hardware Token (FIDO2/U2F)	Possession	Very High	Privileged users, high security
SMS Code	Possession	Medium	Fallback, not recommended
Push Notification	Possession	High	Mobile users
Biometrics (Fingerprint, Face ID)	Inherence	High	Mobile devices, Windows Hello

Recommended Method: Authenticator app (e.g., Microsoft Authenticator, Google Authenticator, Authy)

Not Permitted: - Email-based codes (too insecure) - Security questions (vulnerable to social engineering)

23.2.3 2.3 MFA Registration

Onboarding: 1. New employees register MFA on first working day 2. IT support assists with setup 3. Register at least 2 MFA methods (primary + backup) 4. Generate backup codes and store securely

Self-Service: - Users can manage MFA methods via self-service portal - Changing MFA methods requires re-authentication - Loss of MFA device: IT support process for reset

23.2.4 2.4 MFA Bypass and Emergency Access

Break-Glass Accounts: - Emergency accounts without MFA for system recovery - Secured in safe, only for emergencies - Usage is immediately escalated to CISO - Change password after each use

Temporary MFA Bypass: - Only in exceptional cases (e.g., device loss) - Approval by IT security required - Maximum 24 hours, then automatic suspension - Increased monitoring during bypass period

23.3 3. Password Policies

23.3.1 3.1 Password Complexity

Requirements for Standard Users: - **Minimum Length:** 12 characters - **Complexity:** At least 3 of 4 character types: - Uppercase letters (A-Z) - Lowercase letters (a-z) - Digits (0-9) - Special characters (!@#$%^&*) - **No Dictionary Words:** Password must not be in common password list - **No Personal Information:** No name, date of birth, username

Requirements for Privileged Users: - **Minimum Length:** 16 characters - **Complexity:** All 4 character types required - **Passphrase Recommended:** E.g., "Coffee!Morning@2024#Secure"

Technical Enforcement: - Active Directory Group Policy Objects (GPOs) - Azure AD Password Protection - Password filter for common password checking

23.3.2 3.2 Password Change

Regular Change: - **Standard Users:** Every 90 days (optional if MFA active) - **Privileged Users:** Every 60 days (mandatory) - **Service Accounts:** Every 180 days or upon personnel change

Forced Change: - At first login (initial password) - After password reset by IT support - When compromise is suspected - After security incidents

Password History: - Last 12 passwords cannot be reused - Prevents rotation between few passwords

23.3.3 3.3 Password Reset

Self-Service Password Reset (SSPR): - Users can reset password themselves via {{ meta.iam.sspr_url }} - Verification via: - MFA method (authenticator app, SMS) - Alternative email address - Security questions (only as fallback) - Audit log for all password resets

IT Support Reset: - When all SSPR methods are lost - Identity verification required (ID card, employee ID) - Temporary password, must be changed at first login - Documentation in ticket system

Emergency Reset: - For locked accounts outside business hours - On-call IT support available - Enhanced verification (supervisor confirmation)

23.3.4 3.4 Password Manager

Recommendation: - Use of password manager for all users - Enterprise solution: {{ meta.security.password_manager }} (e.g., 1Password, Bitwarden) - Central management of shared credentials

Features: - Generation of strong, random passwords - Secure encrypted storage - Browser integration for auto-fill - Sharing of credentials within team (encrypted) - Audit log for access

Training: - Onboarding training for new employees - Best practices for password manager usage - Avoiding password reuse

23.4 4. Session Management

23.4.1 4.1 Session Timeouts

Inactivity Timeouts:

System Type	Timeout	Justification
Workstation (local)	15 minutes	Physical access possible
VPN Connection	8 hours	Remote access, re-auth daily

System Type	Timeout	Justification
Web Applications	30 minutes	Balance between security and usability
Privileged Sessions	10 minutes	Elevated risk
Mobile Apps	5 minutes	Device loss risk

Absolute Session Limits: - **Standard Users:** Max. 12 hours, then re-authentication - **Privileged Users:** Max. 4 hours, then re-authentication - **Remote Access:** Max. 8 hours, then re-authentication

23.4.2 4.2 Screen Lock

Automatic Lock: - After inactivity timeout (see above) - Unlock only with password or biometrics - No display of sensitive information on lock screen

Manual Lock: - Users must lock workstation when leaving (Windows+L, Ctrl+Alt+Del) - Awareness campaigns on "Clean Desk Policy" - Spot checks by security team

23.4.3 4.3 Concurrent Sessions

Limits: - **Standard Users:** Max. 3 concurrent sessions - **Privileged Users:** Max. 2 concurrent sessions - **Service Accounts:** Max. 1 session (prevents credential sharing)

Monitoring: - Alerts for unusual session patterns - Automatic suspension on suspected account sharing - Geolocation checks (impossible travel)

23.4.4 4.4 Session Security

Technical Controls: - **Session Tokens:** Cryptographically secure, random tokens - **Token Rotation:** New tokens after re-authentication - **Secure Cookies:** HttpOnly, Secure, SameSite flags - **Session Fixation Protection:** New session ID after login - **HTTPS Enforcement:** All sessions over encrypted connections

23.5 5. Authentication Methods

23.5.1 5.1 Single Sign-On (SSO)

Implementation: - **Identity Provider:** {{ meta.iam.idp }} (e.g., Azure AD, Okta) - **Protocols:** SAML 2.0, OAuth 2.0, OpenID Connect - **Applications:** All cloud SaaS applications via SSO

Benefits: - Single login for all applications - Central authentication and MFA - Reduced password fatigue - Simplified offboarding (central suspension)

Conditional Access: - Risk-based authentication - Device compliance checks - Geolocation-based policies - MFA enforcement at elevated risk

23.5.2 5.2 Certificate-Based Authentication

Use Cases: - Machine-to-machine authentication - VPN access (in addition to MFA) - Wireless network (802.1X) - Code signing and email encryption

PKI Infrastructure: - Internal Certificate Authority (CA): {{ meta.pki.ca }} - Certificate lifecycle management - Automatic renewal before expiration - Revocation checks (CRL, OCSP)

23.5.3 5.3 Biometric Authentication

Supported Methods: - **Windows Hello for Business:** Fingerprint, facial recognition - **Mobile Devices:** Touch ID, Face ID - **Only as Second Factor:** Biometrics do not replace password

Data Protection: - Biometric data stored locally on device (not centrally) - No transmission of raw biometric data - GDPR-compliant processing

23.6 6. Service Accounts and Technical Accounts

23.6.1 6.1 Service Account Policies

Requirements: - **No Interactive Logins:** Service accounts must not be used for human logins - **Strong Passwords:** At least 24 characters, randomly generated - **Password Rotation:** Every 180 days or upon personnel change - **Documentation:** Purpose, owner, systems used

Management: - Central management in password manager or PAM system - CISO approval for new service accounts - Regular reviews (quarterly) - Deactivation of unused accounts

23.6.2 6.2 API Keys and Tokens

Best Practices: - **Rotation:** Rotate API keys every 90 days - **Least Privilege:** Minimal permissions for API keys - **Secrets Management:** Storage in secrets manager (e.g., HashiCorp Vault, Azure Key Vault) - **No Hardcoding:** API keys not in code or config files

Monitoring: - Logging of all API access - Alerts for unusual API usage patterns - Rate limiting for API calls

23.7 7. Monitoring and Alerting

23.7.1 7.1 Authentication Monitoring

Monitored Events: - Failed login attempts (brute-force detection) - Successful logins from unusual locations - MFA bypass attempts - Password resets (especially privileged accounts) - Concurrent sessions from different IPs

Automatic Alerts: - **5 failed logins:** Warning to user - **10 failed logins:** Account lockout (30 minutes) - **Login from new device/location:** MFA challenge - **Impossible travel:** Alert to security team (e.g., login in Germany, 1 hour later in USA)

23.7.2 7.2 Account Lockout

Automatic Lockout: - After 10 failed login attempts - Lockout duration: 30 minutes (automatic unlock) - Manual unlock by IT support possible

Privileged Accounts: - Already after 5 failed attempts - Manual unlock only by CISO or IT security - Investigation upon lockout (possible attack)

23.8 8. Compliance and Audit

23.8.1 8.1 Key Performance Indicators (KPIs)

Metric	Target Value	Measurement
MFA Adoption Rate	> 99%	IAM system
Password Complexity Compliance	100%	AD reports
Failed Logins	< 100 per day	SIEM
Password Resets	< 50 per month	IAM system
Session Timeout Compliance	> 95%	Endpoint monitoring

23.8.2 8.2 Audit Evidence

Documentation: - Authentication logs (success and failure) - MFA registrations and usage - Password changes and resets - Account lockouts and unlocks - Privileged access

Retention: - Authentication logs: {{ meta.retention.log_years }} years - Audit trails: {{ meta.retention.audit_years }} years

23.9 9. References

23.9.1 Internal Documents

- `0240_Policy_Authentication_and_Passwords.md` - Parent policy
- `0230_Richtlinie_IAM_Joiner_Mover_Leaver_und_Zugriffsantraege.md` - IAM processes
- `0320_Policy_Logging_und_Monitoring.md` - Logging policy

23.9.2 External Standards

- **ISO/IEC 27001:2022 Annex A.5.17** - Authentication information
- **ISO/IEC 27001:2022 Annex A.5.18** - Access rights
- **NIST SP 800-63B** - Digital Identity Guidelines (Authentication)
- **OWASP Authentication Cheat Sheet**

Approved by:
Thomas Weber, CISO
Date: {{ meta.document.approval_date }}

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

ewpage

Chapter 24

Policy: Cryptography and Key Management

Document ID: 0260
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.8.24 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

24.1 1. Purpose

This policy defines the principles for the use of cryptographic procedures and the management of cryptographic keys at **AdminSend GmbH**. It ensures that information is protected by appropriate cryptographic controls and keys are managed securely.

24.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Systems:** All IT systems, applications, databases, networks, cloud services
- **Data:** All data at rest, in transit, and in use
- **Cryptographic Procedures:** Encryption, hashing, digital signatures, certificates
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Ausnahmen_und_`

24.3 3. Principles (Policy Statements)

24.3.1 3.1 Risk-Based Use of Cryptography

Cryptographic procedures are deployed based on risk analysis. The protection requirements of information determine the strength and type of cryptographic controls.

24.3.2 3.2 Encryption of Sensitive Data

Sensitive and confidential data is encrypted both at rest and in transit: - **Data at Rest:** Encryption of databases, file systems, backups, mobile devices - **Data in Transit:** TLS/SSL for network communication, VPN for remote access - **Data in Use:** Encryption in memory where technically feasible (e.g., confidential computing)

24.3.3 3.3 Use of Recognized Algorithms

Only recognized and standardized cryptographic algorithms are used: - Symmetric encryption: AES-256 or higher - Asymmetric encryption: RSA-2048 or higher, ECC with at least 256 bits - Hashing: SHA-256 or higher - Deprecated algorithms (MD5, SHA-1, DES, 3DES) are prohibited

24.3.4 3.4 Key Management Lifecycle

Cryptographic keys are managed securely throughout their entire lifecycle: - **Generation:** Secure random number generators, sufficient key length - **Storage:** Hardware Security Modules (HSM), Key Management Systems (KMS) - **Distribution:** Secure transmission channels, authentication of recipients - **Rotation:** Regular key rotation based on risk and compliance requirements - **Archiving:** Secure retention for decryption of historical data - **Destruction:** Secure deletion of keys no longer needed

24.3.5 3.5 Separation of Keys and Data

Cryptographic keys are stored separately from encrypted data. Keys must not be stored in plaintext in configuration files or source code.

24.3.6 3.6 Certificate Management

Digital certificates are managed centrally: - Use of trusted Certificate Authorities (CA) - Regular review and renewal of certificates - Monitoring of expiring certificates - Secure storage of private keys

24.3.7 3.7 Cryptographic Protocols

Secure cryptographic protocols are used for communication: - TLS 1.2 or higher (TLS 1.3 preferred) - SSH-2 for secure remote access - IPsec for VPN connections - Deprecated protocols (SSL, TLS 1.0/1.1) are prohibited

24.3.8 3.8 Compliance with Export Controls

The use of cryptography complies with national and international export control regulations.

24.4 4. Roles and Responsibilities

24.4.1 RACI Matrix: Cryptography and Key Management

Activity	CISO	IT Operations	Crypto Officer	Development	Compliance
Policy Creation	R/A	C	C	C	C
Crypto Architecture	A	C	R	C	I
Key Generation	C	R	R/A	I	I
Key Rotation	C	R	R/A	I	I
Certificate Management	C	R	R/A	I	I
Crypto Monitoring	A	C	R	I	C
Compliance Review	C	I	C	I	R/A

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

24.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **Crypto Officer:** {{ meta.it.crypto_officer }}
- **Key Management Responsible:** {{ meta.it.key_manager }}
- **Implementation Responsible:** IT operations, development
- **Control/Audit Function:** ISMS, internal audit, compliance

24.5 5. Derivations (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

24.5.1 Related Guidelines

- **0270_Richtlinie_Key_Management_und_Verschluesselung.md** - Detailed implementation guideline
- `0280_Policy_Datenklassifizierung_und_Informationshandling.md` - Data classification policy
- `0460_Policy_Lieferanten_und_Cloud_Sicherheit.md` - Cloud security policy
- `0600_Policy_Netzwerksicherheit.md` - Network security policy

24.5.2 Related Standards/Baselines

- Cryptographic algorithms standard

- Key length requirements
- TLS/SSL configuration standard
- Certificate lifecycle standard

24.5.3 Related Processes

- Key generation and rotation process
- Certificate renewal process
- Incident response for key compromise
- Crypto agility process (migration to new algorithms)

24.6 6. Compliance, Monitoring, and Enforcement

24.6.1 Metrics and KPIs

- Number of encrypted systems and databases
- Encryption rate of sensitive data (target: 100%)
- Number of expiring certificates (target: 0 expired certificates)
- Average key rotation time
- Number of violations of crypto standards
- Number of compromised keys

24.6.2 Evidence and Proof

- Encryption inventory
- Key management logs
- Certificate register
- Crypto compliance reports
- Penetration test results
- Audit reports on cryptographic controls

24.6.3 Consequences for Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Use of weak algorithms:** Immediate remediation, retraining - **Insecure key storage:** Immediate key rotation, investigation - **Key compromise:** Incident response, revocation, forensic analysis - **Repeated violations:** Employment law consequences

24.7 7. Exceptions

Exceptions to this policy are only permitted in justified exceptional cases:

- **Exception Process:** See `0640_Policy_Ausnahmen_und_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and crypto officer
- **Documentation:** All exceptions are documented in the risk register
- **Time Limit:** Exceptions are generally time-limited and regularly reviewed
- **Compensating Controls:** Exceptions require alternative security measures

24.8 8. References

24.8.1 Internal Documents

- `0010_ISMS_Informationssicherheitsleitlinie.md` - ISMS policy
- `0270_Richtlinie_Key_Management_und_Verschluesselung.md` - Detailed guideline
- `0280_Policy_Datenklassifizierung_und_Informationshandling.md` - Data classification policy
- `0080_ISMS_Risikoregister_Template.md` - Risk register

24.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.8.24** - Use of cryptography
- **ISO/IEC 27002:2022** - Information security controls
- **NIST SP 800-57** - Recommendation for Key Management
- **NIST SP 800-175B** - Guideline for Using Cryptographic Standards
- **BSI TR-02102** - Cryptographic Procedures: Recommendations and Key Lengths
- **FIPS 140-2/140-3** - Security Requirements for Cryptographic Modules
- **eIDAS Regulation (EU 910/2014)** - Electronic Identification and Trust Services

---

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 25

Guideline: Key Management and Encryption

Document ID: 0270
Document Type: Guideline (detailed)
Related Policy: 0260_Policy_Cryptography_and_Key_Management.md
Standard Reference: ISO/IEC 27001:2022 Annex A.8.24
Owner: {{ meta.it_operations.manager }}
Version: 1.0
Status: Approved
Classification: Confidential
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

25.1 1. Purpose and Scope

This guideline implements the `0260_Policy_Cryptography_and_Key_Management.md` and defines detailed procedures for: - Cryptographic algorithms and standards - Key generation, storage, and rotation - Certificate management - Encryption of data at rest and in transit

Scope: All cryptographic systems at **AdminSend GmbH**

25.2 2. Cryptographic Standards

25.2.1 2.1 Approved Algorithms

Symmetric Encryption: - **AES-256** (Advanced Encryption Standard, 256-bit) - Recommended - **AES-128** - Acceptable for non-critical data - **ChaCha20** - Acceptable for mobile devices

Asymmetric Encryption: - **RSA-4096** - Recommended for long-term security - **RSA-2048** - Acceptable, minimum requirement - **ECDSA P-384** - Recommended for performance - **Ed25519** - Acceptable for SSH keys

Hash Functions: - **SHA-256** - Minimum requirement - **SHA-384, SHA-512** - Recommended for critical applications - **BLAKE2** - Acceptable

Prohibited Algorithms: - MD5, SHA-1 (cryptographically broken) - DES, 3DES (deprecated) - RSA $<$ 2048 bit (too weak) - RC4 (insecure)

25.2.2 2.2 TLS/SSL Configuration

TLS Versions: - **TLS 1.3** - Recommended - **TLS 1.2** - Minimum requirement - **TLS 1.1, 1.0, SSL** - Prohibited

Cipher Suites (Recommended):

```
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_AES_128_GCM_SHA256
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES128-GCM-SHA256
```

Certificates: - Minimum RSA-2048 or ECDSA P-256 - Validity period: Max. 13 months (398 days) - Trusted Certificate Authorities (CAs)

25.3 3. Key Management

25.3.1 3.1 Key Generation

Requirements: - Cryptographically secure random number generators (CSPRNG) - Key lengths per section 2.1 - Generation in secure environment (HSM, Key Vault)

Process: 1. Key request via ticket system 2. Approval by CISO or IT security 3. Generation by Key Management System 4. Secure handover to requester 5. Documentation in key register

25.3.2 3.2 Key Storage

Hardware Security Modules (HSM): - Critical keys (Root CA, master keys) in HSM: {{ meta.security.hsm }} - FIPS 140-2 Level 2 or higher - Physical security and access control

Key Management Systems: - **Cloud:** {{ meta.cloud.key_vault }} (e.g., Azure Key Vault, AWS KMS) - **On-Premises:** {{ meta.security.kms }} (e.g., HashiCorp Vault) - Encrypted storage - Audit logging of all access

Prohibited: - Storage in plaintext - Hardcoding in source code - Storage in configuration files - Transmission via email or chat

25.3.3 3.3 Key Rotation

Rotation Intervals:

Key Type	Rotation	Justification
Data Encryption Keys (DEK)	Annually	Balance between security and effort

Key Type	Rotation	Justification
Key Encryption Keys (KEK)	Every 2 years	Rarely used, higher security
TLS Certificates	Every 12 months	CA requirements
API Keys	Every 90 days	Frequent use, higher risk
SSH Keys	Every 180 days	Administrative access

Automation: - Automatic rotation where possible (cloud services) - Notifications 30 days before expiration - Documentation of all rotations

Emergency Rotation: - On suspected compromise: Immediate rotation - On personnel change: Rotation of all affected keys - On security incidents: Rotation per incident response

25.3.4 3.4 Key Destruction

Process: 1. Mark key as "deprecated" 2. Grace period (30 days) for data decryption 3. Secure deletion from all systems 4. Documentation of destruction

Methods: - Cryptographic overwriting (multiple passes) - HSM: Secure erase function - Physical media: Destruction per DIN 66399

25.4 4. Certificate Management

25.4.1 4.1 Public Key Infrastructure (PKI)

Components: - **Root CA:** {{ meta.pki.root_ca }} (Offline, HSM-protected) - **Issuing CA:** {{ meta.pki.issuing_ca }} (Online, for certificate issuance) - **Certificate Management System:** {{ meta.pki.cms }}

Certificate Types: - **Server Certificates:** Web servers, API endpoints - **Client Certificates:** User authentication, VPN - **Code Signing:** Software signing - **Email Certificates:** S/MIME encryption

25.4.2 4.2 Certificate Lifecycle

Issuance: 1. Create Certificate Signing Request (CSR) 2. Submit request via PKI portal 3. Validation by Certificate Authority 4. Issue and provide certificate 5. Installation and configuration

Renewal: - Automatic notification 60 days before expiration - Renewal 30 days before expiration - Automation via ACME protocol (Let's Encrypt)

Revocation: - On compromise: Immediate revocation - On personnel change: Revocation of all personal certificates - Publication in Certificate Revocation List (CRL) - OCSP (Online Certificate Status Protocol) for real-time checks

25.4.3 4.3 Certificate Inventory

Documentation: - All issued certificates in CMDB - Expiration dates, purpose, owner - Automatic scans for unknown certificates

Monitoring: - Daily check for expiring certificates - Alerts for certificates < 30 days validity - Automatic renewal where possible

25.5 5. Data Encryption

25.5.1 5.1 Data at Rest

Encryption Requirement: - All confidential and highly confidential data - Personal data (GDPR requirement) - Financial data and trade secrets - Backups and archived data

Methods:

Storage Location	Method	Key Management
Laptops/Desktops	BitLocker (Windows), FileVault (macOS)	TPM + Recovery Key in Key Vault
Server Disks	LUKS (Linux), BitLocker (Windows)	Key Vault
Databases	Transparent Data Encryption (TDE)	Database Key Management
Cloud Storage	Server-Side Encryption (SSE)	Cloud Key Management Service
File Servers	Encrypted File System (EFS)	Active Directory + Key Vault

Configuration: - AES-256 for all encryption - Automatic encryption on storage - No user interaction required

25.5.2 5.2 Data in Transit

Encryption Requirement: - All data transmission over public networks - Internal transmission of confidential data - API communication - Email with confidential content

Methods:

Transmission Type	Protocol	Configuration
Web Traffic	HTTPS (TLS 1.2+)	See section 2.2
Email	TLS (SMTP), S/MIME	Opportunistic TLS + encryption for confidential
File Transfer	SFTP, FTPS, HTTPS	No unencrypted protocols
VPN	IPsec, WireGuard	AES-256, Perfect Forward Secrecy
Database	TLS for connections	Enforced encryption

Prohibited Protocols: - FTP (unencrypted) - Telnet (unencrypted) - HTTP for confidential data - SMTP without TLS for confidential emails

25.5.3 5.3 Data in Use

Technologies: - **Confidential Computing:** Encryption during processing (Intel SGX, AMD SEV) - **Homomorphic Encryption:** Computations on encrypted data (experimental) - **Secure Enclaves:** Isolated processing environments

Use Cases: - Processing highly sensitive data in cloud - Multi-party computation - Privacy-preserving analytics

25.6 6. Email Encryption

25.6.1 6.1 S/MIME

Implementation: - S/MIME certificates for all employees - Automatic encryption for emails with "Confidential" classification - Signing of all outgoing emails

Configuration: - Outlook, Thunderbird: S/MIME plugin - Mobile devices: Native S/MIME support - Certificate distribution via Active Directory

25.6.2 6.2 Opportunistic TLS

SMTP TLS: - All email servers support STARTTLS - Enforced encryption for known partners - Fallback to unencrypted only for non-confidential emails

MTA-STS (Mail Transfer Agent Strict Transport Security): - Policy publication via DNS - Enforcement of TLS for incoming emails

25.7 7. Backup Encryption

Requirements: - All backups encrypted (AES-256) - Separate keys for backups (not production keys) - Offline copy of backup keys (safe)

Process: 1. Backup creation with encryption 2. Store key in Key Vault 3. Offline copy of key in safe 4. Regular restore tests (quarterly)

Disaster Recovery: - Backup keys in emergency documentation - Access only by authorized persons - Four-eyes principle for key access

25.8 8. Cloud Encryption

25.8.1 8.1 Cloud Storage

Configuration: - **Azure:** Customer-Managed Keys (CMK) in Azure Key Vault - **AWS:** Customer Master Keys (CMK) in AWS KMS - **Google Cloud:** Customer-Managed Encryption Keys (CMEK)

Benefits: - Control over keys - Ability to rotate keys - Compliance requirements met

25.8.2 8.2 Cloud Databases

Encryption: - Transparent Data Encryption (TDE) enabled - Encrypted connections (TLS) - Customer-managed keys for critical databases

25.9 9. Compliance and Audit

25.9.1 9.1 Key Performance Indicators (KPIs)

Metric	Target Value	Measurement
Encrypted Laptops	100%	Endpoint Management
TLS 1.2+ Usage	100%	Web Server Logs
Certificate Expiration Incidents	0 per year	PKI Monitoring
Key Rotation Compliance	$> 95\%$	Key Management System

25.9.2 9.2 Audit Evidence

Documentation: - Cryptography policy and guidelines - Key register and inventory - Certificate inventory - Encryption configurations - Audit logs for key access

25.10 10. References

25.10.1 Internal Documents

- `0260_Policy_Cryptography_and_Key_Management.md` - Parent policy
- `0420_Policy_Backup_und_Wiederherstellung.md` - Backup policy

25.10.2 External Standards

- **ISO/IEC 27001:2022 Annex A.8.24** - Use of cryptography
- **NIST SP 800-57** - Key Management Recommendations
- **NIST SP 800-52** - TLS Guidelines
- **BSI TR-02102** - Cryptographic Procedures

Approved by:
Thomas Weber, CISO
Date: {{ meta.document.approval_date }}

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

ewpage

Chapter 26

Policy: Data Classification and Information Handling

Document ID: 0280
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.5.12-A.5.14 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

26.1 1. Purpose

This policy defines the principles for data classification and information handling at **AdminSend GmbH**. It ensures that information is classified according to its sensitivity and protection requirements, labeled appropriately, and protected throughout its entire lifecycle.

26.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Information:** All information in any form (digital, physical, verbal)
- **Systems:** All IT systems, applications, databases, storage media
- **Persons:** All employees, contractors, suppliers, and third parties with access to information
- **Lifecycle:** Creation, storage, processing, transmission, archiving, destruction
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Ausnahmen_und_`

26.3 3. Principles (Policy Statements)

26.3.1 3.1 Mandatory Classification

All organizational information must be classified. Classification is performed by the information owner based on confidentiality, integrity, and availability.

26.3.2 3.2 Classification Levels

The organization uses the following classification levels: - **Public:** Information that is or may be publicly accessible - **Internal:** Information for internal use, not intended for the public - **Confidential:** Sensitive information whose disclosure could harm the organization - **Highly Confidential:** Highly sensitive information with the highest protection requirements

26.3.3 3.3 Labeling and Marking

Classified information is labeled accordingly: - Digital documents: Metadata, headers/footers, watermarks - Physical documents: Stamps, stickers, cover sheets - Emails: Subject prefix, banner - Storage media: Labels

26.3.4 3.4 Handling Requirements

Specific handling requirements apply to each classification level: - Access control and permissions - Encryption (at rest, in transit) - Storage and archiving - Transmission and sharing - Destruction and deletion

26.3.5 3.5 Information Owner Responsibility

Each piece of information has a defined information owner who is responsible for: - Classifying the information - Defining access rights - Regular review of classification - Approving access and sharing requests

26.3.6 3.6 Sharing and Distribution

Sharing of classified information follows the need-to-know principle: - Internal sharing: After approval by information owner - External sharing: After approval and with appropriate protective measures (NDA, encryption) - Cloud storage: Only in approved cloud services with adequate security controls

26.3.7 3.7 Secure Destruction

Information is securely destroyed at the end of its lifecycle: - Digital data: Secure deletion (overwriting, degaussing) - Physical documents: Shredding, burning - Storage media: Physical destruction for highly sensitive data

26.3.8 3.8 Data Protection Compliance

Classification and handling of personal data complies with GDPR and other data protection regulations.

26.4 4. Roles and Responsibilities

26.4.1 RACI Matrix: Data Classification and Information Handling

Activity	CISO	Information Owner	Employee	IT Operations	Data Protection Officer
Policy Creation	R/A	C	I	C	C
Classification	C	R/A	I	I	C
Labeling	I	A	R	C	I
Access Approval	C	R/A	I	I	C
Handling Compliance	A	R	R	C	C
Sharing Approval	C	R/A	I	I	C
Secure Destruction	C	A	I	R	C
Monitoring and Audits	R/A	C	I	C	C

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

26.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **Information Owners:** Department heads, system owners
- **Data Protection Officer:** {{ meta.dpo.name }}
- **Implementation Responsible:** All employees, IT operations
- **Control/Audit Function:** ISMS, internal audit, DPO

26.5 5. Derivations (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

26.5.1 Related Guidelines

- **0290_Richtlinie_Datenklassifizierung_Labeling_und_Handling.md** - Detailed implementation guideline
- `0260_Policy_Kryptografie_und_Schluesselmanagement.md` - Cryptography policy
- `0560_Policy_Datenschutz_Schnittstellen.md` - Data protection policy
- `0580_Policy_Aufbewahrung_und_Loeschung.md` - Retention and deletion policy

26.5.2 Related Standards/Baselines

- Classification scheme and handling matrix
- Labeling standards (digital and physical)
- Encryption requirements per classification level
- Destruction standards

26.5.3 Related Processes

- Classification process
- Information owner assignment
- Sharing and distribution approval process
- Secure destruction process

26.6 6. Compliance, Monitoring, and Enforcement

26.6.1 Metrics and KPIs

- Percentage of classified information (target: 100%)
- Percentage of correctly labeled documents
- Number of handling requirement violations
- Number of unauthorized disclosures
- Average time to classify new information
- Compliance rate with destruction requirements

26.6.2 Evidence and Proof

- Classification register
- Information owner assignments
- Sharing approvals
- Destruction certificates
- DLP (Data Loss Prevention) logs
- Audit reports on classification and handling

26.6.3 Consequences for Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Missing classification:** Retraining, correction - **Incorrect labeling:** Correction, retraining - **Unauthorized disclosure:** Warning up to termination, possible legal action - **Improper destruction:** Investigation, retraining - **Repeated violations:** Employment law consequences

26.7 7. Exceptions

Exceptions to this policy are only permitted in justified exceptional cases:

- **Exception Process:** See `0640_Policy_Ausnahmen_und_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and information owner
- **Documentation:** All exceptions are documented in the risk register
- **Time Limit:** Exceptions are generally time-limited and regularly reviewed
- **Compensating Controls:** Exceptions require alternative security measures

26.8 8. References

26.8.1 Internal Documents

- `0010_ISMS_Informationssicherheitsleitlinie.md` - ISMS policy
- `0290_Richtlinie_Datenklassifizierung_Labeling_und_Handling.md` - Detailed guideline
- `0300_Policy_Asset_Management.md` - Asset management policy
- `0080_ISMS_Risikoregister_Template.md` - Risk register

26.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.5.12** - Classification of information
- **ISO/IEC 27001:2022 Annex A.5.13** - Labelling of information
- **ISO/IEC 27001:2022 Annex A.5.14** - Information transfer
- **ISO/IEC 27002:2022** - Information security controls
- **GDPR (EU 2016/679)** - General Data Protection Regulation
- **BSI IT-Grundschutz** - Module CON.6 Deletion and Destruction

---

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 27

Guideline: Data Classification, Labeling and Handling

Document ID: 0290
Document Type: Guideline (detailed)
Related Policy: 0280_Policy_Data_Classification_and_Information_Handling.md
Standard Reference: ISO/IEC 27001:2022 Annex A.5.12, A.5.13
Owner: {{ meta.it_operations.manager }}
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}

27.1 1. Purpose and Scope

This guideline implements the `0280_Policy_Data_Classification_and_Information_Handling.md` and defines: - Classification levels and criteria - Labeling procedures for documents and emails - Handling requirements per classification level

Scope: All information at **AdminSend GmbH**

27.2 2. Classification Levels

27.2.1 2.1 Public

Definition: Information intended for public distribution

Examples: - Marketing materials, press releases - Public website content - Product documentation

Handling: - No access restrictions - No encryption required - Free distribution permitted

27.2.2 2.2 Internal

Definition: Information for internal use, not for the public

Examples: - Internal process documentation - Organizational structures - General business communication

Handling: - Access only for employees and authorized third parties - No encryption required (except for external transmission) - Sharing with third parties only with NDA

27.2.3 2.3 Confidential

Definition: Sensitive business information, damage upon disclosure

Examples: - Contracts, proposals - Personnel data - Financial reports (internal) - Customer data

Handling: - Access only on need-to-know basis - Encryption for transmission and storage - Sharing only with approval - Secure destruction required

27.2.4 2.4 Highly Confidential

Definition: Highly sensitive information, significant damage upon disclosure

Examples: - Trade secrets, M&A plans - Strategic plans - Security concepts - Critical infrastructure data

Handling: - Access only for authorized persons (explicit approval) - Encryption mandatory (at rest and in transit) - No email transmission without encryption - Physical documents in safe - Secure destruction per DIN 66399 P-5

27.3 3. Classification Process

27.3.1 3.1 Responsibilities

Data Owner: - Classification of new information - Review and adjustment upon changes - Approval of access

Creator: - Application of classification during document creation - Labeling per guidelines - Compliance with handling requirements

IT Operations: - Technical implementation (DLP, encryption) - Monitoring and compliance checks

27.3.2 3.2 Classification Criteria

Questions for Determination: 1. What damage occurs upon disclosure? 2. Are there legal/regulatory requirements? 3. Who needs access (public, employees, specific persons)? 4. How long must data be retained?

Decision Tree: - Intended for public? → Public - Only internally relevant? → Internal - Business damage upon disclosure? → Confidential - Significant damage or legal obligation? → Highly Confidential

27.4 4. Labeling Procedures

27.4.1 4.1 Documents

Microsoft Office: - Sensitivity labels in Office 365 - Automatic application via DLP rules - Header/footer with classification

PDF: - Watermark with classification - Metadata tags

Physical Documents: - Stamp or print on each page - Color coding (e.g., red for Highly Confidential)

27.4.2 4.2 Emails

Subject Line: - Prefix: [CONFIDENTIAL], [HIGHLY CONFIDENTIAL] - Automatic via email client

Email Body: - Disclaimer in footer - Encryption for Confidential/Highly Confidential

Outlook Integration: - Sensitivity labels - Automatic encryption upon classification

27.4.3 4.3 Digital Assets

File Systems: - Metadata tags - Separate folder structures per classification - Access control via ACLs

Databases: - Column-level classification - Row-level security - Audit logging for access

27.5 5. Handling Requirements

27.5.1 5.1 Storage

Classification	Storage Location	Encryption	Access Control
Public	Any	Optional	None
Internal	Approved systems	For external storage	Employees
Confidential	Approved systems	Mandatory	Need-to-know
Highly Confidential	Dedicated systems	Mandatory (AES-256)	Explicit approval

27.5.2 5.2 Transmission

Classification	Email	File Transfer	Physical
Public	Unencrypted OK	Any	No requirements
Internal	TLS recommended	SFTP/HTTPS	Sealed envelopes
Confidential	S/MIME mandatory	SFTP/HTTPS encrypted	Registered mail, sealed

Classification	Email	File Transfer	Physical
Highly Confidential	S/MIME + approval	Dedicated channels	Courier, personal handover

27.5.3 5.3 Destruction

Classification	Digital	Paper	Storage Media
Public	Normal deletion	Trash	Normal deletion
Internal	Secure deletion	Shredder P-3	Secure deletion
Confidential	Cryptographic deletion	Shredder P-4	Degaussing + destruction
Highly Confidential	Cryptographic deletion	Shredder P-5	Physical destruction

27.6 6. Data Loss Prevention (DLP)

27.6.1 6.1 DLP Rules

Automatic Detection: - Credit card numbers, social security numbers - Documents with "Confidential" label - Personal data (GDPR)

Actions: - **Warning:** When sending Internal-classified data externally - **Blocking:** When sending Confidential/Highly Confidential without encryption - **Quarantine:** On suspected data leak

27.6.2 6.2 Monitoring

Monitored Channels: - Email (outgoing) - Cloud uploads (OneDrive, SharePoint) - USB devices - Printers

Alerts: - Automatic notification to security team - Incident creation for critical violations

27.7 7. Training and Awareness

Mandatory Training: - Onboarding: Data classification basics - Annually: Refresher and updates

Awareness Materials: - Posters with classification levels - Quick reference cards - Intranet articles

27.8 8. Compliance and Audit

27.8.1 8.1 Key Performance Indicators (KPIs)

Metric	Target Value
Classified Documents	$> 80\%$
DLP Incidents	< 10 per month
Training Participation	100%

27.8.2 8.2 Audit Evidence

- Classification register
- DLP logs and incidents
- Training records
- Access logs

27.9 9. References

27.9.1 Internal Documents

- `0280_Policy_Data_Classification_and_Information_Handling.md`
- `0320_Policy_Logging_und_Monitoring.md`

27.9.2 External Standards

- **ISO/IEC 27001:2022 Annex A.5.12** - Classification of information
- **ISO/IEC 27001:2022 Annex A.5.13** - Labelling of information
- **DIN 66399** - Destruction of data carriers

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 28

Policy: Asset Management

Document ID: 0300
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.5.9-A.5.11 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

28.1 1. Purpose

This policy defines the principles for asset management and inventory control at **AdminSend GmbH**. It ensures that all information assets are identified, documented, classified, and appropriately protected throughout their entire lifecycle.

28.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Asset Types:** Hardware, software, data, information, services, people, intangible assets
- **Systems:** All IT systems, network components, endpoints, servers, cloud resources
- **Lifecycle:** Procurement, commissioning, operation, maintenance, decommissioning, disposal
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Ausnahmen_und_`

28.3 3. Principles (Policy Statements)

28.3.1 3.1 Complete Asset Inventory

All organizational assets are recorded and documented in a central asset inventory. The inventory is regularly updated and checked for completeness.

28.3.2 3.2 Asset Owner Assignment

Each asset has a defined asset owner who is responsible for: - Asset classification - Definition of protection requirements - Approval of access and usage rights - Lifecycle management

28.3.3 3.3 Asset Classification and Tagging

Assets are classified and tagged with metadata: - Classification by protection requirements (confidentiality, integrity, availability) - Technical tags (environment, application, cost center) - Compliance tags (GDPR, PCI-DSS, etc.)

28.3.4 3.4 Lifecycle Management

Assets are managed throughout their entire lifecycle: - **Procurement:** Security requirements, approval process - **Commissioning:** Configuration, hardening, documentation - **Operation:** Maintenance, patching, monitoring - **Decommissioning:** Data deletion, decommissioning - **Disposal:** Secure destruction, recycling

28.3.5 3.5 Acceptable Use

Assets may only be used for approved business purposes. Personal use is only permitted within the framework of the Acceptable Use Policy (`0200_Policy_Akzeptable_Nutzung_IT.md`).

28.3.6 3.6 Return of Assets

Upon role change or departure, all assets must be returned. The return process is part of the leaver process.

28.3.7 3.7 Protection Against Loss and Theft

Assets are protected against loss, theft, and unauthorized access through appropriate measures: - Physical security (access control, alarm systems) - Encryption of mobile devices - Remote wipe functionality - Insurance of critical assets

28.3.8 3.8 Secure Disposal

Assets are securely disposed of at the end of their lifecycle: - Data deletion per recognized standards - Physical destruction for highly sensitive data - Environmentally responsible recycling - Documentation of disposal

28.4 4. Roles and Responsibilities

28.4.1 RACI Matrix: Asset Management

Activity	CISO	Asset Owner	IT Operations	Procurement	Facility Management
Policy Creation	R/A	C	C	C	I
Asset Inventory	A	R	R	C	C
Asset Owner Assignment	C	R/A	I	I	I
Classification	C	R/A	I	I	I
Lifecycle Management	A	R	R	C	C
Secure Disposal	C	A	R	I	R
Monitoring and Audits	R/A	C	C	I	I

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

28.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **Asset Owners:** Department heads, system owners
- **Asset Manager:** {{ meta.it.asset_manager }}
- **Implementation Responsible:** IT operations, procurement, facility management
- **Control/Audit Function:** ISMS, internal audit

28.5 5. Derivations (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

28.5.1 Related Guidelines

- **0310_Richtlinie_Asset_Inventory_Tagging_und_Entsorgung.md** - Detailed implementation guideline
- `0280_Policy_Datenklassifizierung_und_Informationshandling.md` - Data classification policy
- `0200_Policy_Akzeptable_Nutzung_IT.md` - Acceptable use policy
- `0480_Policy_Physische_Sicherheit.md` - Physical security policy

28.5.2 Related Standards/Baselines

- Asset inventory schema (CMDB)
- Tagging standards
- Disposal standards
- Lifecycle management processes

28.5.3 Related Processes

- Asset procurement process
- Asset onboarding and configuration
- Asset return process (leaver)
- Secure disposal process

28.6 6. Compliance, Monitoring, and Enforcement

28.6.1 Metrics and KPIs

- Inventory rate (target: 100% of all assets recorded)
- Number of assets without asset owner
- Number of unclassified assets
- Average time to asset registration
- Number of lost or stolen assets
- Compliance rate with disposal standards

28.6.2 Evidence and Proof

- Asset inventory (CMDB)
- Asset owner assignments
- Classification register
- Disposal certificates
- Audit reports on asset management
- Insurance certificates

28.6.3 Consequences for Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Unregistered assets:** Post-registration, retraining - **Loss of assets:** Investigation, possible cost reimbursement - **Improper disposal:** Retraining, disciplinary action - **Repeated violations:** Employment law consequences

28.7 7. Exceptions

Exceptions to this policy are only permitted in justified exceptional cases:

- **Exception Process:** See `0640_Policy_Ausnahmen_und_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and asset owner
- **Documentation:** All exceptions are documented in the risk register
- **Time Limit:** Exceptions are generally time-limited

28.8 8. References

28.8.1 Internal Documents

- `0010_ISMS_Informationssicherheitsleitlinie.md` - ISMS policy
- `0310_Richtlinie_Asset_Inventory_Tagging_und_Entsorgung.md` - Detailed guideline

- `0720_Anhang_Asset_und_Systeminventar_Template.md` - Asset inventory template
- `0080_ISMS_Risikoregister_Template.md` - Risk register

28.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.5.9** - Inventory of information and other associated assets
- **ISO/IEC 27001:2022 Annex A.5.10** - Acceptable use of information and other associated assets
- **ISO/IEC 27001:2022 Annex A.5.11** - Return of assets
- **ISO/IEC 27002:2022** - Information security controls
- **ITIL 4** - IT Asset Management
- **ISO/IEC 19770** - IT Asset Management

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 29

Guideline: Asset Inventory, Tagging and Disposal

Document ID: 0310
Document Type: Guideline (detailed)
Related Policy: 0300_Policy_Asset_Management.md
Standard Reference: ISO/IEC 27001:2022 Annex A.5.9, A.5.10
Owner: {{ meta.it_operations.manager }}
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}

29.1 1. Purpose and Scope

This guideline implements the `0300_Policy_Asset_Management.md` and defines: - Asset inventory and CMDB management - Asset tagging and labeling - Lifecycle management and disposal

Scope: All IT assets at **AdminSend GmbH**

29.2 2. Asset Categories

29.2.1 2.1 Hardware Assets

- Laptops, desktops, servers
- Network devices (switches, routers, firewalls)
- Mobile devices (smartphones, tablets)
- Peripherals (monitors, printers, scanners)
- Storage media (USB drives, external hard drives)

29.2.2 2.2 Software Assets

- Operating systems and licenses

- Application software
- Cloud subscriptions (SaaS)
- Development tools

29.2.3 2.3 Information Assets

- Databases
- File systems and shares
- Document collections
- Backup media

29.2.4 2.4 Services

- Cloud services (IaaS, PaaS, SaaS)
- Managed services
- Support contracts

29.3 3. Asset Inventory

29.3.1 3.1 CMDB (Configuration Management Database)

System: {{ meta.itsm.cmdb }} (e.g., ServiceNow, Jira Service Management)

Mandatory Fields per Asset: - Asset ID (unique) - Asset type and category - Manufacturer, model, serial number - Location, room - Owner, user - Purchase date, cost - Maintenance contract, end of support - Status (In operation, storage, defective, disposed)

Additional Fields: - IP address, MAC address (network devices) - Operating system, patch level - Installed software - Classification (criticality) - Dependencies to other assets

29.3.2 3.2 Automatic Inventory

Tools: - **Endpoint Management:** {{ meta.endpoint.management }} (e.g., Microsoft Intune, Jamf) - **Network Discovery:** {{ meta.network.discovery }} (e.g., Nmap, Lansweeper) - **Cloud Asset Inventory:** Native cloud tools (Azure Resource Graph, AWS Config)

Process: - Daily automatic scans - Comparison with CMDB - Alerts for unknown assets (shadow IT) - Automatic update of attributes

29.3.3 3.3 Manual Inventory

Occasions: - New asset procurement - Asset handover to employee - Location change - Maintenance or repair - Decommissioning

Process: 1. Physically inspect asset 2. Create/update CMDB entry 3. Attach asset tag 4. Documentation (photos if needed) 5. Handover protocol (for employee assignment)

29.4 4. Asset Tagging

29.4.1 4.1 Tagging Schema

Asset ID Format: `{{ meta.asset.id_format }}`
Example: `LAP-2024-001234` (Laptop, year, sequential number)

Prefixes: - LAP: Laptop - DSK: Desktop - SRV: Server - NET: Network device - MOB: Mobile device - PER: Peripheral

29.4.2 4.2 Physical Tags

Barcode/QR Code Labels: - Self-adhesive, tamper-proof - Placement in visible location - Contains asset ID and QR code for CMDB link

RFID Tags (optional): - For high-value assets - Automatic capture during location change - Integration with access control system

29.4.3 4.3 Digital Tags

Hostname Convention: - Format: `{{ meta.naming.hostname_format }}` - Example: `lap-jdoe-001` (type-user-number)

Metadata: - Cloud resources: Tags for owner, cost center, environment - Virtual machines: Tags for application, criticality

29.5 5. Asset Lifecycle Management

29.5.1 5.1 Procurement

Process: 1. Requirement request via ticket system 2. Approval by supervisor and IT management 3. Procurement through approved suppliers 4. Goods receipt and quality check 5. Create CMDB entry 6. Attach asset tag 7. Provision to user

Documentation: - Order, invoice - Warranty and maintenance contracts - Handover protocol

29.5.2 5.2 Operation

Maintenance: - Regular maintenance per manufacturer specifications - Documentation in CMDB - Firmware and software updates

Monitoring: - Hardware health checks - Capacity planning - End-of-life tracking

29.5.3 5.3 Decommissioning

Trigger: - End of useful life (typically 3-5 years) - Defective, not repairable - Technology change - Employee offboarding

Process: 1. Take asset out of operation 2. Back up data (if required) 3. Securely delete data (see section 6) 4. Set CMDB status to “Decommissioned” 5. Decision: Reuse, sale, or disposal

29.6 6. Secure Data Destruction

29.6.1 6.1 Data Carrier Deletion

Methods per DIN 66399:

Data Carrier	Classification	Method	Standard
HDD	Internal	Software deletion (3-pass)	DIN 66399 H-3
HDD	Confidential	Degaussing + deletion	DIN 66399 H-4
HDD	Highly Confidential	Physical destruction	DIN 66399 H-5
SSD	Internal	Secure Erase (ATA)	DIN 66399 H-3
SSD	Confidential/Highly Confidential	Cryptographic deletion + destruction	DIN 66399 H-5
USB/SD	All	Physical destruction	DIN 66399 H-4

Tools: - **Software:** DBAN, Blancco, Parted Magic - **Hardware:** Degausser, shredder

Documentation: - Deletion protocol with asset ID, date, method, executor - Certificate for third-party disposal

29.6.2 6.2 Mobile Devices

Process: 1. Remote wipe via MDM ({{ meta.mdm.system }}) 2. Factory reset on-site 3. Removal of SIM cards and SD cards 4. Physical verification of deletion 5. Documentation

29.6.3 6.3 Cloud Data

Deletion: - Logical deletion in cloud service - Wait for retention period expiration - Confirmation of final deletion by provider - Documentation (deletion confirmation)

29.7 7. Asset Disposal

29.7.1 7.1 Reuse

Internal: - Refurbishment and reinstallation - Assignment to another employee - Use as test or development device

Donation: - Data destruction per section 6 - Removal of all asset tags and company logos - Documentation of donation (tax)

29.7.2 7.2 Sale

Remarketing: - Only after complete data destruction - Sale through certified remarketing partners - Revenue documentation

29.7.3 7.3 Disposal

Certified Disposal Partners: - WEEE-certified (Waste Electrical and Electronic Equipment) - Disposal certificate required - Environmentally responsible disposal

Process: 1. Data destruction (see section 6) 2. Handover to disposal partner 3. Receive disposal certificate 4. Set CMDB status to "Disposed" 5. Archive documentation

29.8 8. Compliance and Audit

29.8.1 8.1 Key Performance Indicators (KPIs)

Metric	Target Value
CMDB Completeness	$> 95\%$
Asset Tagging Rate	100%
Inventory Discrepancies	$< 2\%$
Disposal Certificates	100%

29.8.2 8.2 Regular Inventories

Frequency: - Complete inventory: Annually - Spot checks: Quarterly - Ad-hoc on suspected loss

Process: 1. CMDB export 2. Physical on-site inspection 3. Comparison CMDB vs. reality 4. Clarification of discrepancies 5. CMDB correction 6. Report to management

29.8.3 8.3 Audit Evidence

- CMDB reports
- Asset handover protocols
- Deletion protocols
- Disposal certificates
- Inventory reports

29.9 9. References

29.9.1 Internal Documents

- `0300_Policy_Asset_Management.md`
- `0280_Policy_Data_Classification_and_Information_Handling.md`

29.9.2 External Standards

- **ISO/IEC 27001:2022 Annex A.5.9** - Inventory of information and other associated assets
- **ISO/IEC 27001:2022 Annex A.5.10** - Acceptable use of information

- **DIN 66399** - Destruction of data carriers
- **WEEE Directive** - Electrical and electronic equipment disposal

---

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 30

Policy: Logging and Monitoring

Document ID: 0320
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.8.15, A.8.16 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

30.1 1. Purpose

This policy defines the principles for logging, monitoring, and security event management at **AdminSend GmbH**. It ensures that security-relevant events are captured, monitored, and analyzed to detect, investigate, and respond to security incidents.

30.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Systems:** All IT systems, applications, network components, security systems
- **Log Sources:** Servers, workstations, network devices, firewalls, IDS/IPS, applications, databases
- **Monitoring Areas:** Security, performance, availability, compliance
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Ausnahmen_und_`

30.3 3. Principles (Policy Statements)

30.3.1 3.1 Comprehensive Logging

All security-relevant events are logged: - Authentication attempts (successful and failed) - Access to sensitive data and systems - Privileged activities (admin access, configuration changes) - Security incidents and anomalies - System and application errors

30.3.2 3.2 Centralized Log Management

Logs are centrally collected, stored, and analyzed in a SIEM (Security Information and Event Management) system. This enables correlated analysis and efficient incident response.

30.3.3 3.3 Log Integrity and Protection

Logs are protected against unauthorized modification and deletion: - Write-protected log storage - Integrity checks (hashing, digital signatures) - Access control to log systems - Encrypted transmission

30.3.4 3.4 Retention and Preservation

Logs are retained according to legal, regulatory, and business requirements: - Security logs: Minimum 12 months online, 7 years archive - Audit logs: Per compliance requirements - Performance logs: Per operational requirements

30.3.5 3.5 Proactive Monitoring and Alerting

Security-relevant events are proactively monitored and alerts are generated for anomalies: - Real-time monitoring of critical systems - Automated alerting rules - Escalation processes for critical alerts - 24/7 SOC (Security Operations Center) for critical systems

30.3.6 3.6 SIEM Use Cases and Detection Rules

SIEM systems are configured with use cases and detection rules to identify known attack patterns and anomalies: - Brute-force attacks - Privilege escalation - Data exfiltration - Malware activities - Insider threats

30.3.7 3.7 Log Analysis and Forensics

Logs are regularly analyzed and used for forensic investigations during security incidents: - Regular log reviews - Threat hunting - Incident investigation - Root cause analysis

30.3.8 3.8 Data Protection Compliance

Logging and monitoring comply with data protection regulations (GDPR): - Minimization of personal data in logs - Purpose limitation of log data - Access control to personal log data - Deletion after retention period expiration

30.4 4. Roles and Responsibilities

30.4.1 RACI Matrix: Logging and Monitoring

Activity	CISO	SOC/Security Operations	IT Operations	System Owner	DPO
Policy Creation	R/A	C	C	C	C
SIEM Operations	A	R	C	I	I
Log Configuration	C	C	R	R	I
Monitoring and Alerting	A	R	C	I	I
Incident Investigation	A	R	C	C	C
Log Retention	C	C	R	I	C
Compliance Review	R/A	C	C	I	C

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

30.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **SOC Manager:** {{ meta.security.soc_manager }}
- **SIEM Administrator:** {{ meta.it.siem_admin }}
- **Implementation Responsible:** SOC, IT operations, system owners
- **Control/Audit Function:** ISMS, internal audit, DPO

30.5 5. Derivations (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

30.5.1 Related Guidelines

- **0330_Richtlinie_Logging_SIEM_und_Audit_Trails.md** - Detailed implementation guideline
- `0400_Policy_Incident_Management.md` - Incident management policy
- `0560_Policy_Datenschutz_Schnittstellen.md` - Data protection policy
- `0340_Policy_Vulnerability_und_Patch_Management.md` - Vulnerability management policy

30.5.2 Related Standards/Baselines

- Log standards and formats

- SIEM use cases and detection rules
- Retention requirements
- Alerting thresholds

30.5.3 Related Processes

- Log onboarding process
- Alert triage and escalation
- Incident investigation
- Log review process

30.6 6. Compliance, Monitoring, and Enforcement

30.6.1 Metrics and KPIs

- Number of log sources in SIEM (target: 100% of critical systems)
- Log completeness and availability (target: 99.9%)
- Average time to alert triage (MTTD - Mean Time To Detect)
- Number of false positives per day
- SIEM use case coverage
- Compliance rate with retention requirements

30.6.2 Evidence and Proof

- SIEM configuration and use cases
- Log retention evidence
- Alert statistics and triage reports
- Incident investigation reports
- Audit reports on logging and monitoring
- Data protection impact assessments

30.6.3 Consequences for Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Deactivation of logging:** Immediate remediation, investigation - **Unauthorized log manipulation:** Incident response, employment law consequences - **Non-compliance with retention:** Remediation, retraining - **Repeated violations:** Employment law consequences

30.7 7. Exceptions

Exceptions to this policy are only permitted in justified exceptional cases:

- **Exception Process:** See `0640_Policy_Ausnahmen_und_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO
- **Documentation:** All exceptions are documented in the risk register
- **Time Limit:** Exceptions are generally time-limited
- **Compensating Controls:** Exceptions require alternative security measures

30.8 8. References

30.8.1 Internal Documents

- `0010_ISMS_Informationssicherheitsleitlinie.md` - ISMS policy
- `0330_Richtlinie_Logging_SIEM_und_Audit_Trails.md` - Detailed guideline
- `0400_Policy_Incident_Management.md` - Incident management policy
- `0080_ISMS_Risikoregister_Template.md` - Risk register

30.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.8.15** - Logging
- **ISO/IEC 27001:2022 Annex A.8.16** - Monitoring activities
- **ISO/IEC 27002:2022** - Information security controls
- **NIST SP 800-92** - Guide to Computer Security Log Management
- **GDPR (EU 2016/679)** - General Data Protection Regulation
- **BSI IT-Grundschutz** - Module OPS.1.1.5 Logging

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 31

Guideline: Logging, SIEM and Audit Trails

Document ID: 0330
Document Type: Guideline (detailed)
Related Policy: 0320_Policy_Logging_and_Monitoring.md
Standard Reference: ISO/IEC 27001:2022 Annex A.8.15, A.8.16
Owner: {{ meta.it_operations.manager }}
Version: 1.0
Status: Approved
Classification: Confidential
Last Updated: {{ meta.document.date }}

31.1 1. Purpose and Scope

This guideline implements the `0320_Policy_Logging_and_Monitoring.md` and defines: - Logging requirements per system type - SIEM integration and use cases - Audit trail requirements and retention

Scope: All IT systems at **AdminSend GmbH**

31.2 2. Logging Requirements

31.2.1 2.1 Events to be Logged

Authentication: - Successful and failed logins - Logout events - MFA challenges and results - Password changes and resets - Account lockouts and unlocks

Authorization: - Access to confidential data - Privileged operations (sudo, admin rights) - Access denials - Permission changes

System Events: - System start and shutdown - Service starts and stops - Configuration changes - Software installations and updates - Errors and exceptions

Data Events: - File access (read, write, delete) - Database queries (for sensitive data) - Data exports and downloads - Backup operations

Network Events: - Firewall blocks and allows - VPN connections - Network scans - Traffic anomalies

31.2.2 2.2 Log Format and Content

Mandatory Fields: - Timestamp (UTC, ISO 8601) - Event type and severity - Source (system, application, IP) - User/account - Action/operation - Result (success/failure) - Additional context information

Example (JSON):

```
{
  "timestamp": "2024-02-02T10:15:30Z",
  "event_type": "authentication",
  "severity": "info",
  "source_ip": "192.168.1.100",
  "user": "jdoe",
  "action": "login",
  "result": "success",
  "mfa_method": "authenticator_app"
}
```

31.2.3 2.3 Logging Levels

System Type	Logging Level	Rationale
Production systems	INFO	Balance between detail and performance
Development systems	DEBUG	Troubleshooting
Security systems (firewall, IDS)	VERBOSE	Maximum visibility
Privileged systems	VERBOSE	Compliance and forensics

31.3 3. SIEM Integration

31.3.1 3.1 SIEM System

Platform: {{ meta.security.siem_solution }} (e.g., Splunk, Microsoft Sentinel, Elastic SIEM)

Architecture: - Log collection via agents or syslog - Central log aggregation - Normalization and enrichment - Correlation and alerting - Long-term archiving

31.3.2 3.2 Log Sources

Priority 1 (Critical): - Active Directory / Azure AD - Firewalls and IDS/IPS - VPN gateways - Privileged Access Management (PAM) - Databases with confidential data

Priority 2 (High): - Web servers and application servers - Email gateways - Cloud services (Azure, AWS, Google Cloud) - Endpoint Detection and Response (EDR)

Priority 3 (Medium): - Workstations and laptops - Network switches - Printers and IoT devices

31.3.3 3.3 SIEM Use Cases

Authentication: - Brute-force attacks (> 10 failed logins in 5 minutes) - Impossible travel (logins from geographically impossible locations) - Privileged account usage outside business hours

Malware and Intrusion: - Malware detections by EDR - IDS/IPS alerts - Command & Control (C2) communication - Lateral movement (unusual internal connections)

Data Exfiltration: - Large data volume uploads to external destinations - Access to many confidential files in short time - Unusual database queries

Compliance: - Access to PII (Personally Identifiable Information) - Changes to security configurations - Privileged operations without approval

31.3.4 3.4 Alerting and Response

Severity Levels: - **Critical:** Immediate escalation to on-call security (24/7) - **High:** Escalation within 1 hour - **Medium:** Processing within 4 hours - **Low:** Processing within 1 business day

Automated Response: - Account lockout on brute-force - IP blocking on malware C2 - Endpoint quarantine on malware detection

31.4 4. Audit Trails

31.4.1 4.1 Requirements

Immutability: - Logs must not be modified retroactively - Cryptographic signatures or write-once storage - Access to logs only for authorized personnel

Completeness: - Continuous recording of all relevant events - Monitoring of log integrity - Alerts on log failures

Traceability: - Who did what when? - Reconstruction of event chains - Forensic analysis possible

31.4.2 4.2 Privileged Access

Additional Requirements: - Session recording for privileged access - Four-eyes principle for critical operations - Approval workflow before access - Detailed logging of all actions

PAM Integration: - Privileged Access Management System: {{ meta.security.pam_solution }} - Just-in-Time (JIT) access - Automatic password rotation - Session monitoring and recording

31.4.3 4.3 Compliance Audit Trails

Regulatory Requirements: - GDPR: Access to personal data - SOX: Financially relevant transactions - HIPAA: Access to health data (if applicable)

Documentation: - Who accessed which data? - Purpose of access - Approval (if required) - Time period

31.5 5. Log Retention

31.5.1 5.1 Retention Periods

Log Type	Retention (Online)	Retention (Archive)	Rationale
Security logs	90 days	{{ meta.retention.log_years }} years	Forensics, compliance
Authentication logs	90 days	{{ meta.retention.log_years }} years	Audit, compliance
System logs	30 days	1 year	Troubleshooting
Application logs	30 days	1 year	Debugging
Audit trails (compliance)	180 days	{{ meta.retention.audit_years }} years	Regulatory

31.5.2 5.2 Archiving

Process: 1. Logs older than retention period (online) are archived 2. Compression and encryption 3. Transfer to archive storage (e.g., Azure Blob Archive, AWS Glacier) 4. Verification of archiving 5. Deletion from online SIEM

Archive Access: - Only with justified need (forensics, audit) - Approval by CISO - Restoration to SIEM for analysis

31.5.3 5.3 Secure Deletion

After Retention Expiry: - Automatic deletion from archive - Cryptographic deletion (destroy keys) - Documentation of deletion

31.6 6. Log Security

31.6.1 6.1 Access Control

Permissions: - **Security Team:** Full access to all logs - **IT Operations:** Access to system and application logs - **Auditors:** Read-only access to audit trails - **Developers:** Access only to dev logs

Authentication: - MFA for SIEM access - Privileged accounts for admin operations - Audit logging for SIEM access

31.6.2 6.2 Encryption

In Transit: - TLS 1.2+ for log transmission - Mutual TLS for critical systems

At Rest: - Encryption of SIEM storage (AES-256) - Encryption of archive logs

31.6.3 6.3 Integrity Protection

Methods: - Cryptographic signatures (HMAC) - Write-Once-Read-Many (WORM) storage - Blockchain-based log integrity (optional)

Monitoring: - Regular integrity checks - Alerts on tampering attempts

31.7 7. Monitoring and Alerting

31.7.1 7.1 Log Health Monitoring

Monitored Metrics: - Log ingestion rate (logs per second) - Log latency (time until log in SIEM) - Missing log sources - SIEM storage capacity

Alerts: - Log source not sending logs (> 15 minutes) - Unusually high log rate (possible attack or error) - SIEM storage > 80% full

31.7.2 7.2 Security Monitoring

24/7 Security Operations Center (SOC): - Monitoring of all SIEM alerts - Triage and incident response - Escalation for critical incidents

Automation: - SOAR (Security Orchestration, Automation and Response) - Automated playbooks for common incidents - Integration with ticketing system

31.8 8. Compliance and Audit

31.8.1 8.1 Key Performance Indicators (KPIs)

Metric	Target Value
Log source availability	> 99%
SIEM alert response time (critical)	< 15 minutes
False positive rate	< 10%
Log retention compliance	100%

31.8.2 8.2 Audit Evidence

- SIEM configuration and use cases
- Log retention reports
- Incident response documentation
- SIEM access logs

31.9 9. References

31.9.1 Internal Documents

- `0320_Policy_Logging_and_Monitoring.md`
- `0400_Policy_Incident_Management.md`

31.9.2 External Standards

- **ISO/IEC 27001:2022 Annex A.8.15** - Logging
- **ISO/IEC 27001:2022 Annex A.8.16** - Monitoring activities
- **NIST SP 800-92** - Guide to Computer Security Log Management

---

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 32

Policy: Vulnerability and Patch Management

Document ID: 0340
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.8.8 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

32.1 1. Purpose

This policy defines the principles for vulnerability and patch management at **AdminSend GmbH**. It ensures that technical vulnerabilities are identified, assessed, and remediated in a timely manner to minimize the risk of security incidents.

32.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Systems:** All IT systems, applications, operating systems, network components, firmware
- **Vulnerability Types:** Software vulnerabilities, configuration errors, missing patches
- **Environments:** Production, test, development, cloud, on-premise
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

32.3 3. Principles (Policy Statements)

32.3.1 3.1 Proactive Vulnerability Identification

Vulnerabilities are proactively identified through regular vulnerability scans, penetration tests, and security assessments.

32.3.2 3.2 Risk-Based Prioritization

Vulnerabilities are prioritized by risk (CVSS score, exploitability, impact, exposure). Critical vulnerabilities have highest priority.

32.3.3 3.3 Timely Remediation

Vulnerabilities are remediated within defined SLAs: - **Critical (CVSS 9.0-10.0):** 7 days - **High (CVSS 7.0-8.9):** 30 days - **Medium (CVSS 4.0-6.9):** 90 days - **Low (CVSS 0.1-3.9):** 180 days or based on risk assessment

32.3.4 3.4 Patch Management Lifecycle

Patches are deployed through a structured process: - **Identification:** Monitoring of vendor security bulletins - **Assessment:** Risk and impact analysis - **Testing:** Validation in test environment - **Deployment:** Controlled rollout to production - **Verification:** Confirmation of successful installation

32.3.5 3.5 Emergency Patching

For critical zero-day vulnerabilities or actively exploited exploits, an accelerated emergency patch process exists.

32.3.6 3.6 Compensating Controls

When patches cannot be applied immediately, compensating controls are implemented (e.g., network segmentation, WAF rules, IPS signatures).

32.3.7 3.7 Vulnerability Disclosure

Vulnerabilities in own products or services are disclosed responsibly (responsible disclosure).

32.3.8 3.8 Continuous Monitoring

Systems are continuously monitored for new vulnerabilities. Automated scanning tools are deployed.

32.4 4. Roles and Responsibilities

32.4.1 RACI Matrix: Vulnerability and Patch Management

Activity	CISO	Vulnerability Manager	IT Operations	System Owner	Change Management
Policy creation	R/A	C	C	C	I
Vulnerability scanning	A	R	C	I	I
Vulnerability assessment	A	R	C	C	I
Patch testing	C	C	R	R	I
Patch deployment	C	C	R	A	R
Emergency patching	A	R	R	C	C
Monitoring and reporting	A	R	C	I	I

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

32.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **Vulnerability Manager:** {{ meta.security.vuln_manager }}
- **Patch Manager:** {{ meta.it.patch_manager }}
- **Implementation Responsible:** IT Operations, System Owners
- **Control/Audit Function:** ISMS, Internal Audit

32.5 5. Derivations (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

32.5.1 Related Guidelines

- **0350_Guideline_Vulnerability_Scans_Patching_and_Exploitation_Response.md** - Detailed implementation guideline
- `0360_Policy_Change_and_Release_Management.md` - Change Management Policy
- `0400_Policy_Incident_Management.md` - Incident Management Policy
- `0540_Policy_Configuration_and_Hardening.md` - Configuration Management Policy

32.5.2 Related Standards/Baselines

- Vulnerability scanning schedule
- Patch SLAs and prioritization
- Emergency patch process

- Compensating controls catalog

32.5.3 Related Processes

- Vulnerability management process
- Patch management process
- Emergency patch process
- Penetration testing process

32.6 6. Compliance, Monitoring and Enforcement

32.6.1 Metrics and KPIs

- Number of open vulnerabilities by severity
- Mean time to remediate (MTTR)
- Patch compliance rate (target: 95% within SLA)
- Number of overdue patches
- Number of emergency patches per quarter
- Vulnerability scan coverage (target: 100% of critical systems)

32.6.2 Evidence and Proof

- Vulnerability scan reports
- Patch deployment logs
- Remediation evidence
- Compensating controls documentation
- Penetration test reports
- Patch compliance audit reports

32.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Unpatched critical systems:** Immediate remediation, investigation - **SLA violations:** Escalation, remediation plan - **Unauthorized patching:** Rollback, retraining - **Repeated violations:** Employment consequences

32.7 7. Exceptions

Exceptions to this policy are only permitted in justified cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and System Owner
- **Documentation:** All exceptions are documented in the risk register
- **Time Limitation:** Exceptions are generally time-limited
- **Compensating Controls:** Exceptions require alternative security measures

32.8 8. References

32.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0350_Guideline_Vulnerability_Scans_Patching_and_Exploitation_Response.md` - Detailed Guideline
- `0360_Policy_Change_and_Release_Management.md` - Change Management Policy
- `0080_ISMS_Risk_Register_Template.md` - Risk Register

32.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.8.8** - Management of technical vulnerabilities
- **ISO/IEC 27002:2022** - Information security controls
- **NIST SP 800-40** - Guide to Enterprise Patch Management Technologies
- **CVSS v3.1** - Common Vulnerability Scoring System
- **CWE/SANS Top 25** - Most Dangerous Software Weaknesses
- **OWASP Top 10** - Web Application Security Risks

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 33

Guideline: Vulnerability Scans, Patching and Exploitation Response

Document ID: 0350
Document Type: Guideline (detailed)
Related Policy: 0340_Policy_Vulnerability_and_Patch_Management.md
Standard Reference: ISO/IEC 27001:2022 Annex A.8.8
Owner: {{ meta.it_operations.manager }}
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}

33.1 1. Purpose and Scope

This guideline implements the `0340_Policy_Vulnerability_and_Patch_Management.md` and defines: - Vulnerability scanning processes and frequencies - Patch management workflows - Exploitation response for actively exploited vulnerabilities

Scope: All IT systems at **AdminSend GmbH**

33.2 2. Vulnerability Scanning

33.2.1 2.1 Scan Types

Authenticated Scans: - With credentials, deeper analysis - Detection of configuration weaknesses - Software inventory and patch level

Unauthenticated Scans: - Without credentials, attacker perspective - Detection of externally visible vulnerabilities - Network services and open ports

Web Application Scans: - OWASP Top 10 vulnerabilities - SQL injection, XSS, CSRF - API security tests

33.2.2 2.2 Scan Frequencies

System Type	Authenticated	Unauthenticated	Web App
Production systems	Weekly	Monthly	Monthly
Development systems	Monthly	Quarterly	On deployment
Critical infrastructure	Weekly	Weekly	Weekly
External systems	N/A	Weekly	Weekly

Ad-hoc Scans: - After new systems/applications - After critical vulnerability disclosures - After security incidents

33.2.3 2.3 Scanning Tools

Vulnerability Scanner: {{ meta.security.vuln_scanner }} (e.g., Tenable Nessus, Qualys, Rapid7)
Web Application Scanner: {{ meta.security.web_scanner }} (e.g., Burp Suite, OWASP ZAP)
Container Scanner: {{ meta.security.container_scanner }} (e.g., Trivy, Snyk)

33.2.4 2.4 Scan Process

1. **Planning:** Define scan time window (outside business hours)
2. **Execution:** Automated scans
3. **Analysis:** Review of results by security team
4. **Prioritization:** Vulnerabilities by severity and exploitability
5. **Remediation:** Ticket creation for IT operations
6. **Verification:** Re-scan after remediation

33.3 3. Vulnerability Assessment

33.3.1 3.1 Severity Classification

CVSS Score (Common Vulnerability Scoring System): - **Critical (9.0-10.0):** Immediate remediation required - **High (7.0-8.9):** Remediation within 7 days - **Medium (4.0-6.9):** Remediation within 30 days - **Low (0.1-3.9):** Remediation within 90 days

33.3.2 3.2 Prioritization

Factors: - CVSS score - Exploitability (exploit available?) - Asset criticality - Exposure (internet-facing?) - Compensating controls present?

Prioritization Matrix: | CVSS | Internet-facing | Exploit Available | Priority | SLA | |——|——————|———————-|———-|——| | Critical | Yes | Yes | P1 | 24 hours | | Critical | Yes | No | P1 | 48 hours | | Critical | No | Yes | P2 | 7 days | | High | Yes | Yes | P2 | 7 days | | High | No | No | P3 | 30 days |

33.3.3 3.3 False Positives

Process: - Security team reviews vulnerability - If false positive: Mark in scanner - Document rationale - Regular review (quarterly)

33.4 4. Patch Management

33.4.1 4.1 Patch Sources

Operating Systems: - Windows: WSUS / Windows Update - Linux: Package managers (apt, yum, dnf) - macOS: Software Update

Applications: - Vendor updates - Third-party patch management (e.g., Ninite, Chocolatey)

Firmware: - Vendor portals - Automatic update checks

33.4.2 4.2 Patch Process

Phase 1: Patch Identification - Automatic notifications from vendors - Vulnerability scan results - Security advisories (CVE, CERT)

Phase 2: Assessment and Prioritization - Check relevance for own systems - Assess severity and exploitability - Prioritize according to Section 3.2

Phase 3: Testing - Test in dev/test environment - Compatibility check - Create rollback plan

Phase 4: Deployment - Staging: Pilot group (10% of systems) - Monitor for issues (24 hours) - Rollout: Remaining systems - Verification: Patch successfully installed?

Phase 5: Verification - Re-scan to confirm remediation - Documentation in ticketing system

33.4.3 4.3 Patch Windows

Maintenance Windows: - **Production systems:** Sunday 02:00-06:00 - **Development systems:** Daily outside business hours - **Critical patches:** Emergency maintenance window as needed

Automatic Patching: - Workstations: Automatic, outside business hours - Servers: Manual after testing - Critical systems: Change approval required

33.4.4 4.4 Emergency Patching

Triggers: - Actively exploited exploit (zero-day) - Critical vulnerability in internet-facing system - Ransomware campaign

Process: 1. **Immediate Assessment:** Identify affected systems 2. **Emergency Change:** Accelerated approval 3. **Minimal Testing:** Test only critical functions 4. **Immediate Deployment:** Within 24 hours 5. **Monitoring:** Enhanced monitoring after patch

33.5 5. Exploitation Response

33.5.1 5.1 Threat Intelligence

Sources: - **CISA KEV (Known Exploited Vulnerabilities):** https://www.cisa.gov/known-exploited-vulnerabilities-catalog - **CERT-Bund:** https://www.cert-bund.de/ - **Vendor Security Advisories** - **Threat Intelligence Feeds:** {{ meta.security.threat_intel }}

Monitoring: - Daily check for new exploits - Automatic alerts for critical vulnerabilities - Cross-reference with own systems

33.5.2 5.2 Zero-Day Response

Process: 1. **Detection:** Threat intelligence or IDS/IPS alert 2. **Assessment:** Identify affected systems 3. **Containment:** Immediate measures to minimize risk 4. **Mitigation:** Workarounds or compensating controls 5. **Patching:** As soon as patch available 6. **Lessons Learned:** Post-incident review

Immediate Measures (Containment): - Network segmentation (firewall rules) - Disable affected services - Update IDS/IPS signatures - Enhanced monitoring

33.5.3 5.3 Compensating Controls

When Patching Not Immediately Possible: - **Network Isolation:** Isolate affected systems - **WAF Rules:** Web Application Firewall rules - **IPS Signatures:** Intrusion Prevention System - **Access Restrictions:** Only authorized users - **Enhanced Monitoring:** SIEM alerts for exploitation attempts

Documentation: - Rationale for delayed patching - Implemented compensating controls - Risk assessment - Planned patch date

33.6 6. Vulnerability Disclosure

33.6.1 6.1 Responsible Disclosure

Process for External Researchers: 1. **Report:** security@{{ meta.organization.domain }} 2. **Acknowledgment:** Within 24 hours 3. **Assessment:** Within 7 days 4. **Remediation:** According to severity SLA 5. **Disclosure:** Coordinated with researcher (90 days)

Bug Bounty Program (Optional): - Platform: {{ meta.security.bug_bounty }} (e.g., HackerOne, Bugcrowd) - Scope: Defined systems and applications - Rewards: By severity

33.6.2 6.2 Vendor Disclosure

For Vulnerabilities in Vendor Products: 1. Report to vendor 2. Coordinate with vendor for patch 3. No public disclosure before patch availability 4. Implement workarounds

33.7 7. Compliance and Audit

33.7.1 7.1 Key Performance Indicators (KPIs)

Metric	Target Value
Critical patches (SLA compliance)	$> 95\%$
Scan coverage	100% of all systems
Mean time to patch (critical)	< 7 days
Open critical vulnerabilities	< 5

33.7.2 7.2 Reporting

Monthly Vulnerability Report: - Number of vulnerabilities by severity - Patch compliance rate - SLA violations - Trend analysis

Quarterly Management Report: - Vulnerability posture - Risk development - Improvement measures

33.7.3 7.3 Audit Evidence

- Scan reports and history
- Patch deployment logs
- Remediation tickets
- Compensating controls documentation

33.8 8. References

33.8.1 Internal Documents

- `0340_Policy_Vulnerability_and_Patch_Management.md`
- `0400_Policy_Incident_Management.md`

33.8.2 External Standards

- **ISO/IEC 27001:2022 Annex A.8.8** - Management of technical vulnerabilities
- **NIST SP 800-40** - Guide to Enterprise Patch Management
- **CVSS v3.1** - Common Vulnerability Scoring System

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 34

Policy: Change and Release Management

Document ID: 0360
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.8.32 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

34.1 1. Purpose

This policy defines the principles for change and release management at **AdminSend GmbH**. It ensures that changes to IT systems are controlled, tested, and documented to minimize operational disruptions and security risks.

34.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Systems:** All IT systems, applications, infrastructure, networks, cloud services
- **Change Types:** Standard changes, normal changes, emergency changes
- **Environments:** Production, test, development
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

34.3 3. Principles (Policy Statements)

34.3.1 3.1 Controlled Changes

All changes to production IT systems must be approved, documented, and tracked through the change management process.

34.3.2 3.2 Change Categorization

Changes are categorized by risk and impact: - **Standard Changes:** Pre-approved, low-risk, recurring changes - **Normal Changes:** Regular changes with CAB approval - **Emergency Changes:** Urgent changes to resolve critical issues

34.3.3 3.3 Change Advisory Board (CAB)

A Change Advisory Board evaluates and approves normal and emergency changes. The CAB consists of representatives from IT, security, business, and change management.

34.3.4 3.4 Risk and Impact Analysis

A risk and impact analysis is performed before each change. Security risks are assessed and mitigation measures defined.

34.3.5 3.5 Testing and Validation

Changes are validated in test environments before being rolled out to production. Critical changes require comprehensive testing.

34.3.6 3.6 Rollback Planning

A rollback plan exists for every change to quickly return to the previous state in case of problems.

34.3.7 3.7 Documentation and Traceability

All changes are documented (description, justification, approval, execution, result). Changes are traceable and auditable.

34.3.8 3.8 Security Review

Changes with security relevance require a security review by the security team before approval.

34.4 4. Roles and Responsibilities

34.4.1 RACI Matrix: Change and Release Management

Activity	Change Manager	CAB	CISO	Change Requester	IT Operations
Policy creation	C	C	R/A	I	C
Change request	I	I	I	R	I

Activity	Change Manager	CAB	CISO	Change Requester	IT Operations
Risk analysis	R	C	C	C	C
CAB approval	R	A	C	I	I
Security review	C	C	R/A	I	I
Change implementation	C	I	I	I	R/A
Rollback	R	I	C	I	R/A
Post-implementation review	R/A	C	C	C	C

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

34.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **Change Manager:** {{ meta.it.change_manager }}
- **CAB Chair:** {{ meta.it.cab_chair }}
- **Implementation Responsible:** IT Operations, Development
- **Control/Audit Function:** ISMS, Internal Audit

34.5 5. Derivations (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

34.5.1 Related Guidelines

- **0370_Guideline_Change_Management_with_Security_Approvals.md** - Detailed implementation guideline
- `0340_Policy_Vulnerability_and_Patch_Management.md` - Patch Management Policy
- `0380_Policy_Secure_Development.md` - Secure Development Policy
- `0400_Policy_Incident_Management.md` - Incident Management Policy

34.5.2 Related Standards/Baselines

- Change categorization and approval processes
- CAB composition and decision criteria
- Testing and validation requirements
- Rollback procedures

34.5.3 Related Processes

- Change management process

- Emergency change process
- Release management process
- Post-implementation review

34.6 6. Compliance, Monitoring and Enforcement

34.6.1 Metrics and KPIs

- Number of changes per category (standard, normal, emergency)
- Change success rate (target: >95%)
- Number of failed changes and rollbacks
- Average change lead time
- Number of unauthorized changes (target: 0)
- Security review coverage for security-relevant changes (target: 100%)

34.6.2 Evidence and Proof

- Change tickets and approvals
- CAB meeting minutes
- Security review documentation
- Test results
- Rollback documentation
- Post-implementation review reports

34.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Unauthorized change:** Rollback, investigation, retraining - **Missing documentation:** Completion, warning - **Skipped security review:** Investigation, disciplinary action - **Repeated violations:** Employment consequences

34.7 7. Exceptions

Exceptions to this policy are only permitted in justified cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by Change Manager and CISO
- **Documentation:** All exceptions are documented and discussed in post-implementation review
- **Time Limitation:** Exceptions are generally time-limited

34.8 8. References

34.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0370_Guideline_Change_Management_with_Security_Approvals.md` - Detailed Guideline
- `0340_Policy_Vulnerability_and_Patch_Management.md` - Patch Management Policy
- `0080_ISMS_Risk_Register_Template.md` - Risk Register

34.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.8.32** - Change management
- **ISO/IEC 27002:2022** - Information security controls
- **ITIL 4** - Change Enablement
- **ISO/IEC 20000** - IT Service Management

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 35

Guideline: Change Management with Security Approvals

Document ID: 0370
Document Type: Guideline (detailed)
Related Policy: 0360_Policy_Change_and_Release_Management.md
Standard Reference: ISO/IEC 27001:2022 Annex A.8.32
Owner: {{ meta.it_operations.manager }}
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}

35.1 1. Purpose and Scope

This guideline implements the `0360_Policy_Change_and_Release_Management.md` and defines: - Change management processes with security reviews - Change categories and approval workflows - Rollback procedures and post-implementation reviews

Scope: All IT changes at **AdminSend GmbH**

35.2 2. Change Categories

35.2.1 2.1 Standard Changes

Definition: Pre-approved, low-risk, frequent changes

Examples: - Password resets - Software updates (tested) - Adding users to standard groups

Approval: No individual approval required
Security Review: Not required

35.2.2 2.2 Normal Changes

Definition: Planned changes with medium risk

Examples: - Configuration changes - Software installations - Network changes

Approval: Change Advisory Board (CAB)
Security Review: For security-relevant changes

35.2.3 2.3 Emergency Changes

Definition: Unplanned, urgent changes

Examples: - Critical security patches - System outages - Active security incidents

Approval: Emergency CAB (ECAB)
Security Review: Retrospectively

35.3 3. Change Management Process

35.3.1 3.1 Change Request (RFC)

Mandatory Fields: - Change title and description - Justification (business justification) - Affected systems and services - Risk assessment - Rollback plan - Test results - Planned time window

Security-Relevant Additional Fields: - Impact on security controls - Changes to firewall rules - New external connections - Privileged access required

35.3.2 3.2 Risk Assessment

Risk Matrix: | Likelihood | Impact Low | Impact Medium | Impact High | |————|————|————|————-| | Low | Low | Low | Medium | | Medium | Low | Medium | High | | High | Medium | High | Critical |

Impact: - **Low:** Single user affected - **Medium:** Department affected - **High:** Entire organization affected

35.3.3 3.3 Security Review

Triggers: - Changes to security systems (firewall, IDS, etc.) - New external connections - Privileged access - Changes to authentication/authorization - Risk “High” or “Critical”

Review by IT Security: - Review of change request - Assess security impact - Recommend additional controls - Approval or rejection

SLA: Security review within 2 business days

35.3.4 3.4 Change Advisory Board (CAB)

Members: - Change Manager (chair) - IT Operations - IT Security (for security-relevant changes) - Application Owner (for application changes) - Business Representative

Frequency: Weekly (Tuesday 10:00 AM)

Tasks: - Review and approval of normal changes - Prioritization in case of conflicts - Risk assessment - Schedule planning

35.3.5 3.5 Implementation

Pre-Implementation: - Create backup - Provide rollback plan - Communication to affected users - Prepare monitoring

Implementation: - Execute change according to plan - Document all steps - Document deviations

Post-Implementation: - Functional test - Monitor for errors (24 hours) - Update change status - Complete documentation

35.3.6 3.6 Rollback

Triggers: - Functional test failed - Critical errors in production - Security issues detected

Process: 1. Rollback decision by Change Manager 2. Rollback according to rollback plan 3. Verify restoration 4. Root cause analysis 5. New change request for retry

35.4 4. Emergency Changes

35.4.1 4.1 Emergency CAB (ECAB)

Members: - Change Manager or deputy - IT Operations (on-call) - CISO or IT Security (on-call)

Availability: 24/7

Approval Process: - Telephone or email approval - Documentation retrospectively - Review in next regular CAB

35.4.2 4.2 Emergency Change Process

Accelerated Workflow: 1. **Initiation:** Incident Manager creates emergency RFC 2. **Assessment:** ECAB assesses urgency and risk 3. **Approval:** ECAB approves (or rejects) 4. **Implementation:** Immediate execution 5. **Documentation:** Retrospective completion 6. **Review:** In next CAB

Security Review: - For critical security patches: Retrospectively - For other emergency changes: Before implementation (if possible)

35.5 5. Security Controls

35.5.1 5.1 Segregation of Duties

Principle: No person may request, approve, and implement a change

Roles: - **Requester:** Requests change - **Approver:** Approves change (CAB) - **Implementer:** Executes change - **Reviewer:** Reviews post-implementation

35.5.2 5.2 Privileged Changes

Additional Requirements: - Four-eyes principle during implementation - Session recording - Detailed documentation - Post-implementation security review

35.5.3 5.3 Firewall Changes

Special Requirements: - Justification for each new rule - Document source and destination IP/port - Time limitation (where possible) - Regular review (quarterly)

Approval: - IT Security: Mandatory - Network Team: Technical feasibility - Application Owner: Business justification

35.6 6. Testing and Validation

35.6.1 6.1 Test Environments

Requirements: - Dev/test environment for all critical systems - As identical to production as possible - Isolated from production

Test Process: 1. Implement change in dev/test 2. Perform functional test 3. Performance test (if needed) 4. Security test (for security-relevant changes) 5. Document test results

35.6.2 6.2 Security Testing

For Security-Relevant Changes: - Vulnerability scan after change - Penetration test (for critical changes) - Code review (for software changes) - Configuration review

35.7 7. Documentation and Audit

35.7.1 7.1 Change Documentation

Mandatory Documentation: - Change Request (RFC) - Approvals - Implementation log - Test results - Post-implementation review

Retention: {{ meta.retention.change_years }} years

35.7.2 7.2 Post-Implementation Review (PIR)

Execution: - Within 7 days after implementation - For all normal and emergency changes

Content: - Success of implementation - Problems encountered - Lessons learned - Improvement suggestions

35.7.3 7.3 Compliance and Audit

Key Performance Indicators (KPIs): | Metric | Target Value | |———|————–| | Successful changes | > 95% | | Emergency changes | < 10% of all changes | | Unauthorized changes | 0 | | PIR completion rate | 100% |

Audit Evidence: - Change logs - Approvals - Security reviews - PIR reports

35.8 8. References

35.8.1 Internal Documents

- `0360_Policy_Change_and_Release_Management.md`
- `0400_Policy_Incident_Management.md`

35.8.2 External Standards

- **ISO/IEC 27001:2022 Annex A.8.32** - Change management
- **ITIL 4** - Change Enablement Practice

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 36

Policy: Secure Development

Document ID: 0380
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.8.25-A.8.28 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

36.1 1. Purpose

This policy defines the principles for secure software development (Secure SDLC) at **AdminSend GmbH**. It ensures that security is integrated into all phases of the software development lifecycle and that applications are developed, tested, and operated securely.

36.2 2. Scope

This policy applies to:

- **Organizational Units:** All development teams and locations of AdminSend GmbH
- **Applications:** All internally developed applications, APIs, microservices, mobile apps
- **Development Phases:** Requirements, design, implementation, testing, deployment, maintenance
- **Development Models:** Agile, Waterfall, DevOps, DevSecOps
- **Locations:** {{ netbox.site.name }} and all other development sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

36.3 3. Principles (Policy Statements)

36.3.1 3.1 Security by Design

Security is integrated into the development process from the beginning (Shift Left). Security requirements are defined in the requirements phase and considered in design.

36.3.2 3.2 Secure Coding Standards

Developers follow recognized secure coding standards (OWASP, CERT, CWE). Code is developed according to best practices to avoid common vulnerabilities.

36.3.3 3.3 Code Reviews and Peer Reviews

All code changes undergo code reviews. Security-relevant code requires additional security reviews by the security team.

36.3.4 3.4 Automated Security Testing

Security testing is integrated into the CI/CD pipeline: - **SAST (Static Application Security Testing):** Static code analysis - **DAST (Dynamic Application Security Testing):** Dynamic security tests - **SCA (Software Composition Analysis):** Analysis of dependencies and open-source components - **Container Scanning:** Security review of container images

36.3.5 3.5 Secrets Management

Secrets (passwords, API keys, certificates) are never stored in code or repositories. Secrets are managed in dedicated secrets management systems.

36.3.6 3.6 Dependency Management

External libraries and dependencies are checked for known vulnerabilities. Outdated or insecure dependencies are updated promptly.

36.3.7 3.7 Security Testing Before Production Release

Comprehensive security tests are performed before production release: - Penetration testing for critical applications - Security acceptance testing - Vulnerability assessment

36.3.8 3.8 Secure Deployment and Configuration

Applications are deployed with secure configurations. Default credentials are changed, unnecessary features disabled, hardening measures applied.

36.4 4. Roles and Responsibilities

36.4.1 RACI Matrix: Secure Development

Activity	CISO	Security Champion	Developer	DevOps	Security Team
Policy creation	R/A	C	C	C	C
Security requirements	C	R	C	I	R/A
Secure coding	I	C	R/A	I	C
Code review	I	R	R	I	C
Security review	A	C	I	I	R
SAST/DAST/SCA	C	C	I	R	R/A
Penetration testing	A	I	I	I	R
Security training	A	C	R	R	R

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

36.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **Security Champion:** Developer with security expertise in each team
- **Application Security Lead:** {{ meta.security.appsec_lead }}
- **Implementation Responsible:** Developers, DevOps, Security Team
- **Control/Audit Function:** ISMS, Internal Audit

36.5 5. Derivations (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

36.5.1 Related Guidelines

- **0390_Guideline_Secure_SDLC_Coding_Review_and_Secrets.md** - Detailed implementation guideline
- `0360_Policy_Change_and_Release_Management.md` - Change Management Policy
- `0340_Policy_Vulnerability_and_Patch_Management.md` - Vulnerability Management Policy
- `0260_Policy_Cryptography_and_Key_Management.md` - Cryptography Policy

36.5.2 Related Standards/Baselines

- Secure coding standards (OWASP, CERT)
- Code review checklists
- SAST/DAST/SCA tool configurations
- Secrets management standards

36.5.3 Related Processes

- Secure SDLC process
- Code review process
- Security testing process
- Vulnerability disclosure process

36.6 6. Compliance, Monitoring and Enforcement

36.6.1 Metrics and KPIs

- Number of security vulnerabilities per release (target: 50% annual reduction)
- Code review coverage (target: 100%)
- SAST/DAST/SCA coverage (target: 100% of critical applications)
- Mean time to remediate vulnerabilities (MTTR)
- Number of secrets in code (target: 0)
- Security training completion rate (target: 100% annually)

36.6.2 Evidence and Proof

- Code review documentation
- SAST/DAST/SCA reports
- Penetration test reports
- Security acceptance test results
- Secrets scanning reports
- Security training evidence

36.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Secrets in code:** Immediate rotation, incident response, retraining - **Skipped code reviews:** Rollback, completion, warning - **Ignored security findings:** Remediation, retraining - **Repeated violations:** Employment consequences

36.7 7. Exceptions

Exceptions to this policy are only permitted in justified cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and Application Security Lead
- **Documentation:** All exceptions are documented in the risk register
- **Time Limitation:** Exceptions are generally time-limited
- **Compensating Controls:** Exceptions require alternative security measures

36.8 8. References

36.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy

- `0390_Guideline_Secure_SDLC_Coding_Review_and_Secrets.md` - Detailed Guideline
- `0360_Policy_Change_and_Release_Management.md` - Change Management Policy
- `0080_ISMS_Risk_Register_Template.md` - Risk Register

36.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.8.25** - Secure development lifecycle
- **ISO/IEC 27001:2022 Annex A.8.26** - Application security requirements
- **ISO/IEC 27001:2022 Annex A.8.27** - Secure system architecture and engineering principles
- **ISO/IEC 27001:2022 Annex A.8.28** - Secure coding
- **OWASP Top 10** - Web Application Security Risks
- **OWASP ASVS** - Application Security Verification Standard
- **NIST SP 800-218** - Secure Software Development Framework (SSDF)
- **CWE Top 25** - Most Dangerous Software Weaknesses

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 37

Guideline: Secure SDLC, Code Reviews and Secrets Management

Document ID: 0390
Document Type: Guideline (detailed)
Related Policy: 0380_Policy_Secure_Development.md
Standard Reference: ISO/IEC 27001:2022 Annex A.8.25, A.8.26
Owner: {{ meta.development.manager }}
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}

37.1 1. Purpose and Scope

This guideline implements the `0380_Policy_Secure_Development.md` and defines: - Secure Software Development Lifecycle (SSDLC) - Code review processes and security checks - Secrets management and secure configuration

Scope: All software development at **AdminSend GmbH**

37.2 2. Secure SDLC Phases

37.2.1 2.1 Requirements Phase

- Define security requirements
- Conduct threat modeling
- Identify compliance requirements

37.2.2 2.2 Design Phase

- Security architecture review
- Data flow diagrams

- Authentication/authorization design

37.2.3 2.3 Development Phase

- Follow secure coding standards
- SAST (Static Application Security Testing)
- Dependency scanning

37.2.4 2.4 Testing Phase

- DAST (Dynamic Application Security Testing)
- Penetration testing
- Security test cases

37.2.5 2.5 Deployment Phase

- Security configuration review
- Secrets management
- Deployment checklist

37.2.6 2.6 Maintenance Phase

- Vulnerability management
- Security patches
- Incident response

37.3 3. Secure Coding Standards

37.3.1 3.1 OWASP Top 10

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

37.3.2 3.2 Input Validation

- Validate all inputs (whitelist approach)
- Parameterized queries (SQL injection prevention)
- Output encoding (XSS prevention)

37.3.3 3.3 Authentication & Authorization

- Do not implement custom cryptography
- Use established frameworks (OAuth 2.0, OpenID Connect)
- Least privilege principle

37.3.4 3.4 Error Handling

- No sensitive information in error messages

- Centralized error logging
- Graceful degradation

37.4 4. Code Reviews

37.4.1 4.1 Peer Code Review

Process: - Every code change requires at least 1 approval - Review before merge to main branch - Checklist for security aspects

Security Review Checklist: - [ ] Input validation present? - [ ] No secrets in code? - [ ] Secure cryptography used? - [ ] Error handling correct? - [ ] Logging implemented?

37.4.2 4.2 Security Champion Review

For Security-Critical Changes: - Additional review by Security Champion - Security Champion: Developer with security training - At least 1 Security Champion per team

37.4.3 4.3 Automated Code Review

Tools: - **SAST:** {{ meta.security.sast_tool }} (e.g., SonarQube, Checkmarx) - **Dependency Check:** {{ meta.security.dependency_tool }} (e.g., Snyk, Dependabot) - **Secrets Scanning:** {{ meta.security.secrets_scanner }} (e.g., GitGuardian, TruffleHog)

Integration: - CI/CD pipeline - Automatic scans on every commit - Blocking on critical/high findings

37.5 5. Secrets Management

37.5.1 5.1 Prohibited Practices

Never: - Commit secrets to Git - Secrets in configuration files (plaintext) - Secrets in environment variables (production) - Secrets in logs or error messages

37.5.2 5.2 Secrets Management System

System: {{ meta.security.secrets_manager }} (e.g., HashiCorp Vault, Azure Key Vault, AWS Secrets Manager)

Features: - Central secrets storage (encrypted) - Dynamic secrets (short-lived) - Audit logging of all access - Secrets rotation

37.5.3 5.3 Secrets Rotation

Frequency: - API keys: Every 90 days - Database credentials: Every 180 days - Service account passwords: Every 180 days

Automation: - Automatic rotation where possible - Notification before expiry

37.5.4 5.4 Development vs. Production

Separate Secrets: - Dev/Test: Separate secrets (lower privileges) - Production: Production secrets (higher privileges) - No reuse between environments

37.6 6. Dependency Management

37.6.1 6.1 Third-Party Libraries

Requirements: - Only use approved libraries - Regular updates - Vulnerability scanning

Approval Process: - Request via ticketing system - Security review of library - License compliance check - Approval by security team

37.6.2 6.2 Software Composition Analysis (SCA)

Tools: {{ meta.security.sca_tool }} (e.g., Snyk, WhiteSource)

Process: - Automatic scanning on build - Identification of known vulnerabilities (CVEs) - Alerts on critical vulnerabilities - Remediation recommendations

37.6.3 6.3 Dependency Updates

Strategy: - Security updates: Immediately - Minor updates: Monthly - Major updates: After testing

37.7 7. CI/CD Security

37.7.1 7.1 Pipeline Security

Security Gates: 1. **Commit:** Secrets scanning 2. **Build:** SAST, dependency check 3. **Test:** Unit tests, security tests 4. **Deploy:** DAST, configuration review

Blocking On: - Critical/high SAST findings - Known exploited vulnerabilities - Secrets in code

37.7.2 7.2 Container Security

Image Scanning: - Scan all container images - Only deploy signed images - Regular re-scans

Best Practices: - Minimal base images - Non-root user - Read-only filesystem

37.7.3 7.3 Infrastructure as Code (IaC)

Security Scanning: - Terraform, CloudFormation, etc. - Tools: Checkov, Terrascan - Check for misconfigurations

37.8 8. Security Testing

37.8.1 8.1 SAST (Static Application Security Testing)

Frequency: On every commit
Tool: {{ meta.security.sast_tool }}

Coverage: All programming languages

37.8.2 8.2 DAST (Dynamic Application Security Testing)

Frequency: Weekly (staging), before every release
Tool: {{ meta.security.dast_tool }}
Scope: Web applications, APIs

37.8.3 8.3 Penetration Testing

Frequency: - New applications: Before go-live - Existing applications: Annually - After critical changes: Ad-hoc

Execution: - Internal or external pentesters - Scope definition - Remediation of all findings - Re-test after fixes

37.9 9. Compliance and Audit

37.9.1 9.1 Key Performance Indicators (KPIs)

Metric	Target Value
Code review coverage	100%
SAST scan coverage	100%
Critical/high findings (open)	0
Secrets in code	0

37.9.2 9.2 Audit Evidence

- Code review logs
- SAST/DAST reports
- Penetration test reports
- Secrets rotation logs

37.10 10. References

37.10.1 Internal Documents

- `0380_Policy_Secure_Development.md`
- `0340_Policy_Vulnerability_and_Patch_Management.md`

37.10.2 External Standards

- **ISO/IEC 27001:2022 Annex A.8.25** - Secure development lifecycle
- **ISO/IEC 27001:2022 Annex A.8.26** - Application security requirements
- **OWASP ASVS** - Application Security Verification Standard
- **NIST SP 800-218** - Secure Software Development Framework

---

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 38

Policy: Incident Management

Document ID: 0400
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.5.24-A.5.28 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

38.1 1. Purpose

This policy defines the principles for incident management and security incident response at **AdminSend GmbH**. It ensures that security incidents are detected, assessed, handled, and documented in a timely manner to minimize damage and learn from incidents.

38.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Incident Types:** Security incidents, data breaches, malware, phishing, DDoS, insider threats
- **Systems:** All IT systems, applications, networks, cloud services
- **Personnel:** All employees, contractors, suppliers
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

38.3 3. Principles (Policy Statements)

38.3.1 3.1 Incident Response Capability

The organization maintains an incident response capability with defined processes, roles, and tools for handling security incidents.

38.3.2 3.2 Reporting Obligation

All employees are required to report suspected or confirmed security incidents immediately. There are no negative consequences for good-faith reports.

38.3.3 3.3 Incident Categorization and Prioritization

Incidents are categorized by severity and impact: - **Critical:** Severe impact on business operations or data protection - **High:** Significant impact, but business operations not critically endangered - **Medium:** Moderate impact, limited impairment - **Low:** Minor impact, no immediate danger

38.3.4 3.4 Incident Response Lifecycle

Incidents are handled through a structured process: - **Detection & Reporting:** Detection and reporting - **Triage & Assessment:** Assessment and prioritization - **Containment:** Containment for damage limitation - **Eradication:** Elimination of the cause - **Recovery:** Restoration of normal operations - **Post-Incident Review:** Follow-up and lessons learned

38.3.5 3.5 Escalation and Communication

Critical incidents are escalated according to defined escalation paths to management, legal, PR, and authorities as appropriate. Communication follows established communication plans.

38.3.6 3.6 Forensics and Evidence Preservation

Forensic analysis is performed for severe incidents. Evidence is securely preserved and documented for possible legal action.

38.3.7 3.7 Data Breach Notification

Data breaches are reported to supervisory authorities and affected individuals within 72 hours in accordance with GDPR and other regulatory requirements.

38.3.8 3.8 Continuous Improvement

Lessons learned are derived from every incident. Insights flow into the improvement of processes, controls, and awareness.

38.4 4. Roles and Responsibilities

38.4.1 RACI Matrix: Incident Management

Activity	CISO	Incident Manager	SOC	IT Operations	Legal/DPO	Management
Policy creation	R/A	C	C	C	C	I
Incident detection	A	C	R	C	I	I
Incident triage	A	R	R	C	I	I
Incident response	A	R	R	R	C	I
Escalation	A	R	C	I	C	I
Data breach notification	A	C	I	I	R	C
Forensics	A	C	R	C	C	I
Post-incident review	R/A	R	C	C	C	C

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

38.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **Incident Manager:** {{ meta.security.incident_manager }}
- **SOC Manager:** {{ meta.security.soc_manager }}
- **Data Protection Officer:** {{ meta.dpo.name }}
- **Implementation Responsible:** SOC, IT Operations, Incident Response Team
- **Control/Audit Function:** ISMS, Internal Audit

38.5 5. Derivations (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

38.5.1 Related Guidelines

- **0410_Guideline_Incident_Response_and_Major_Incident_Process.md** - Detailed implementation guideline
- `0320_Policy_Logging_and_Monitoring.md` - Logging and Monitoring Policy
- `0440_Policy_Business_Continuity_ICT_Readiness.md` - Business Continuity Policy
- `0560_Policy_Data_Protection_Interfaces.md` - Data Protection Policy

38.5.2 Related Standards/Baselines

- Incident response playbooks
- Incident severity matrix
- Escalation paths

- Data breach notification process

38.5.3 Related Processes

- Incident response process
- Major incident process
- Data breach notification process
- Post-incident review process

38.6 6. Compliance, Monitoring and Enforcement

38.6.1 Metrics and KPIs

- Number of incidents per category and severity
- MTTD (Mean Time To Detect) - Average detection time
- MTTR (Mean Time To Respond) - Average response time
- MTTR (Mean Time To Resolve) - Average resolution time
- Number of data breaches and notifications
- Post-incident review completion rate (target: 100%)

38.6.2 Evidence and Proof

- Incident tickets and documentation
- Incident response logs
- Forensics reports
- Data breach notifications
- Post-incident review reports
- Lessons learned documentation

38.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Unreported incident:** Retraining, warning - **Delayed data breach notification:** Compliance investigation, possible fines - **Evidence tampering:** Severe disciplinary action - **Repeated violations:** Employment consequences

38.7 7. Exceptions

Exceptions to this policy are only permitted in justified cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO
- **Documentation:** All exceptions are documented in the risk register
- **Time Limitation:** Exceptions are generally time-limited

38.8 8. References

38.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0410_Guideline_Incident_Response_and_Major_Incident_Process.md` - Detailed Guideline
- `0320_Policy_Logging_and_Monitoring.md` - Logging and Monitoring Policy
- `0080_ISMS_Risk_Register_Template.md` - Risk Register

38.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.5.24** - Information security incident management planning and preparation
- **ISO/IEC 27001:2022 Annex A.5.25** - Assessment and decision on information security events
- **ISO/IEC 27001:2022 Annex A.5.26** - Response to information security incidents
- **ISO/IEC 27001:2022 Annex A.5.27** - Learning from information security incidents
- **ISO/IEC 27001:2022 Annex A.5.28** - Collection of evidence
- **NIST SP 800-61** - Computer Security Incident Handling Guide
- **GDPR (EU 2016/679)** - Art. 33, 34 - Data Breach Notification
- **NIS2 Directive** - Network and Information Security Directive

---

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 39

Guideline: Incident Response and Major Incident Process

Document ID: 0410
Document Type: Guideline (detailed)
Related Policy: 0400_Policy_Incident_Management.md
Standard Reference: ISO/IEC 27001:2022 Annex A.5.24, A.5.25, A.5.26
Owner: {{ meta.it_operations.manager }}
Version: 1.0
Status: Approved
Classification: Confidential
Last Updated: {{ meta.document.date }}

39.1 1. Purpose and Scope

This guideline implements the `0400_Policy_Incident_Management.md` and defines: - Incident response processes and workflows - Major incident management - Security incident response and forensics

Scope: All incidents at **AdminSend GmbH**

39.2 2. Incident Categories

39.2.1 2.1 Severity Levels

Severity	Definition	Examples	Response Time
P1 (Critical)	Critical service outage	Production outage, data loss, active cyberattack	15 minutes
P2 (High)	Severe impairment	Performance issues, partial outage	1 hour

Severity	Definition	Examples	Response Time
P3 (Medium)	Moderate impairment	Individual users affected	4 hours
P4 (Low)	Minor impairment	Cosmetic errors	1 business day

39.2.2 2.2 Security Incidents

Categories: - Malware infections - Phishing attacks - Unauthorized access - Data breaches - DDoS attacks - Insider threats

All security incidents at least P2

39.3 3. Incident Response Process

39.3.1 3.1 Detection & Reporting

Reporting Channels: - **IT Support:** {{ meta.support.phone }}, {{ meta.support.email }} - **Security Team:** {{ meta.security.email }}, {{ meta.security.phone }} - **Self-Service Portal:** {{ meta.itsm.portal }}

Required Information: - Description of problem - Affected systems/users - Time of occurrence - Impact

39.3.2 3.2 Triage & Classification

Process: 1. Create incident ticket 2. Determine severity level 3. Assign category 4. Assign to responsible team 5. First response within SLA

Escalation: - P1: Immediate escalation to on-call - P2: Escalation after 1 hour without progress - Security incidents: Parallel to security team

39.3.3 3.3 Investigation & Diagnosis

Steps: 1. Analyze symptoms 2. Check logs 3. Identify affected systems 4. Determine root cause 5. Identify workaround (if possible)

Documentation: - Document all steps in ticket - Attach logs and screenshots - Timestamps for all actions

39.3.4 3.4 Resolution & Recovery

Process: 1. Implement fix or apply workaround 2. Perform functional test 3. Inform users 4. Monitor for recurrence

Verification: - User confirms resolution - Monitoring shows normal values - No further reports

39.3.5 3.5 Closure & Post-Incident Review

Closure: - Close ticket after user confirmation - Complete documentation - Verify categorization

Post-Incident Review (PIR): - Mandatory for P1/P2 incidents - Within 7 days after closure - Document lessons learned - Define improvement measures

39.4 4. Major Incident Management

39.4.1 4.1 Major Incident Criteria

An incident is "Major" when: - Severity P1 - Multiple critical services affected - Many users affected (> 100) - Media attention possible - Regulatory reporting obligation

39.4.2 4.2 Major Incident Team

Roles: - **Incident Manager:** Coordination, communication - **Technical Lead:** Technical solution - **Communications Lead:** Stakeholder communication - **Security Lead:** For security incidents - **Management Representative:** Decisions

Availability: 24/7 on-call rotation

39.4.3 4.3 Major Incident Process

Phase 1: Mobilization (0-15 minutes) 1. Declare major incident 2. Alert major incident team 3. Establish war room (physical or virtual) 4. Set up incident bridge (conference call)

Phase 2: Containment (15-60 minutes) 1. Limit impact 2. Implement workaround (if possible) 3. Inform stakeholders 4. Intensify monitoring

Phase 3: Resolution (variable) 1. Identify root cause 2. Implement permanent solution 3. Gradual restoration 4. Verification

Phase 4: Recovery (variable) 1. All services restored 2. Monitoring at normal state 3. Inform users 4. End major incident

Phase 5: Post-Incident Review (within 48 hours) 1. Reconstruct timeline 2. Root cause analysis 3. Lessons learned 4. Define action items 5. Management report

39.4.4 4.4 Communication

Internal Communication: - Status updates every 30 minutes - Stakeholder notifications - Intranet status page

External Communication: - Customer notifications (if applicable) - Media statement (if needed) - Regulatory notifications

39.5 5. Security Incident Response

39.5.1 5.1 Security Incident Response Team (SIRT)

Members: - CISO or Security Lead - IT security analysts - IT forensics expert - Legal/Compliance - HR (for insider threats)

39.5.2 5.2 Security Incident Process

Phase 1: Preparation - Incident response plan current - Tools and playbooks ready - Team trained

Phase 2: Identification - Security event detected (SIEM, EDR, etc.) - Triage: Is it an incident? - Determine severity

Phase 3: Containment - **Short-term:** Immediate measures (lock account, isolate network) - **Long-term:** Permanent isolation

Phase 4: Eradication - Remove malware - Patch vulnerabilities - Change compromised credentials

Phase 5: Recovery - Restore systems - Intensify monitoring - Gradual return to normal operations

Phase 6: Lessons Learned - Post-incident review - Playbook updates - Identify training needs

39.5.3 5.3 Forensics

When Required: - Data breaches - Insider threats - Legal investigations - Severe security incidents

Process: 1. **Preservation:** Secure evidence 2. **Collection:** Collect data (disk images, logs, memory dumps) 3. **Analysis:** Forensic analysis 4. **Reporting:** Forensics report 5. **Chain of Custody:** Complete documentation

Tools: {{ meta.security.forensics_tools }}

39.5.4 5.4 Reporting Obligations

Internal: - CISO: Immediately - Management: Within 4 hours - Data Protection Officer: For data breaches

External: - **GDPR:** Data protection authority within 72 hours (for data breaches) - **Affected Individuals:** Without undue delay - **Law Enforcement:** For criminal acts

39.6 6. Incident Communication

39.6.1 6.1 Status Updates

Frequency: - P1: Every 30 minutes - P2: Every 2 hours - P3/P4: Daily

Channels: - Email to stakeholders - Status page ({{ meta.status.url }}) - Intranet notifications

39.6.2 6.2 Stakeholder Matrix

Stakeholder	P1	P2	P3	P4
Affected users	Immediately	1h	4h	1d
Management	15min	2h	-	-
CISO (Security)	Immediately	Immediately	4h	-
Customers (external)	1h	4h	-	-

39.7 7. Compliance and Audit

39.7.1 7.1 Key Performance Indicators (KPIs)

Metric	Target Value
P1 response time	< 15 minutes
P1 resolution time	< 4 hours
Major incident PIR completion	100%
Security incident detection time	< 1 hour

39.7.2 7.2 Audit Evidence

- Incident tickets and logs
- Post-incident review reports
- Communication logs
- Forensics reports (for security incidents)

39.8 8. References

39.8.1 Internal Documents

- `0400_Policy_Incident_Management.md`
- `0320_Policy_Logging_and_Monitoring.md`

39.8.2 External Standards

- **ISO/IEC 27001:2022 Annex A.5.24** - Information security incident management planning
- **ISO/IEC 27001:2022 Annex A.5.25** - Assessment and decision on information security events
- **ISO/IEC 27001:2022 Annex A.5.26** - Response to information security incidents
- **NIST SP 800-61** - Computer Security Incident Handling Guide

---

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 40

Policy: Backup and Recovery

Document ID: 0420
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.8.13 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

40.1 1. Purpose

This policy defines the principles for backup and recovery at **AdminSend GmbH**. It ensures that critical data and systems can be restored in case of data loss, corruption, or disasters.

40.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Systems:** All IT systems, databases, applications, file systems, VMs, cloud resources
- **Data:** All business-critical and personal data
- **Backup Types:** Full, incremental, differential, snapshot, cloud backup
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

40.3 3. Principles (Policy Statements)

40.3.1 3.1 Backup Strategy Based on RPO/RTO

Backup strategies are defined based on Recovery Point Objective (RPO) and Recovery Time Objective (RTO): - **Critical Systems:** RPO < 1 hour, RTO < 4 hours - **Important Systems:** RPO < 24 hours, RTO < 24 hours - **Standard Systems:** RPO < 7 days, RTO < 72 hours

40.3.2 3.2 3-2-1 Backup Rule

Backups follow the 3-2-1 rule: - **3** copies of data (original + 2 backups) - **2** different storage media/technologies - **1** copy offsite/offline (air-gapped or geographically separated)

40.3.3 3.3 Encrypted Backups

All backups are stored encrypted (at rest) and transmitted encrypted (in transit). Encryption keys are securely managed and stored separately from backups.

40.3.4 3.4 Regular Backup Tests

Backups are regularly tested to ensure recoverability: - **Critical Systems:** Monthly restore tests - **Important Systems:** Quarterly restore tests - **Standard Systems:** Annual restore tests

40.3.5 3.5 Immutable Backups

Critical backups are stored as immutable to provide protection against ransomware and accidental deletion.

40.3.6 3.6 Backup Monitoring and Alerting

Backup jobs are continuously monitored. Failed backups trigger immediate alerts and are prioritized for remediation.

40.3.7 3.7 Retention and Preservation

Backups are retained according to legal, regulatory, and business requirements: - **Daily Backups:** 30 days - **Weekly Backups:** 12 weeks - **Monthly Backups:** 12 months - **Annual Backups:** 7 years (or per compliance requirements)

40.3.8 3.8 Disaster Recovery Integration

Backup strategies are integrated into disaster recovery and business continuity plans.

40.4 4. Roles and Responsibilities

40.4.1 RACI Matrix: Backup and Recovery

Activity	CISO	Backup Administrator	IT Operations	System Owner	BCM Manager
Policy creation	R/A	C	C	C	C
Backup configuration	C	R/A	C	C	I
Backup execution	I	R/A	C	I	I
Backup monitoring	C	R/A	C	I	I
Restore tests	C	R	R	R/A	C
Disaster recovery	A	C	R	C	R
Compliance review	R/A	C	I	I	C

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

40.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **Backup Administrator:** {{ meta.it.backup_admin }}
- **BCM Manager:** {{ meta.bcm.manager }}
- **Implementation Responsible:** IT Operations, System Owners
- **Control/Audit Function:** ISMS, Internal Audit

40.5 5. Derivations (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

40.5.1 Related Guidelines

- **0430__Guideline__Backup__Restore__and__Regular__Tests.md** - Detailed implementation guideline
- `0440_Policy_Business_Continuity_ICT_Readiness.md` - Business Continuity Policy
- `0260_Policy_Cryptography_and_Key_Management.md` - Cryptography Policy
- `0580_Policy_Retention_and_Deletion.md` - Retention Policy

40.5.2 Related Standards/Baselines

- RPO/RTO matrix
- Backup schedule
- Retention requirements

- Restore test procedures

40.5.3 Related Processes

- Backup process
- Restore process
- Backup test process
- Disaster recovery process

40.6 6. Compliance, Monitoring and Enforcement

40.6.1 Metrics and KPIs

- Backup success rate (target: 99.9%)
- Number of failed backups
- Average backup duration
- Restore success rate (target: 100%)
- Average restore duration (RTO compliance)
- Backup test completion rate (target: 100%)

40.6.2 Evidence and Proof

- Backup logs and job status
- Restore test protocols
- Backup monitoring reports
- Disaster recovery test reports
- Compliance evidence (retention)
- Backup compliance audit reports

40.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Missing backups:** Immediate remediation, investigation - **Untested backups:** Completion, retraining - **Unencrypted backups:** Immediate encryption, investigation - **Repeated violations:** Employment consequences

40.7 7. Exceptions

Exceptions to this policy are only permitted in justified cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and System Owner
- **Documentation:** All exceptions are documented in the risk register
- **Time Limitation:** Exceptions are generally time-limited
- **Compensating Controls:** Exceptions require alternative security measures

40.8 8. References

40.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0430_Guideline_Backup_Restore_and_Regular_Tests.md` - Detailed Guideline
- `0440_Policy_Business_Continuity_ICT_Readiness.md` - Business Continuity Policy
- `0080_ISMS_Risk_Register_Template.md` - Risk Register

40.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.8.13** - Information backup
- **ISO/IEC 27002:2022** - Information security controls
- **ISO 22301** - Business Continuity Management
- **GDPR (EU 2016/679)** - General Data Protection Regulation (backup of personal data)

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 41

Guideline: Backup, Restore and Regular Tests

Document ID: 0430
Document Type: Guideline (detailed)
Related Policy: 0420_Policy_Backup_and_Recovery.md
Standard Reference: ISO/IEC 27001:2022 Annex A.8.13
Owner: {{ meta.it_operations.manager }}
Version: 1.0
Status: Approved
Classification: Confidential
Last Updated: {{ meta.document.date }}

41.1 1. Purpose and Scope

This guideline implements the `0420_Policy_Backup_and_Recovery.md` and defines: - Backup strategies and frequencies - Restore processes and tests - Backup monitoring and verification

Scope: All data and systems at **AdminSend GmbH**

41.2 2. Backup Strategy

41.2.1 2.1 3-2-1 Rule

Principle: - **3** copies of data (1 production + 2 backups) - **2** different media types (e.g., disk + tape/cloud) - **1** copy off-site (geographically separated)

41.2.2 2.2 Backup Types

Full Backup: - Complete backup of all data - Frequency: Weekly (Sunday) - Longest restore time, but simplest recovery

Incremental Backup: - Only changes since last backup - Frequency: Daily - Fastest backup, longer restore time

Differential Backup: - Changes since last full backup - Frequency: Optional, as needed - Balance between full and incremental

41.2.3 2.3 Backup Frequencies

System Type	Full	Incremental	RPO	RTO
Critical databases	Daily	Hourly	1h	4h
Production servers	Weekly	Daily	24h	8h
File servers	Weekly	Daily	24h	8h
Workstations	Monthly	Weekly	7d	24h
Email	Daily	Hourly	1h	4h

RPO (Recovery Point Objective): Maximum data loss
RTO (Recovery Time Objective): Maximum recovery time

41.3 3. Backup Implementation

41.3.1 3.1 Backup Systems

On-Premises: - **Backup Server:** {{ meta.backup.server }} - **Backup Software:** {{ meta.backup.software }} (e.g., Veeam, Commvault) - **Storage:** {{ meta.backup.storage }} (disk, tape)

Cloud Backup: - **Cloud Provider:** {{ meta.cloud.backup_provider }} (e.g., Azure Backup, AWS Backup) - **Encryption:** AES-256 - **Geo-Redundancy:** Enabled

41.3.2 3.2 Backup Windows

Production Systems: - Backup window: 22:00 - 06:00 - Minimal performance impact - Monitoring during backup

Development Systems: - Backup window: Anytime - No performance requirements

41.3.3 3.3 Encryption

In Transit: - TLS 1.2+ for backup transmission - VPN for off-site backups

At Rest: - AES-256 encryption of all backups - Key management via Key Vault - Separate keys for backups

41.3.4 3.4 Retention

Retention Scheme (GFS - Grandfather-Father-Son): - **Daily:** 7 days - **Weekly:** 4 weeks - **Monthly:** 12 months - **Yearly:** {{ meta.retention.backup_years }} years

Compliance Backups: - Financial data: 10 years - Personnel data: Per GDPR - Emails: {{ meta.retention.email_years }} years

41.4 4. Restore Processes

41.4.1 4.1 Restore Types

File-Level Restore: - Individual files or folders - Self-service for users (limited) - IT support for extensive restores

System-Level Restore: - Complete server recovery - Bare-metal recovery - Only by IT operations

Database Restore: - Point-in-time recovery - Transaction logs - Only by database admins

41.4.2 4.2 Restore Process

Step 1: Request - Create ticket with details (what, when, why) - Approval by supervisor (for extensive restores)

Step 2: Preparation - Check backup catalog - Prepare restore target - Plan downtime (if required)

Step 3: Restore - Perform restore - Monitor progress - Error handling

Step 4: Verification - Check data integrity - Functional test - User confirmation

Step 5: Documentation - Restore log - Lessons learned - Close ticket

41.4.3 4.3 Disaster Recovery

In Case of Total Failure: 1. Activate disaster recovery plan 2. Provide alternative infrastructure 3. Restore critical systems first 4. Gradual restoration of additional systems 5. Verification and return to normal operations

Details: See `0160_Disaster_Recovery_and_Business_Continuity.md` (IT Operation Templates)

41.5 5. Backup Monitoring

41.5.1 5.1 Monitored Metrics

Backup Jobs: - Successful/failed backups - Backup duration - Backup size - Change rate

Storage: - Available storage space - Growth rate - Deduplication rate

Performance: - Backup speed - Network utilization - Storage performance

41.5.2 5.2 Alerting

Critical Alerts: - Backup failed (2x consecutive) - Storage > 90% full - Backup window exceeded - Encryption failed

Escalation: - First notification: Backup admin - After 2 hours: IT Operations Manager - After 4 hours: CISO (for critical systems)

41.5.3 5.3 Reporting

Daily Backup Report: - Status of all backup jobs - Failed backups - Storage utilization

Monthly Management Report: - Backup success rate - Restore statistics - Capacity planning - Compliance status

41.6 6. Backup Tests

41.6.1 6.1 Test Frequencies

Test Type	Frequency	Execution
File-level restore	Monthly	Sample
System-level restore	Quarterly	Critical systems
Database restore	Monthly	Point-in-time recovery
Disaster recovery	Annually	Full DR test

41.6.2 6.2 Test Process

Planning: 1. Define test scope 2. Set test time window 3. Inform stakeholders 4. Prepare test environment

Execution: 1. Restore to test environment 2. Check data integrity 3. Functional test 4. Performance test 5. Time measurement (RTO verification)

Documentation: 1. Create test protocol 2. Document success/failure 3. Problems and lessons learned 4. Define improvement measures

Follow-up: 1. Clean up test environment 2. Adjust backup processes (if required) 3. Management report

41.6.3 6.3 Disaster Recovery Drill

Annual DR Test: - Simulation of total failure - Activation of DR plan - Restoration of critical systems - Time measurement and documentation - Management presentation

Participants: - IT operations - Application owners - Management - Business representatives

41.7 7. Backup Security

41.7.1 7.1 Access Control

Permissions: - **Backup Admins:** Full access to backup system - **System Admins:** Restore permission for own systems - **Users:** Self-service restore (limited)

Authentication: - MFA for backup system access - Privileged accounts for backup admins

41.7.2 7.2 Immutable Backups

Ransomware Protection: - Immutable backups (write-once-read-many) - Air-gapped backups (offline) - Separate credentials for backup storage

Retention Lock: - Backups cannot be deleted prematurely - Protection against accidental or malicious deletion

41.7.3 7.3 Audit Logging

Logged Events: - Backup job starts and ends - Restore requests and executions - Configuration changes - Access to backup system

Retention: {{ meta.retention.log_years }} years

41.8 8. Compliance and Audit

41.8.1 8.1 Key Performance Indicators (KPIs)

Metric	Target Value
Backup success rate	> 99%
Restore success rate	100%
RTO compliance	100%
RPO compliance	100%
Test completion rate	100%

41.8.2 8.2 Audit Evidence

- Backup logs and reports
- Restore test protocols
- DR drill documentation
- Compliance reports

41.9 9. References

41.9.1 Internal Documents

- `0420_Policy_Backup_and_Recovery.md`
- `0160_Disaster_Recovery_and_Business_Continuity.md` (IT Operation)

41.9.2 External Standards

- **ISO/IEC 27001:2022 Annex A.8.13** - Information backup
- **NIST SP 800-34** - Contingency Planning Guide

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 42

Policy: Business Continuity ICT Readiness

Document ID: 0440
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.5.29, A.5.30 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

42.1 1. Purpose

This policy defines the principles for ICT continuity and disaster recovery at **AdminSend GmbH**. It ensures that IT systems and services can continue or be quickly restored during disruptions to ensure business continuity.

42.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Systems:** All business-critical IT systems, applications, infrastructure, cloud services
- **Scenarios:** Natural disasters, cyberattacks, system failures, pandemics, supplier failures
- **Interfaces:** Integration with BCM (Business Continuity Management)
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

42.3 3. Principles (Policy Statements)

42.3.1 3.1 ICT Continuity Planning

ICT continuity plans exist for all business-critical IT services, defining recovery strategies, resources, and responsibilities.

42.3.2 3.2 Business Impact Analysis (BIA)

Regular business impact analyses identify critical IT services and their RPO/RTO requirements. The BIA is coordinated with the BCM team.

42.3.3 3.3 Redundancy and High Availability

Critical IT systems are designed with redundancy and high availability: - Redundant components (servers, storage, network) - Geographically distributed data centers - Load balancing and failover mechanisms - Cloud-based disaster recovery

42.3.4 3.4 Disaster Recovery Plans (DRP)

Detailed disaster recovery plans describe step-by-step procedures for restoring IT systems after a failure.

42.3.5 3.5 Regular Tests and Exercises

ICT continuity and DR plans are regularly tested: - **Critical Systems:** Annual DR tests - **Important Systems:** Every 2 years - **Tabletop Exercises:** Quarterly

42.3.6 3.6 Alternative Workplaces and Remote Work

Employees can work from alternative locations or remotely during site failures. Remote access infrastructure is designed for high availability.

42.3.7 3.7 Supplier and Cloud Provider Continuity

Critical suppliers and cloud providers are assessed for their business continuity capabilities. SLAs contain continuity requirements.

42.3.8 3.8 Incident-to-Crisis Escalation

Clear escalation paths define when an IT incident escalates to a business continuity crisis and the BCM team is activated.

42.4 4. Roles and Responsibilities

42.4.1 RACI Matrix: Business Continuity ICT Readiness

Activity	CISO	BCM Manager	IT Operations	CIO	Crisis Management Team
Policy creation	R/A	C	C	C	I
BIA execution	C	R/A	C	C	I
DRP creation	A	C	R	C	I
DR tests	A	C	R	C	I
Crisis activation	C	R/A	C	C	R
Recovery execution	A	C	R	R	C
Post-incident review	R/A	R	C	C	C

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

42.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **BCM Manager:** {{ meta.bcm.manager }}
- **DR Coordinator:** {{ meta.it.dr_coordinator }}
- **CIO:** Anna Schmidt
- **Implementation Responsible:** IT Operations, System Owners
- **Control/Audit Function:** ISMS, Internal Audit

42.5 5. Derivations (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

42.5.1 Related Guidelines

- **0450_Guideline_ICT_DR_Interfaces_to_BCM.md** - Detailed implementation guideline
- `0420_Policy_Backup_and_Recovery.md` - Backup Policy
- `0400_Policy_Incident_Management.md` - Incident Management Policy
- BCM Handbook (see `templates/en/bcm/`)

42.5.2 Related Standards/Baselines

- RPO/RTO matrix
- DR plan templates
- Test scenarios
- Escalation paths

42.5.3 Related Processes

- Business impact analysis process
- Disaster recovery process
- DR test process
- Crisis management process

42.6 6. Compliance, Monitoring and Enforcement

42.6.1 Metrics and KPIs

- Number of critical systems with DR plans (target: 100%)
- DR test completion rate (target: 100%)
- Average recovery time (RTO compliance)
- Number of successful DR tests
- BIA currency (target: annual update)
- Availability of critical systems (target: 99.9%)

42.6.2 Evidence and Proof

- Business impact analysis reports
- Disaster recovery plans
- DR test protocols
- Availability metrics
- Crisis management exercise protocols
- BCM/DR audit reports

42.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Missing DR plans:** Immediate creation, escalation - **Untested DR plans:** Completion, retraining - **RTO/RPO violations:** Root cause analysis, remediation - **Repeated violations:** Employment consequences

42.7 7. Exceptions

Exceptions to this policy are only permitted in justified cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and BCM Manager
- **Documentation:** All exceptions are documented in the risk register
- **Time Limitation:** Exceptions are generally time-limited
- **Compensating Controls:** Exceptions require alternative continuity measures

42.8 8. References

42.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy

- `0450_Guideline_ICT_DR_Interfaces_to_BCM.md` - Detailed Guideline
- `0420_Policy_Backup_and_Recovery.md` - Backup Policy
- BCM Handbook (`templates/en/bcm/`)

42.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.5.29** - Information security during disruption
- **ISO/IEC 27001:2022 Annex A.5.30** - ICT readiness for business continuity
- **ISO 22301** - Business Continuity Management Systems
- **ISO/IEC 27031** - ICT readiness for business continuity
- **BSI Standard 100-4** - Business Continuity Management

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 43

Guideline: ICT Disaster Recovery - Interfaces to BCM

Document ID: 0450
Document Type: Guideline (detailed)
Related Policy: 0440_Policy_Business_Continuity_ICT_Readiness.md
Standard Reference: ISO/IEC 27001:2022 Annex A.5.29, A.5.30
Owner: {{ meta.it_operations.manager }}
Version: 1.0
Status: Approved
Classification: Confidential
Last Updated: {{ meta.document.date }}

43.1 1. Purpose and Scope

This guideline implements the `0440_Policy_Business_Continuity_ICT_Readiness.md` and defines: - ICT disaster recovery plans and processes - Interfaces to Business Continuity Management (BCM) - ICT readiness for emergency situations

Scope: All IT systems and services at **AdminSend GmbH**

43.2 2. ICT Disaster Recovery Strategy

43.2.1 2.1 Recovery Objectives

RTO (Recovery Time Objective): | System Tier | RTO | Rationale | |————-|—|————| | Tier 1 (Critical) | 4 hours | Business-critical systems | | Tier 2 (Important) | 24 hours | Important business functions | | Tier 3 (Standard) | 72 hours | Standard IT services |

RPO (Recovery Point Objective): | System Tier | RPO | Backup Frequency | |————-|——|————–| | Tier 1 | 1 hour | Hourly | | Tier 2 | 24 hours | Daily | | Tier 3 | 7 days | Weekly |

43.2.2 2.2 DR Strategies

Hot Site: - Fully redundant infrastructure - Real-time replication - Immediate failover capability - For Tier 1 systems

Warm Site: - Partially pre-configured infrastructure - Regular backups - Activation within hours - For Tier 2 systems

Cold Site: - Basic infrastructure available - Recovery from backups - Activation within days - For Tier 3 systems

43.3 3. DR Infrastructure

43.3.1 3.1 Primary Data Center

Location: {{ netbox.site.primary }}
Systems: All production systems
Redundancy: N+1 for critical components

43.3.2 3.2 DR Site

Location: {{ netbox.site.dr }}
Distance: > 50 km from primary site
Systems: Replicated Tier 1 systems, backup infrastructure

43.3.3 3.3 Cloud DR

Cloud Provider: {{ meta.cloud.dr_provider }}
Regions: {{ meta.cloud.primary_region }}, {{ meta.cloud.dr_region }}
Services: IaaS for DR workloads

43.4 4. Interfaces to BCM

43.4.1 4.1 Business Impact Analysis (BIA)

ICT Input for BIA: - System dependencies - RTO/RPO capabilities - Single points of failure - Recovery costs

BIA Output for ICT: - Criticality of business processes - Maximum tolerable downtime (MTD) - Recovery prioritization

43.4.2 4.2 BCM Plans

ICT Contributions: - IT Disaster Recovery Plan (DRP) - Technical recovery procedures - IT personnel contact lists - Escalation paths

BCM Coordination: - Alignment with Business Continuity Plans (BCP) - Joint exercises and tests - Consistent communication

43.4.3 4.3 Crisis Management

ICT Role in Crisis Team: - IT representative in crisis team - Status updates on IT systems - Technical decision support - Coordination of IT recovery

43.5 5. DR Activation

43.5.1 5.1 Activation Criteria

Automatic Activation: - Complete failure of primary site - Critical infrastructure components failed - Natural disasters

Manual Activation: - Decision by crisis team - Planned failover tests - Maintenance activities

43.5.2 5.2 Activation Process

Phase 1: Assessment (0-30 minutes) 1. Assess extent of damage 2. Decide on DR activation 3. Inform crisis team 4. Mobilize DR team

Phase 2: Activation (30 minutes - 4 hours) 1. Activate DR infrastructure 2. Restore systems (by priority) 3. Switch network routing 4. Functional test

Phase 3: Operation (variable) 1. Operation in DR mode 2. Intensify monitoring 3. Regular status updates 4. Prepare return

Phase 4: Failback (planned) 1. Restore primary site 2. Synchronize data 3. Planned failback 4. Verification

43.6 6. DR Tests

43.6.1 6.1 Test Types

Tabletop Exercise: - Frequency: Quarterly - Walkthrough of DR plan - No technical activation

Partial Failover: - Frequency: Semi-annually - Individual systems failover - Minimal business impact

Full DR Drill: - Frequency: Annually - Complete failover of all Tier 1 systems - Planned downtime required

43.6.2 6.2 Test Documentation

Test Protocol: - Date, participants, scope - Steps performed - Measured RTO/RPO - Problems and lessons learned - Improvement measures

43.7 7. Compliance and Audit

43.7.1 7.1 Key Performance Indicators (KPIs)

Metric	Target Value
DR test success rate	100%

Metric	Target Value
RTO compliance (test)	100%
RPO compliance (test)	100%
DR plan currency	< 6 months

43.7.2 7.2 Audit Evidence

- DR plans and procedures
- Test protocols
- BIA documentation
- Failover logs

43.8 8. References

43.8.1 Internal Documents

- `0440_Policy_Business_Continuity_ICT_Readiness.md`
- `0430_Guideline_Backup_Restore_and_Regular_Tests.md`
- BCM Handbook (if available)

43.8.2 External Standards

- **ISO/IEC 27001:2022 Annex A.5.29** - Information security during disruption
- **ISO/IEC 27001:2022 Annex A.5.30** - ICT readiness for business continuity
- **ISO 22301** - Business Continuity Management

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 44

Policy: Supplier and Cloud Security

Document ID: 0460
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.5.19-A.5.23 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

44.1 1. Purpose

This policy defines the principles for supplier and cloud security management at **AdminSend GmbH**. It ensures that suppliers, service providers, and cloud providers meet security requirements and are securely managed throughout their entire lifecycle.

44.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Supplier Types:** IT service providers, cloud providers, SaaS vendors, outsourcing partners, subcontractors
- **Services:** IaaS, PaaS, SaaS, managed services, outsourcing
- **Lifecycle:** Selection, onboarding, operation, monitoring, offboarding
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

44.3 3. Principles (Policy Statements)

44.3.1 3.1 Third-Party Risk Assessment

All suppliers undergo a security risk assessment before contract signing. The assessment considers data access, criticality, and compliance requirements.

44.3.2 3.2 Contractual Security Requirements

Contracts with suppliers contain binding security requirements: - Information security clauses - Data protection requirements (GDPR) - Audit rights and evidence obligations - Incident notification obligations - Subcontractor regulations

44.3.3 3.3 Cloud Security Assessment

Cloud providers are evaluated according to recognized standards (ISO 27001, SOC 2, CSA STAR). The shared responsibility model is documented and understood.

44.3.4 3.4 Data Classification and Cloud Usage

Storage and processing of data in the cloud is based on data classification: - **Public:** All cloud services permitted - **Internal:** Approved cloud services with appropriate controls - **Confidential:** Only certified cloud services with encryption - **Strictly Confidential:** Only on-premise or dedicated cloud with enhanced controls

44.3.5 3.5 Supplier Lifecycle Management

Suppliers are managed throughout their entire lifecycle: - **Onboarding:** Security assessment, contract negotiation - **Operation:** Continuous monitoring, regular reviews - **Offboarding:** Secure data return/deletion, access revocation

44.3.6 3.6 Regular Supplier Reviews

Critical suppliers are reviewed annually. Reviews include security compliance, incident history, certifications, and performance.

44.3.7 3.7 Supply Chain Security

The security of the entire supply chain is considered. Suppliers must pass security requirements to their subcontractors.

44.3.8 3.8 Cloud Data Residency and Compliance

Data locations (data residency) are documented and comply with regulatory requirements (GDPR, Schrems II).

44.4 4. Roles and Responsibilities

44.4.1 RACI Matrix: Supplier and Cloud Security

Activity	CISO	Procurement	Legal	DPO	Business Owner	IT Operations
Policy creation	R/A	C	C	C	I	C
Risk assessment	R/A	C	C	C	C	C
Contract negotiation	C	R	R/A	C	C	I
Security review	R/A	I	I	C	C	C
Supplier monitoring	A	C	I	I	C	R
Cloud security assessment	R/A	C	I	C	C	C
Offboarding	C	C	I	C	C	R/A

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

44.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **Third-Party Risk Manager:** {{ meta.security.tprm_manager }}
- **Cloud Security Architect:** {{ meta.security.cloud_architect }}
- **Data Protection Officer:** {{ meta.dpo.name }}
- **Implementation Responsible:** Procurement, Legal, IT Operations
- **Control/Audit Function:** ISMS, Internal Audit

44.5 5. Derivations (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

44.5.1 Related Guidelines

- **0470_Guideline_Third_Party_Risk_Assessment_and_Cloud_Controls.md** - Detailed implementation guideline
- `0280_Policy_Data_Classification_and_Information_Handling.md` - Data Classification Policy
- `0560_Policy_Data_Protection_Interfaces.md` - Data Protection Policy
- `0440_Policy_Business_Continuity_ICT_Readiness.md` - Business Continuity Policy

44.5.2 Related Standards/Baselines

- Third-party risk assessment framework
- Cloud security assessment criteria
- Contractual security clauses (templates)
- Supplier security scorecard

44.5.3 Related Processes

- Third-party risk management process
- Cloud service approval process
- Supplier review process
- Supplier offboarding process

44.6 6. Compliance, Monitoring and Enforcement

44.6.1 Metrics and KPIs

- Number of suppliers with current security assessment (target: 100% of critical suppliers)
- Average supplier security score
- Number of supplier security incidents
- Cloud service approval rate
- Supplier review completion rate (target: 100% annually)
- Number of unapproved cloud services (shadow IT)

44.6.2 Evidence and Proof

- Third-party risk assessments
- Supplier security scorecards
- Contracts with security clauses
- Cloud security assessments
- Supplier review reports
- Supplier security audit reports

44.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Use of unapproved cloud services:** Immediate deactivation, investigation - **Missing risk assessments:** Completion, contract suspension - **Supplier security incidents:** Incident response, contract review - **Repeated violations:** Contract termination, employment consequences

44.7 7. Exceptions

Exceptions to this policy are only permitted in justified cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and Business Owner
- **Documentation:** All exceptions are documented in the risk register
- **Time Limitation:** Exceptions are generally time-limited
- **Compensating Controls:** Exceptions require alternative security measures

44.8 8. References

44.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy

- `0470_Guideline_Third_Party_Risk_Assessment_and_Cloud_Controls.md` - Detailed Guideline
- `0280_Policy_Data_Classification_and_Information_Handling.md` - Data Classification Policy
- `0080_ISMS_Risk_Register_Template.md` - Risk Register

44.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.5.19** - Information security in supplier relationships
- **ISO/IEC 27001:2022 Annex A.5.20** - Addressing information security within supplier agreements
- **ISO/IEC 27001:2022 Annex A.5.21** - Managing information security in the ICT supply chain
- **ISO/IEC 27001:2022 Annex A.5.22** - Monitoring, review and change management of supplier services
- **ISO/IEC 27001:2022 Annex A.5.23** - Information security for use of cloud services
- **ISO/IEC 27017** - Cloud Security Controls
- **ISO/IEC 27018** - Cloud Privacy
- **CSA STAR** - Cloud Security Alliance Security, Trust & Assurance Registry
- **GDPR (EU 2016/679)** - Art. 28 - Data processing

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 45

Guideline: Third-Party Risk Assessment and Cloud Controls

Document ID: 0470
Document Type: Guideline (detailed)
Associated Policy: 0460_Policy_Supplier_and_Cloud_Security.md
Standard Reference: ISO/IEC 27001:2022 Annex A.5.19, A.5.20, A.5.21, A.5.22, A.5.23
Owner: {{ meta.procurement.manager }}
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}

45.1 1. Purpose and Scope

This guideline specifies the `0460_Policy_Supplier_and_Cloud_Security.md` and defines: - Third-Party Risk Assessment processes - Cloud Security Controls and Compliance - Supplier management and monitoring

Scope: All suppliers and cloud services at **AdminSend GmbH**

45.2 2. Third-Party Risk Assessment

45.2.1 2.1 Supplier Categorization

Criticality: | Category | Definition | Examples | Assessment Depth | |———-|————|———-|———————| | Critical | Access to confidential data or critical systems | Cloud providers, Managed Security Services | Comprehensive | | High | Important business services | ERP vendors, Payment providers | Detailed | | Medium | Standard services | Office software, Marketing tools | Standard | | Low | Minimal impact | Office supplies, Catering | Minimal |

45.2.2 2.2 Pre-Contract Assessment

Phase 1: Initial Screening - Security controls questionnaire - Certifications (ISO 27001, SOC 2) - Data protection compliance (GDPR) - Financial stability

Phase 2: Detailed Assessment (Critical/High) - Security audit or on-site visit - Penetration test reports - Incident response capabilities - Business continuity plans

Phase 3: Contract Negotiation - Security clauses in contract - SLAs for security and availability - Audit rights - Incident notification obligations

45.2.3 2.3 Ongoing Monitoring

Frequency: - Critical: Quarterly review - High: Semi-annually - Medium: Annually - Low: At contract renewal

Monitoring Activities: - Check certification status - Security incidents at supplier - Request compliance reports - Performance against SLAs

45.2.4 2.4 Offboarding

Process: 1. Data return or deletion 2. Revoke access 3. Confirm confidentiality obligations 4. Final documentation

45.3 3. Cloud Security Controls

45.3.1 3.1 Cloud Service Models

IaaS (Infrastructure as a Service): - Shared Responsibility Model - Customer responsible for OS, applications, data - Provider responsible for infrastructure

PaaS (Platform as a Service): - Provider responsible for platform - Customer responsible for applications, data

SaaS (Software as a Service): - Provider responsible for everything except data - Customer responsible for data and access control

45.3.2 3.2 Cloud Security Assessment

Before Cloud Adoption: - Cloud Security Posture Assessment - Check data residency and compliance - Evaluate encryption options - Backup and DR capabilities

Cloud Security Controls: - Identity and Access Management (IAM) - Network segmentation - Encryption (at rest, in transit) - Logging and monitoring - Compliance certifications

45.3.3 3.3 Cloud Access Security Broker (CASB)

Functions: - Visibility into cloud usage - Data Loss Prevention (DLP) - Threat Protection - Compliance monitoring

CASB System: {{ meta.security.casb_solution }}

45.3.4 3.4 Multi-Cloud and Hybrid-Cloud

Governance: - Unified security policies across all clouds - Central identity provider (SSO) - Consistent monitoring

Cloud Providers: - Primary: {{ meta.cloud.primary_provider }} - Secondary: {{ meta.cloud.secondary_provider }}

45.4 4. Contract Management

45.4.1 4.1 Security Clauses

Mandatory Clauses: - Data protection and GDPR compliance - Security controls and standards - Incident notification (within 24 hours) - Audit rights - Data return at contract end - Liability for data breaches

45.4.2 4.2 Service Level Agreements (SLAs)

Security SLAs: - Availability (e.g., 99.9%) - Incident response time - Patch management timeframe - Backup frequency and retention

45.4.3 4.3 Data Processing Agreements (DPA)

GDPR Requirements: - Data Processing Agreement (DPA) - Technical and organizational measures (TOMs) - Sub-processor list - Data transfer to third countries

45.5 5. Supplier Risk Management

45.5.1 5.1 Risk Register

Documentation: - Supplier, service, criticality - Identified risks - Mitigation measures - Residual risk - Review date

45.5.2 5.2 Incident Management

For Supplier Incidents: 1. Notification by supplier (SLA: 24h) 2. Impact assessment 3. Coordinate mitigation measures 4. Inform own customers (if required) 5. Post-incident review

45.5.3 5.3 Business Continuity

Supplier Failure Scenarios: - Identify alternative suppliers - Define exit strategy - Ensure data portability

45.6 6. Compliance and Audit

45.6.1 6.1 Metrics (KPIs)

Metric	Target Value
Suppliers with current assessment	100%

Metric	Target Value
Critical suppliers with ISO 27001	> 90%
SLA compliance	> 95%
Incident notification compliance	100%

45.6.2 6.2 Audit Evidence

- Supplier assessments
- Contracts with security clauses
- SLA reports
- Incident documentation

45.7 7. References

45.7.1 Internal Documents

- `0460_Policy_Supplier_and_Cloud_Security.md`
- `0400_Policy_Incident_Management.md`

45.7.2 External Standards

- **ISO/IEC 27001:2022 Annex A.5.19** - Information security in supplier relationships
- **ISO/IEC 27001:2022 Annex A.5.20** - Addressing information security within supplier agreements
- **ISO/IEC 27001:2022 Annex A.5.21** - Managing information security in the ICT supply chain
- **ISO/IEC 27001:2022 Annex A.5.22** - Monitoring, review and change management of supplier services
- **ISO/IEC 27001:2022 Annex A.5.23** - Information security for use of cloud services

---

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 46

Policy: Physical Security

Document ID: 0480
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.7.1-A.7.4 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

46.1 1. Purpose

This policy defines the principles for physical security at **AdminSend GmbH**. It ensures that physical access to facilities, equipment, and information is controlled and monitored to prevent unauthorized access, theft, and damage.

46.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Facilities:** Offices, data centers, server rooms, warehouses, production facilities
- **Assets:** IT equipment, servers, network components, mobile devices, documents
- **Persons:** Employees, visitors, contractors, suppliers
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

46.3 3. Principles (Policy Statements)

46.3.1 3.1 Perimeter Security

Physical security areas are protected by perimeter security (fences, walls, security doors). Entry points are controlled and monitored.

46.3.2 3.2 Access Control

Access to sensitive areas is controlled: - Electronic access control systems (badge, biometrics) - Visitor management and escort requirements - Logging of all access - Regular review of access rights

46.3.3 3.3 Security Zones

Facilities are divided into security zones: - **Public:** Reception, meeting rooms - **Internal:** Offices, workspaces - **Restricted:** Server rooms, data centers - **High Security:** Critical infrastructure, vault rooms

46.3.4 3.4 Video Surveillance

Critical areas are video monitored. Recordings are stored and protected according to data protection requirements.

46.3.5 3.5 Protection Against Environmental Hazards

IT equipment is protected against environmental hazards: - Fire protection (smoke detectors, extinguishing systems) - Air conditioning and temperature monitoring - Water protection (leak detection) - Power supply (UPS, emergency generators)

46.3.6 3.6 Secure Disposal

Physical media and documents are securely disposed of (shredding, incineration, certified disposal).

46.3.7 3.7 Clear Desk and Clear Screen

Workspaces are cleared when absent (Clear Desk). Screens are locked (Clear Screen).

46.3.8 3.8 Equipment Security

IT equipment is protected against theft (Kensington locks, alarm systems, inventory management).

46.4 4. Roles and Responsibilities

46.4.1 RACI Matrix: Physical Security

Activity	CISO	Facility Management	Security	IT Operations	HR
Policy Creation	R/A	C	C	C	I

Activity	CISO	Facility Management	Security	IT Operations	HR
Access Control	C	R/A	R	I	C
Visitor Management	I	R/A	R	I	C
Video Surveillance	C	R/A	R	I	C
Environmental Protection	C	R/A	I	C	I
Equipment Security	C	C	I	R/A	I
Compliance Review	R/A	C	C	I	I

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

46.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **Facility Manager:** {{ meta.facility.manager }}
- **Security Manager:** {{ meta.security.physical_security_manager }}
- **Implementation Responsible:** Facility Management, Security, IT Operations
- **Control/Audit Function:** ISMS, Internal Audit

46.5 5. Derivatives (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

46.5.1 Associated Guidelines

- **0490_Guideline_Access_Visitors_and_Equipment_Protection.md** - Detailed implementation guideline
- `0300_Policy_Asset_Management.md` - Asset Management Policy
- `0560_Policy_Data_Protection_Interfaces.md` - Data Protection Policy (video surveillance)

46.5.2 Associated Standards/Baselines

- Security zones concept
- Access control matrix
- Visitor management process
- Video surveillance guideline

46.5.3 Associated Processes

- Access control process

- Visitor management process
- Incident response for physical security incidents
- Equipment disposal process

46.6 6. Compliance, Monitoring and Enforcement

46.6.1 Metrics and KPIs

- Number of unauthorized access attempts
- Number of visitors and compliance with escort requirements
- Number of physical security incidents (theft, break-in)
- Access control system availability (Target: 99.9%)
- Clear Desk/Clear Screen compliance rate
- Number of lost or stolen assets

46.6.2 Evidence and Proof

- Access control logs
- Visitor logs
- Video surveillance recordings
- Security incident reports
- Facility audit reports
- Equipment inventory

46.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Unauthorized Access:** Immediate escalation, investigation - **Tailgating:** Warning, retraining - **Clear Desk/Screen Violations:** Warning, retraining - **Repeated Violations:** Employment consequences

46.7 7. Exceptions

Exceptions to this policy are only permitted in justified exceptional cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and Facility Manager
- **Documentation:** All exceptions are documented in the risk register
- **Time Limitation:** Exceptions are generally time-limited

46.8 8. References

46.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0490_Guideline_Access_Visitors_and_Equipment_Protection.md` - Detailed Guideline
- `0300_Policy_Asset_Management.md` - Asset Management Policy
- `0080_ISMS_Risk_Register_Template.md` - Risk Register

46.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.7.1** - Physical security perimeters
- **ISO/IEC 27001:2022 Annex A.7.2** - Physical entry
- **ISO/IEC 27001:2022 Annex A.7.3** - Securing offices, rooms and facilities
- **ISO/IEC 27001:2022 Annex A.7.4** - Physical security monitoring
- **GDPR (EU 2016/679)** - Data protection for video surveillance
- **BSI IT-Grundschutz** - Module INF.1 General Building

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 47

Guideline: Access, Visitors and Equipment Protection

Document ID: 0490
Document Type: Guideline (detailed)
Associated Policy: 0480_Policy_Physical_Security.md
Standard Reference: ISO/IEC 27001:2022 Annex A.7.1, A.7.2, A.7.3, A.7.4
Owner: {{ meta.facilities.manager }}
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}

47.1 1. Purpose and Scope

This guideline specifies the `0480_Policy_Physical_Security.md` and defines: - Access control systems and processes - Visitor management - Physical protection of IT equipment

Scope: All locations of **AdminSend GmbH**

47.2 2. Security Zones

47.2.1 2.1 Zone Classification

Zone 1 (Public): - Reception area, lobby - No access control - Video surveillance

Zone 2 (Internal): - Office areas, meeting rooms - Access card required - Employees and registered visitors

Zone 3 (Restricted): - Server rooms, data centers - Additional authentication (PIN, biometrics) - Authorized personnel only

Zone 4 (High Security): - Critical infrastructure - Four-eyes principle - Video surveillance and logging

47.3 3. Access Control System

47.3.1 3.1 Access Cards

Card Type: RFID cards with photo
Issuance: During onboarding by HR
Validity: Until contract end

Card Loss: 1. Immediate report to Security 2. Disable card (within 15 minutes) 3. Issue new card 4. Documentation

47.3.2 3.2 Biometric Authentication

For Zone 3/4: - Fingerprint scanner - Iris scanner (optional) - Data protection compliant (GDPR)

47.3.3 3.3 Access Logs

Logging: - All access attempts (success and failure) - Timestamp, person, door/zone - Retention: {{ meta.retention.access_years }} years

Monitoring: - Alerts for unauthorized access attempts - Alerts for access outside business hours (Zone 3/4)

47.4 4. Visitor Management

47.4.1 4.1 Visitor Registration

Process: 1. Host pre-registers visitor (email, portal) 2. Visitor reports to reception 3. ID check (ID card, driver's license) 4. Issue visitor badge 5. Host picks up visitor

Visitor Badge: - Temporary RFID card - Validity: 1 day - Automatic deactivation after expiration

47.4.2 4.2 Escort

Requirement: - Visitors must be escorted at all times - No unaccompanied visitors in Zone 2/3/4 - Host responsible

Exceptions: - Long-term contractors with own badge - After background check and NDA

47.4.3 4.3 Visitor Log

Documentation: - Name, company, ID number - Host, purpose of visit - Entry and exit time - Retention: {{ meta.retention.visitor_years }} years

47.5 5. Physical Protection of Equipment

47.5.1 5.1 Server Rooms and Data Centers

Requirements: - Air conditioning (18-27°C, 40-60% humidity) - Fire detection and suppression system - Uninterruptible power supply (UPS) - Emergency generator - Water sensors (leak detection)

Access Control: - Zone 3 or 4 - Logging of all access - Video surveillance

47.5.2 5.2 Workspaces

Clean Desk Policy: - No confidential documents on desk (end of day) - Screen lock when absent - Lockable cabinets for confidential materials

Kensington Locks: - Mandatory for laptops in offices - Theft protection

47.5.3 5.3 Mobile Devices

Security Requirements: - Encryption (BitLocker, FileVault) - Remote wipe capability (MDM) - No confidential data locally (prefer cloud storage)

In Case of Loss: 1. Immediate report to IT support 2. Trigger remote wipe 3. Create incident ticket 4. Police report (in case of theft)

47.6 6. Video Surveillance

47.6.1 6.1 Monitored Areas

Cameras: - Entrances and exits - Server rooms (Zone 3/4) - Parking lots - No surveillance in offices, restrooms, changing rooms

47.6.2 6.2 Data Protection

GDPR Compliance: - Signs indicating video surveillance - Purpose limitation (security, access control) - Access only for authorized personnel - Retention: 30 days (then automatic deletion)

47.7 7. Emergency Access

47.7.1 7.1 Break-Glass Procedure

For Emergencies: - Physical key in sealed envelope - Storage in safe - Use only in emergencies (fire, medical emergency) - Documentation of each use

47.7.2 7.2 Evacuation

Evacuation Plan: - Escape routes marked - Assembly points defined - Regular evacuation drills (annually)

47.8 8. Compliance and Audit

47.8.1 8.1 Metrics (KPIs)

Metric	Target Value
Unescorted visitors	0
Access card losses	< 5 per year
Clean-desk compliance	$> 90\%$
Evacuation drills	1 per year

47.8.2 8.2 Audit Evidence

- Access logs
- Visitor logs
- Video recordings (30 days)
- Evacuation drill protocols

47.9 9. References

47.9.1 Internal Documents

- `0480_Policy_Physical_Security.md`
- `0300_Policy_Asset_Management.md`

47.9.2 External Standards

- **ISO/IEC 27001:2022 Annex A.7.1** - Physical security perimeters
- **ISO/IEC 27001:2022 Annex A.7.2** - Physical entry
- **ISO/IEC 27001:2022 Annex A.7.3** - Securing offices, rooms and facilities
- **ISO/IEC 27001:2022 Annex A.7.4** - Physical security monitoring

---

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 48

Policy: Mobile Device and Remote Work

Document ID: 0500
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.6.7, A.6.8, A.8.9 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

48.1 1. Purpose

This policy defines the principles for Mobile Device Management and Remote Work at **AdminSend GmbH**. It ensures that mobile devices and remote access are securely managed and comply with the organization's security requirements.

48.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Devices:** Laptops, smartphones, tablets, wearables (corporate-owned and BYOD)
- **Access Methods:** VPN, Remote Desktop, cloud services, mobile apps
- **Persons:** All employees, contractors with remote access
- **Locations:** {{ netbox.site.name }}, home office, public places, travel

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

48.3 3. Principles (Policy Statements)

48.3.1 3.1 Mobile Device Management (MDM)

All mobile devices with access to corporate resources are managed through an MDM system. MDM enables configuration, monitoring, and remote wipe.

48.3.2 3.2 BYOD (Bring Your Own Device)

Personal devices may only be used for business purposes after approval and enrollment in MDM. BYOD devices are subject to the same security requirements as corporate devices.

48.3.3 3.3 Device Encryption

All mobile devices must be fully encrypted (Full Disk Encryption). Encryption is enforced and monitored through MDM.

48.3.4 3.4 Secure Remote Access

Remote access to corporate resources is exclusively through secure channels: - VPN with multi-factor authentication - Zero Trust Network Access (ZTNA) - Secure remote desktop solutions

48.3.5 3.5 Device Compliance

Mobile devices must meet compliance requirements: - Current operating system version - Installed security updates - Enabled screen lock - No jailbreak/root - Installed endpoint security software

48.3.6 3.6 Lost/Stolen Device Response

In case of loss or theft of mobile devices, an incident is immediately reported. Remote wipe is performed to prevent data loss.

48.3.7 3.7 Public Wi-Fi and Network Security

Use of public Wi-Fi networks is only permitted via VPN. Unencrypted connections to corporate resources are prohibited.

48.3.8 3.8 Remote Work Security

Remote workspaces must meet security requirements: - Secure network connection - Physical security (screen lock, clear desk) - No sharing of credentials - Compliance with Acceptable Use Policy

48.4 4. Roles and Responsibilities

48.4.1 RACI Matrix: Mobile Device and Remote Work

Activity	CISO	IT Operations	MDM Administrator	Employee	HR
Policy Creation	R/A	C	C	I	C
MDM Operations	A	R	R	I	I
Device Enrollment	I	C	R	R/A	I

Activity	CISO	IT Operations	MDM Administrator	Employee	HR
Compliance Monitoring	A	C	R	I	I
Lost Device Response	A	R	R	R	C
Remote Access Provisioning	C	R/A	C	I	I
Security Training	A	I	I	R	R

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

48.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **MDM Administrator:** {{ meta.it.mdm_admin }}
- **Remote Access Manager:** {{ meta.it.remote_access_manager }}
- **Implementation Responsible:** IT Operations, Employees
- **Control/Audit Function:** ISMS, Internal Audit

48.5 5. Derivatives (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

48.5.1 Associated Guidelines

- **0510_Guideline_MDM_BringYourOwnDevice_and_Remote_Access.md** - Detailed implementation guideline
- `0200_Policy_Acceptable_Use_of_IT.md` - Acceptable Use Policy
- `0240_Policy_Authentication_and_Passwords.md` - Authentication Policy
- `0620_Policy_Endpoint_Security.md` - Endpoint Security Policy

48.5.2 Associated Standards/Baselines

- MDM configuration standards
- Device compliance requirements
- BYOD guideline
- Remote access standards

48.5.3 Associated Processes

- Device enrollment process
- Lost/stolen device response process
- Remote access provisioning process
- BYOD approval process

48.6 6. Compliance, Monitoring and Enforcement

48.6.1 Metrics and KPIs

- MDM enrollment rate (Target: 100% of mobile devices)

- Device compliance rate (Target: 95%)
- Number of non-compliant devices
- Average time to remote wipe for lost devices
- VPN usage rate for remote work
- Number of lost/stolen device incidents

48.6.2 Evidence and Proof

- MDM enrollment status
- Device compliance reports
- Remote access logs
- Lost device incident reports
- BYOD approval documentation
- Security training evidence

48.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Non-enrolled Devices:** Access block, enrollment requirement - **Non-Compliance:** Access restriction until remediation - **Unreported Device Loss:** Investigation, disciplinary action - **Repeated Violations:** Employment consequences

48.7 7. Exceptions

Exceptions to this policy are only permitted in justified exceptional cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO
- **Documentation:** All exceptions are documented in the risk register
- **Time Limitation:** Exceptions are generally time-limited
- **Compensating Controls:** Exceptions require alternative security measures

48.8 8. References

48.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0510_Guideline_MDM_BringYourOwnDevice_and_Remote_Access.md` - Detailed Guideline
- `0620_Policy_Endpoint_Security.md` - Endpoint Security Policy
- `0080_ISMS_Risk_Register_Template.md` - Risk Register

48.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.6.7** - Remote working
- **ISO/IEC 27001:2022 Annex A.6.8** - Information security event reporting
- **ISO/IEC 27001:2022 Annex A.8.9** - Configuration management
- **NIST SP 800-46** - Guide to Enterprise Telework, Remote Access, and BYOD Security
- **GDPR (EU 2016/679)** - Data protection for BYOD and remote work

---

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 49

Guideline: MDM, Bring Your Own Device and Remote Access

Document ID: 0510
Document Type: Guideline (detailed)
Associated Policy: 0500_Policy_Mobile_Device_and_Remote_Work.md
Standard Reference: ISO/IEC 27001:2022 Annex A.6.7, A.8.9
Owner: {{ meta.it_operations.manager }}
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}

49.1 1. Purpose and Scope

This guideline specifies the `0500_Policy_Mobile_Device_and_Remote_Work.md` and defines: - Mobile Device Management (MDM) requirements - BYOD guidelines and processes - Remote access controls

Scope: All mobile devices and remote access at **AdminSend GmbH**

49.2 2. Mobile Device Management (MDM)

49.2.1 2.1 MDM System

Platform: {{ meta.mdm.system }} (e.g., Microsoft Intune, Jamf, MobileIron)

Managed Devices: - Corporate-owned smartphones and tablets - BYOD devices with corporate access - Laptops (optional, depending on MDM capability)

49.2.2 2.2 MDM Enrollment

Process: 1. Receive device or BYOD request approved 2. Install MDM app 3. Perform enrollment 4. Pass compliance checks 5. Corporate access activated

Mandatory Enrollment: - All corporate-owned devices - All BYOD devices with email access or corporate apps

49.2.3 2.3 MDM Policies

Enforced Settings: - Device encryption enabled - PIN/passcode (min. 6 characters) or biometrics - Automatic screen lock (5 minutes) - OS updates within 30 days - Jailbreak/root detection

Prohibited Activities: - Jailbreak or rooting - Installation from unknown sources - Disabling security features

49.2.4 2.4 Compliance Checks

Automatic Checks: - OS version current? - Encryption active? - Jailbreak/root detected? - Malware detected?

For Non-Compliance: - Warning to user (24-hour deadline) - Restricted access - Complete block after 7 days

49.3 3. BYOD (Bring Your Own Device)

49.3.1 3.1 BYOD Authorization

Prerequisites: - Request via self-service portal - Approval by supervisor - Sign BYOD agreement - MDM enrollment

Eligible Devices: - Smartphones (iOS, Android) - Tablets (iOS, Android) - Laptops (case-by-case review)

49.3.2 3.2 BYOD Agreement

Contents: - Terms of use - Security requirements - MDM enrollment requirement - Remote wipe consent - Data protection (separation private/business) - Liability for loss

49.3.3 3.3 Containerization

Technology: - Separate containers for business data - Encrypted containers - No mixing private/business

Examples: - iOS: Managed Apps - Android: Work Profile - Windows: Windows Information Protection (WIP)

49.3.4 3.4 BYOD Offboarding

At Contract End or BYOD Termination: 1. Remote wipe of business container 2. Removal of corporate apps 3. Revocation of certificates 4. MDM unenrollment 5. Private data remains intact

49.4 4. Remote Access

49.4.1 4.1 VPN Access

VPN System: {{ meta.network.vpn_solution }}

Requirements: - Multi-factor authentication (MFA) - Endpoint compliance check before connection - Split tunneling prohibited (full tunnel) - Session timeout: 8 hours

VPN Clients: - Corporate-approved clients - Automatic updates - Kill switch enabled

49.4.2 4.2 Zero Trust Network Access (ZTNA)

Principles: - Never Trust, Always Verify - Least Privilege Access - Micro-segmentation

Implementation: - Identity-based access control - Device posture checks - Continuous authentication

49.4.3 4.3 Remote Desktop

Technologies: - RDP over VPN (Windows) - SSH over VPN (Linux) - Citrix/VMware Horizon (Virtual Desktops)

Security Controls: - MFA for remote desktop - Session recording (privileged access) - Idle timeout: 30 minutes

49.5 5. Remote Work Security

49.5.1 5.1 Home Office Requirements

Network: - Secure Wi-Fi (WPA3 or WPA2) - No public Wi-Fi without VPN - Router firmware current

Workspace: - Private workspace (no third-party visibility) - Screen lock when absent - No use by family members

49.5.2 5.2 Public Places

Allowed with Restrictions: - Work in cafes, airports, hotels - VPN mandatory - Privacy screen for laptop - No confidential conversations

Prohibited: - Public computers (internet cafes) - Unsecured Wi-Fi without VPN - Unattended device

49.5.3 5.3 Travel

International Travel: - Report to IT Security (high-risk countries) - Travel laptop without confidential data - Encryption mandatory - No use of local USB drives

49.6 6. Mobile Application Management (MAM)

49.6.1 6.1 Approved Apps

Corporate Apps: - Email ({{ meta.email.mobile_app }}) - Collaboration ({{ meta.collaboration.mobile_app }}) - VPN client - Authenticator app

Approval Process: - Request via IT portal - Security review - Approval by IT Security

49.6.2 6.2 App Wrapping

For Corporate-Owned Apps: - MDM policies integrated into app - Enforce encryption - Copy/paste control

49.7 7. Incident Response

49.7.1 7.1 Device Loss

Immediate Actions: 1. Report to IT Support ({{ meta.support.phone }}) 2. Trigger remote wipe (within 1 hour) 3. Change passwords 4. Create incident ticket 5. Police report (in case of theft)

49.7.2 7.2 Compromise

For Suspected Malware: 1. Disconnect device from network 2. Inform IT Security 3. Forensic analysis (if required) 4. Rebuild device 5. Lessons learned

49.8 8. Compliance and Audit

49.8.1 8.1 Metrics (KPIs)

Metric	Target Value
MDM enrollment rate	100%
Compliance rate	$> 95\%$
OS update rate (30 days)	$> 90\%$
Remote wipe success rate	100%

49.8.2 8.2 Audit Evidence

- MDM enrollment logs
- Compliance reports
- BYOD agreements
- Remote access logs

49.9 9. References

49.9.1 Internal Documents

- `0500_Policy_Mobile_Device_and_Remote_Work.md`
- `0250_Guideline_MFA_Password_Rules_and_Session_Management.md`

49.9.2 External Standards

- **ISO/IEC 27001:2022 Annex A.6.7** - Remote working
- **ISO/IEC 27001:2022 Annex A.8.9** - Configuration management
- **NIST SP 800-124** - Guidelines for Managing the Security of Mobile Devices

---

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 50

Policy: HR Security

Document ID: 0520
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.6.1-A.6.4 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

50.1 1. Purpose

This policy defines the principles for HR Security at **AdminSend GmbH**. It ensures that security responsibilities are understood and fulfilled throughout the employment lifecycle - from hiring through termination.

50.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Persons:** All employees, contractors, temporary workers, interns
- **Lifecycle:** Pre-employment, onboarding, employment, offboarding
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

50.3 3. Principles (Policy Statements)

50.3.1 3.1 Pre-Employment Screening

Appropriate background checks are conducted before hiring (references, qualifications, criminal record if applicable). Screening is based on role and protection requirements.

50.3.2 3.2 Contractual Security Obligations

Employment contracts contain security clauses: - Confidentiality agreements (NDA) - Acceptable Use Policy acknowledgement - Data protection obligations - Intellectual property rights

50.3.3 3.3 Security Awareness and Training

All employees undergo security awareness training: - **Onboarding:** Initial security training - **Annually:** Refresher training - **Role-specific:** Additional training for privileged roles

50.3.4 3.4 Joiner-Mover-Leaver Process

Security-relevant activities are performed throughout the employment lifecycle: - **Joiner:** Access provisioning, training, equipment issuance - **Mover:** Access adjustment for role changes - **Leaver:** Access revocation, equipment return, exit interview

50.3.5 3.5 Disciplinary Process

Security violations are handled according to defined disciplinary procedures. Violations are documented and may lead to employment consequences.

50.3.6 3.6 Responsibilities and Duties

Employees are obligated to: - Comply with security policies - Report security incidents - Participate in security training - Maintain confidentiality

50.3.7 3.7 Privileged Roles

Employees with privileged access are subject to enhanced requirements: - Extended background checks - Additional security training - Regular recertification - Strict monitoring

50.3.8 3.8 Offboarding and Access Revocation

Upon termination of employment, all access is immediately revoked: - IT access deactivated (Target: < 1 day) - Equipment returned - Confidentiality obligations renewed - Exit interview conducted

50.4 4. Roles and Responsibilities

50.4.1 RACI Matrix: HR Security

Activity	CISO	HR	Hiring Manager	IT Operations	Legal
Policy Creation	R/A	C	C	I	C
Background Checks	C	R/A	C	I	C

Activity	CISO	HR	Hiring Manager	IT Operations	Legal
Contract Clauses	C	R	I	I	R/A
Security Training	R/A	C	I	C	I
Joiner Process	C	R	R/A	R	I
Mover Process	C	R	R/A	R	I
Leaver Process	C	R/A	C	R	I
Disciplinary Process	C	R/A	C	I	C

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

50.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **HR Manager:** {{ meta.hr.manager }}
- **Security Awareness Manager:** {{ meta.security.awareness_manager }}
- **Implementation Responsible:** HR, Hiring Manager, IT Operations
- **Control/Audit Function:** ISMS, Internal Audit

50.5 5. Derivatives (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

50.5.1 Associated Guidelines

- **0530_Guideline_HR_Onboarding_Role_Change_Offboarding.md** - Detailed implementation guideline
- `0220_Policy_Access_Control_and_Identity_Management.md` - Access Control Policy
- `0200_Policy_Acceptable_Use_of_IT.md` - Acceptable Use Policy
- `0120_ISMS_Training_Awareness_and_Competence.md` - Training and Awareness

50.5.2 Associated Standards/Baselines

- Background check requirements
- Contractual security clauses (templates)
- Security training curriculum
- Joiner-Mover-Leaver checklists

50.5.3 Associated Processes

- Pre-employment screening process
- Joiner-Mover-Leaver process
- Security training process
- Disciplinary process

50.6 6. Compliance, Monitoring and Enforcement

50.6.1 Metrics and KPIs

- Background check completion rate (Target: 100%)
- Security training completion rate (Target: 100% annually)
- Average time to access provisioning (Joiner)
- Average time to access revocation (Leaver) (Target: < 1 day)
- Number of security violations and disciplinary procedures
- NDA signing rate (Target: 100%)

50.6.2 Evidence and Proof

- Background check documentation
- Contracts with security clauses
- Security training evidence
- Joiner-Mover-Leaver checklists
- Disciplinary procedure documentation
- Exit interview protocols

50.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Missing Background Checks:** Completion before access provisioning - **Incomplete Training:** Access restriction until completion - **Security Violations:** Disciplinary procedure per HR process - **Repeated Violations:** Employment consequences up to termination

50.7 7. Exceptions

Exceptions to this policy are only permitted in justified exceptional cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and HR Manager
- **Documentation:** All exceptions are documented in the risk register
- **Time Limitation:** Exceptions are generally time-limited

50.8 8. References

50.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0530_Guideline_HR_Onboarding_Role_Change_Offboarding.md` - Detailed Guideline
- `0220_Policy_Access_Control_and_Identity_Management.md` - Access Control Policy
- `0080_ISMS_Risk_Register_Template.md` - Risk Register

50.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.6.1** - Screening
- **ISO/IEC 27001:2022 Annex A.6.2** - Terms and conditions of employment

- **ISO/IEC 27001:2022 Annex A.6.3** - Information security awareness, education and training
- **ISO/IEC 27001:2022 Annex A.6.4** - Disciplinary process
- Employment law requirements (Germany)
- **GDPR (EU 2016/679)** - Data protection for background checks

---

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 51

Guideline: HR Security - Onboarding, Role Change, Offboarding

Document ID: 0530
Document Type: Guideline (detailed)
Associated Policy: 0520_Policy_HR_Security.md
Standard Reference: ISO/IEC 27001:2022 Annex A.6.1, A.6.2, A.6.3, A.6.4
Owner: {{ meta.hr.manager }}
Version: 1.0
Status: Approved
Classification: Confidential
Last Updated: {{ meta.document.date }}

51.1 1. Purpose and Scope

This guideline specifies the `0520_Policy_HR_Security.md` and defines: - Security aspects in the HR lifecycle - Onboarding, role change, and offboarding processes - Background checks and confidentiality obligations

Scope: All employees, contractors, and third parties at **AdminSend GmbH**

51.2 2. Pre-Employment

51.2.1 2.1 Background Checks

Standard Employees: - Identity verification (ID card) - Check references (2 references) - Verify educational qualifications - Check work authorization

Privileged Roles: - Extended background checks - Criminal record certificate - Credit check (for financial access) - Social media screening (optional)

External Contractors: - Company background check - NDA before access - Sponsor responsibility

51.2.2 2.2 Employment Contract

Security Clauses: - Confidentiality obligation - Acceptable Use Policy - Intellectual property rights - Post-employment obligations

51.3 3. Onboarding

51.3.1 3.1 First Day of Work

HR Activities: 1. Hand over welcome package 2. Sign employment contract 3. Acknowledge security policies 4. Record emergency contacts

IT Activities: 1. Account creation (see `0230_Guideline_IAM`) 2. Hardware issuance 3. IT orientation 4. MFA registration

51.3.2 3.2 Security Training

Mandatory Training (First Week): - Information Security Awareness (2 hours) - Data Protection / GDPR (1 hour) - Acceptable Use Policy (30 minutes) - Phishing Awareness (30 minutes)

Confirmation: - Quiz (passing threshold: 80%) - Signature on training certificate

51.3.3 3.3 Role-Specific Training

Developers: - Secure Coding Training - OWASP Top 10

Administrators: - Privileged Access Management - Incident Response

HR/Finance: - Data Privacy - Social Engineering Awareness

51.4 4. Role Change (Mover)

51.4.1 4.1 Internal Transfer

HR Process: 1. Update new role in HR system 2. Inform old and new supervisor 3. IT ticket for access changes

IT Process: 1. Revoke old access 2. Provision new access 3. Adjust hardware (if required) 4. Update documentation

Details: See `0230_Guideline_IAM`

51.4.2 4.2 Promotions

Additional Checks: - For privileged roles: Extended background check - Security training for new responsibilities - Four-eyes principle for critical access

51.5 5. Offboarding

51.5.1 5.1 Planned Departure

2 Weeks Before Departure: - Plan knowledge transfer - Create handover checklist - Review access

Last Day of Work: - Hardware return - Return access card - Exit interview - Account deactivation (end of day)

After Departure: - Account deletion (after 30 days) - Email forwarding (30 days) - Data archiving

Details: See `0230_Guideline_IAM`

51.5.2 5.2 Unplanned Departure

Immediate Actions (within 1 hour): 1. Deactivate all accounts 2. Block VPN access 3. Deactivate access card 4. Remote wipe mobile devices 5. Inform supervisor and Security

Reasons: - Termination for cause - Security incidents - Suspected data misuse

51.5.3 5.3 Post-Employment

Confidentiality Obligation: - Remains in effect after departure - No disclosure of trade secrets - Return of all documents

Rehiring: - New background check - New security training - New accounts (no reactivation of old accounts)

51.6 6. Confidentiality Obligations

51.6.1 6.1 Non-Disclosure Agreement (NDA)

Signing: - At hiring (in employment contract) - For access to confidential projects - For data processing (external service providers)

Contents: - Definition of confidential information - Usage restrictions - Duration of obligation - Consequences of violations

51.6.2 6.2 Intellectual Property (IP)

Regulation: - All work results belong to the company - No private use of company code - Disclosure of inventions

51.7 7. Disciplinary Measures

51.7.1 7.1 Security Violations

Categories: - **Minor:** Unintentional violations (e.g., password sharing) - **Medium:** Negligent violations (e.g., data loss through carelessness) - **Severe:** Intentional violations (e.g., data theft)

Measures: - Minor: Warning, retraining - Medium: Written reprimand - Severe: Termination, criminal charges

51.7.2 7.2 Process

1. Incident report
2. Investigation by HR and Security
3. Hearing of employee

4. Decision on measures
5. Documentation
6. Implementation

51.8 8. External Contractors

51.8.1 8.1 Onboarding

Prerequisites: - Contract with security clauses - NDA signed - Background check (by contractor company) - Internal sponsor

Access: - Time-limited - Project-based only - Regular recertification (quarterly)

51.8.2 8.2 Monitoring

Enhanced Monitoring: - Access to confidential data - Privileged activities - Data exports

51.8.3 8.3 Offboarding

At Project End: - Immediate access revocation - Data return or deletion - Confirmation of confidentiality obligation

51.9 9. Compliance and Audit

51.9.1 9.1 Metrics (KPIs)

Metric	Target Value
Background check completion	100%
Security training (onboarding)	100%
Offboarding completion (on last day)	100%
NDA signing	100%

51.9.2 9.2 Audit Evidence

- Background check documentation
- Training certificates
- NDA signatures
- Offboarding checklists

51.10 10. References

51.10.1 Internal Documents

- `0520_Policy_HR_Security.md`
- `0230_Guideline_IAM_Joiner_Mover_Leaver_and_Access_Requests.md`

51.10.2 External Standards

- **ISO/IEC 27001:2022 Annex A.6.1** - Screening
- **ISO/IEC 27001:2022 Annex A.6.2** - Terms and conditions of employment
- **ISO/IEC 27001:2022 Annex A.6.3** - Information security awareness, education and training
- **ISO/IEC 27001:2022 Annex A.6.4** - Disciplinary process

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 52

Policy: Configuration and Hardening

Document ID: 0540
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.8.9, A.8.10 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

52.1 1. Purpose

This policy defines the principles for secure configuration and system hardening at **AdminSend GmbH**. It ensures that IT systems are securely configured and hardened against attacks.

52.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Systems:** All servers, workstations, network devices, applications, cloud resources
- **Environments:** Production, test, development
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

52.3 3. Principles (Policy Statements)

52.3.1 3.1 Security Baselines

Security baselines exist for all system types, defining minimum requirements for secure configuration. Baselines are based on recognized standards (CIS Benchmarks, BSI, vendor best practices).

52.3.2 3.2 Secure by Default

Systems are deployed with secure default configurations. Insecure default settings are changed, unnecessary features disabled.

52.3.3 3.3 Hardening Measures

Systems are hardened: - Removal of unnecessary software and services - Disabling of unneeded ports and protocols - Changing default credentials - Minimizing attack surface

52.3.4 3.4 Configuration Management

Configurations are centrally managed and versioned (Infrastructure as Code, configuration management tools). Changes are controlled through change management.

52.3.5 3.5 Configuration Drift Detection

Deviations from security baselines (configuration drift) are automatically detected and reported. Unauthorized changes are rolled back.

52.3.6 3.6 Least Functionality

Systems are configured according to the principle of least functionality. Only required functions and services are enabled.

52.3.7 3.7 Secure Configuration Reviews

Configurations are regularly reviewed: - **Critical Systems:** Quarterly - **Important Systems:** Semi-annually - **Standard Systems:** Annually

52.3.8 3.8 Documentation

All configuration deviations from baselines are documented and justified. Documentation is current and traceable.

52.4 4. Roles and Responsibilities

52.4.1 RACI Matrix: Configuration and Hardening

Activity	CISO	IT Operations	System Owner	Security Team	Change Management
Policy Creation	R/A	C	C	C	I
Baseline Creation	A	C	C	R	I
System Hardening	C	R/A	C	C	I

Activity	CISO	IT Operations	System Owner	Security Team	Change Management
Configuration Management	C	R/A	C	I	C
Drift Detection	A	C	I	R	I
Configuration Reviews	A	C	R	R	I
Compliance Review	R/A	C	C	C	I

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

52.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **Configuration Manager:** {{ meta.it.config_manager }}
- **Security Architect:** {{ meta.security.architect }}
- **Implementation Responsible:** IT Operations, System Owner
- **Control/Audit Function:** ISMS, Internal Audit

52.5 5. Derivatives (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

52.5.1 Associated Guidelines

- **0550_Guideline_Security_Baselines_Hardening_and_Config_Changes.md** - Detailed implementation guideline
- `0360_Policy_Change_and_Release_Management.md` - Change Management Policy
- `0340_Policy_Vulnerability_and_Patch_Management.md` - Vulnerability Management Policy

52.5.2 Associated Standards/Baselines

- Security baselines (Windows, Linux, network devices, cloud)
- Hardening guides
- Configuration management standards
- Drift detection rules

52.5.3 Associated Processes

- Configuration management process
- Hardening process
- Configuration review process
- Drift remediation process

52.6 6. Compliance, Monitoring and Enforcement

52.6.1 Metrics and KPIs

- Baseline compliance rate (Target: 95%)
- Number of configuration drift findings
- Average time to drift remediation
- Configuration review completion rate (Target: 100%)
- Number of systems with default credentials (Target: 0)
- Hardening coverage (Target: 100% of critical systems)

52.6.2 Evidence and Proof

- Security baselines documentation
- Configuration management logs
- Drift detection reports
- Configuration review reports
- Hardening checklists
- Audit reports on configuration compliance

52.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Non-hardened Systems:** Immediate remediation, production block - **Configuration Drift:** Remediation by priority - **Default Credentials:** Immediate change, incident response - **Repeated Violations:** Employment consequences

52.7 7. Exceptions

Exceptions to this policy are only permitted in justified exceptional cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and System Owner
- **Documentation:** All exceptions are documented in the risk register
- **Time Limitation:** Exceptions are generally time-limited
- **Compensating Controls:** Exceptions require alternative security measures

52.8 8. References

52.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0550_Guideline_Security_Baselines_Hardening_and_Config_Changes.md` - Detailed Guideline
- `0360_Policy_Change_and_Release_Management.md` - Change Management Policy
- `0080_ISMS_Risk_Register_Template.md` - Risk Register

52.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.8.9** - Configuration management

- **ISO/IEC 27001:2022 Annex A.8.10** - Information deletion
- **CIS Benchmarks** - Center for Internet Security Configuration Benchmarks
- **NIST SP 800-123** - Guide to General Server Security
- **BSI IT-Grundschutz** - Security requirements

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 53

Guideline: Security Baselines, Hardening and Configuration Changes

Document ID: 0550
Document Type: Guideline (detailed)
Associated Policy: 0540_Policy_Configuration_and_Hardening.md
Standard Reference: ISO/IEC 27001:2022 Annex A.8.9
Owner: {{ meta.it_operations.manager }}
Version: 1.0
Status: Approved
Classification: Confidential
Last Updated: {{ meta.document.date }}

53.1 1. Purpose and Scope

This guideline specifies the `0540_Policy_Configuration_and_Hardening.md` and defines: - Security baselines for different system types - Hardening processes and standards - Configuration management and change control

Scope: All IT systems at **AdminSend GmbH**

53.2 2. Security Baselines

53.2.1 2.1 Windows Server

Baseline Standard: CIS Benchmark Level 1

Core Requirements: - Disable local administrator accounts (except break-glass) - Windows Firewall enabled - Windows Defender enabled - Automatic updates enabled - SMBv1 disabled - PowerShell logging enabled - Audit policies configured

Tools: - Group Policy Objects (GPOs) - Microsoft Security Compliance Toolkit - CIS-CAT Pro

53.2.2 2.2 Linux Server

Baseline Standard: CIS Benchmark Level 1

Core Requirements: - Root login via SSH disabled - SSH key-based authentication - Firewall (iptables/firewalld) enabled - SELinux/AppArmor enabled - Automatic security updates - Unnecessary services disabled - Audit daemon (auditd) enabled

Tools: - Ansible/Puppet for configuration management - Lynis for security audits

53.2.3 2.3 Network Devices

Baseline Standard: Vendor best practices + CIS Benchmarks

Core Requirements: - Default passwords changed - SNMP v3 (or disabled) - Unused ports disabled - Management access only via dedicated VLAN - Logging to SIEM - NTP configured

53.2.4 2.4 Cloud Workloads

Baseline Standard: Cloud Security Posture Management (CSPM)

Azure: - Azure Security Benchmark - Microsoft Defender for Cloud recommendations

AWS: - AWS Foundational Security Best Practices - CIS AWS Foundations Benchmark

GCP: - CIS Google Cloud Platform Foundation Benchmark

53.3 3. Hardening Process

53.3.1 3.1 Build Phase

Golden Images: - Pre-configured, hardened images - Regular updates (monthly) - Automated builds (CI/CD)

Process: 1. Base image (vendor) 2. Apply hardening scripts 3. Security scan 4. Approval 5. Image repository

53.3.2 3.2 Deployment Phase

Automation: - Infrastructure as Code (Terraform, ARM Templates) - Configuration Management (Ansible, Puppet, Chef) - Compliance checks before deployment

Manual Steps: - Only for exceptions - Documentation required - Post-deployment verification

53.3.3 3.3 Maintenance Phase

Regular Reviews: - Quarterly configuration audits - Drift detection (deviations from baseline) - Remediation of non-compliance

53.4 4. Configuration Management

53.4.1 4.1 Configuration Management Database (CMDB)

System: {{ meta.itsm.cmdb }}

Documented Configurations: - System type and version - Installed software - Network configuration - Security configuration - Baseline version

53.4.2 4.2 Configuration Baselines

Baseline Versions: - Major version: For significant changes - Minor version: For smaller updates - Patch version: For security fixes

Example: Windows-Server-Baseline v2.1.3

53.4.3 4.3 Drift Detection

Monitoring: - Automatic scans (daily) - Comparison with baseline - Alerts for deviations

Tools: - Microsoft Defender for Cloud (Azure) - AWS Config (AWS) - Chef InSpec, Ansible Tower

Remediation: - Automatic correction (where possible) - Manual correction with ticket - Exception process (see Section 6)

53.5 5. Configuration Changes

53.5.1 5.1 Change Process

All Configuration Changes Through Change Management: - Create change request (RFC) - Security impact assessment - Testing in dev/test - CAB approval - Implementation - Verification

Details: See `0370_Guideline_Change_Management_with_Security_Approvals`

53.5.2 5.2 Emergency Changes

For Critical Security Fixes: - Expedited process - ECAB approval - Retrospective documentation

53.5.3 5.3 Configuration Backup

Before Each Change: - Backup of current configuration - Versioning - Rollback capability

Retention: {{ meta.retention.config_years }} years

53.6 6. Exceptions and Deviations

53.6.1 6.1 Exception Process

Request: - Justification (business justification) - Risk assessment - Compensating controls - Time limitation

Approval: - CISO approval required - Documentation in exception register - Regular review (quarterly)

Details: See `0640_Policy_Exceptions_and_Risk_Waivers.md`

53.6.2 6.2 Legacy Systems

For Systems That Cannot Meet Baseline: - Implement compensating controls - Network isolation - Enhanced monitoring - Create migration plan

53.7 7. Compliance Monitoring

53.7.1 7.1 Automated Compliance Scanning

Tools: - **Windows:** Microsoft Security Compliance Toolkit, CIS-CAT - **Linux:** Lynis, OpenSCAP - **Cloud:** Cloud Security Posture Management (CSPM) - **Network:** Nessus, Qualys

Frequency: - Critical systems: Weekly - Standard systems: Monthly

53.7.2 7.2 Compliance Reporting

Monthly Compliance Report: - Compliance rate per baseline - Top non-compliance items - Trend analysis - Remediation status

Target: > 95% compliance

53.7.3 7.3 Audit Evidence

- Baseline documents
- Compliance scan reports
- Exception register
- Remediation tickets

53.8 8. Hardening Standards

53.8.1 8.1 Reference Standards

Primary: - CIS Benchmarks (Center for Internet Security) - DISA STIGs (Defense Information Systems Agency Security Technical Implementation Guides) - Vendor best practices

Secondary: - NIST Cybersecurity Framework - BSI IT-Grundschutz

53.8.2 8.2 Baseline Documentation

For Each Baseline: - Scope and applicability - Configuration settings (detailed) - Justification for each setting - Test procedures - Rollback procedures

Location: {{ meta.documentation.baseline_repo }}

53.9 9. Compliance and Audit

53.9.1 9.1 Metrics (KPIs)

Metric	Target Value
Baseline compliance rate	> 95%
Drift remediation time	< 7 days
Golden image currency	< 30 days
Exceptions with current review	100%

53.9.2 9.2 Audit Evidence

- Baseline documents
- Compliance scan reports
- Configuration backups
- Change records

53.10 10. References

53.10.1 Internal Documents

- `0540_Policy_Configuration_and_Hardening.md`
- `0370_Guideline_Change_Management_with_Security_Approvals.md`
- `0640_Policy_Exceptions_and_Risk_Waivers.md`

53.10.2 External Standards

- **ISO/IEC 27001:2022 Annex A.8.9** - Configuration management
- **CIS Benchmarks** - https://www.cisecurity.org/cis-benchmarks/
- **NIST SP 800-70** - Security Configuration Checklists

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 54

Policy: Data Protection Interfaces

Document ID: 0560
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.5.31-A.5.34 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

54.1 1. Purpose

This policy defines the interfaces between information security and data protection at **AdminSend GmbH**. It ensures that ISMS and data protection requirements are aligned and coordinated.

54.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Data:** All personal data according to GDPR
- **Processes:** All processing activities of personal data
- **Interfaces:** ISMS Data Protection Management System
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

54.3 3. Principles (Policy Statements)

54.3.1 3.1 Coordination of ISMS and Data Protection

ISMS and data protection management are coordinated. CISO and DPO work closely together and align measures.

54.3.2 3.2 Privacy by Design and by Default

Data protection is integrated into systems and processes from the beginning (Privacy by Design). Privacy-friendly default settings are standard (Privacy by Default).

54.3.3 3.3 Data Protection Impact Assessment (DPIA)

Data Protection Impact Assessments are conducted for high-risk processing. DPIA is coordinated with ISMS risk analysis.

54.3.4 3.4 Data Subject Rights

Processes for fulfilling data subject rights are established: - Right of access (Art. 15 GDPR) - Right to rectification (Art. 16 GDPR) - Right to erasure (Art. 17 GDPR) - Right to data portability (Art. 20 GDPR) - Right to object (Art. 21 GDPR)

54.3.5 3.5 Record of Processing Activities

A record of processing activities (RoPA) is maintained and kept current. RoPA is aligned with ISMS asset inventory.

54.3.6 3.6 Data Processing

Data processors are engaged according to GDPR Art. 28. Data Processing Agreements (DPA) contain required security measures.

54.3.7 3.7 Data Breaches

Data breaches are handled according to GDPR Art. 33/34. Notification obligations to supervisory authorities and data subjects are met (72-hour deadline).

54.3.8 3.8 International Data Transfers

International data transfers only occur with appropriate safeguards (adequacy decision, standard contractual clauses, BCR).

54.4 4. Roles and Responsibilities

54.4.1 RACI Matrix: Data Protection Interfaces

Activity	CISO	DPO	IT Operations	Business Owner	Legal
Policy Creation	R/A	R/A	C	C	C
DPIA Execution	C	R/A	C	R	C

Activity	CISO	DPO	IT Operations	Business Owner	Legal
Data Subject Rights	I	R/A	C	C	C
RoPA Maintenance	C	R/A	C	R	I
DPA Negotiation	C	R/A	I	C	R
Data Breach Notification	R/A	R/A	C	C	C
Privacy by Design	R	R/A	R	R	I

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

54.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO) and {{ meta.dpo.name }} (DPO)
- **Data Protection Officer:** {{ meta.dpo.name }}
- **Privacy Officer:** {{ meta.privacy.officer }}
- **Implementation Responsible:** IT Operations, Business Owner
- **Control/Audit Function:** ISMS, Internal Audit, Data Protection Authority

54.5 5. Derivatives (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

54.5.1 Associated Guidelines

- **0570_Guideline_Data_Protection_Requirements_and_Data_Processing.md** - Detailed implementation guideline
- `0280_Policy_Data_Classification_and_Information_Handling.md` - Data Classification Policy
- `0400_Policy_Incident_Management.md` - Incident Management Policy (data breaches)
- `0460_Policy_Supplier_and_Cloud_Security.md` - Supplier Security Policy (DPA)

54.5.2 Associated Standards/Baselines

- DPIA methodology
- Data subject rights processes
- DPA templates
- Data breach notification process

54.5.3 Associated Processes

- Data Protection Impact Assessment (DPIA)
- Data subject rights process
- Data breach notification process
- Privacy by Design review

54.6 6. Compliance, Monitoring and Enforcement

54.6.1 Metrics and KPIs

- Number of DPIAs conducted
- Average processing time for data subject rights (Target: < 30 days)
- Number of data breaches and notifications
- RoPA currency (Target: quarterly update)
- Number of DPAs with current security measures (Target: 100%)
- Privacy by Design review coverage

54.6.2 Evidence and Proof

- DPIA documentation
- Record of processing activities (RoPA)
- Data subject rights requests and responses
- Data Processing Agreements (DPA)
- Data breach notifications
- Privacy by Design reviews

54.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **GDPR Violations:** Incident response, notification to supervisory authority, potential fines - **Unreported Data Breaches:** Compliance investigation, disciplinary action - **Missing DPIAs:** Completion, processing suspension - **Repeated Violations:** Employment consequences, fines

54.7 7. Exceptions

Exceptions to this policy are only permitted in justified exceptional cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and DPO
- **Documentation:** All exceptions are documented in the risk register
- **Time Limitation:** Exceptions are generally time-limited

54.8 8. References

54.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0570_Guideline_Data_Protection_Requirements_and_Data_Processing.md` - Detailed Guideline
- `0280_Policy_Data_Classification_and_Information_Handling.md` - Data Classification Policy
- `0080_ISMS_Risk_Register_Template.md` - Risk Register

54.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.5.31** - Legal, statutory, regulatory and contractual requirements
- **ISO/IEC 27001:2022 Annex A.5.32** - Intellectual property rights
- **ISO/IEC 27001:2022 Annex A.5.33** - Protection of records
- **ISO/IEC 27001:2022 Annex A.5.34** - Privacy and protection of PII
- **GDPR (EU 2016/679)** - General Data Protection Regulation
- **ISO/IEC 27701** - Privacy Information Management System
- **BDSG** - German Federal Data Protection Act

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 55

Guideline: Data Protection Requirements and Data Processing

Document ID: 0570
Document Type: Guideline (detailed)
Associated Policy: 0560_Policy_Data_Protection_Interfaces.md
Standard Reference: ISO/IEC 27001:2022 Annex A.5.34
Owner: {{ meta.dpo.name }}
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}

55.1 1. Purpose and Scope

This guideline specifies the `0560_Policy_Data_Protection_Interfaces.md` and defines: - GDPR compliance requirements - Data processing processes - Data subject rights and their implementation

Scope: All personal data at **AdminSend GmbH**

55.2 2. GDPR Principles

55.2.1 2.1 Lawfulness, Fairness and Transparency

Legal Bases (Art. 6 GDPR): - Consent (Art. 6(1)(a)) - Contract performance (Art. 6(1)(b)) - Legal obligation (Art. 6(1)(c)) - Legitimate interest (Art. 6(1)(f))

Documentation: - Document legal basis for each processing - Record of processing activities (RoPA)

55.2.2 2.2 Purpose Limitation

Principle: - Collect data only for specified, explicit purposes - No further processing for other purposes (without new legal basis)

55.2.3 2.3 Data Minimization

Principle: - Collect only necessary data - Regular review of necessity

55.2.4 2.4 Accuracy

Measures: - Keep data current - Correct inaccurate data - Processes for data updates

55.2.5 2.5 Storage Limitation

Deletion Concept: - Define retention periods - Automatic deletion after expiration - Documentation of deletion

Details: See `0590_Guideline_Records_Retention_and_Secure_Deletion.md`

55.2.6 2.6 Integrity and Confidentiality

Technical Measures: - Encryption - Access control - Logging and monitoring

55.2.7 2.7 Accountability

Proof Obligation: - Documentation of all measures - Data Protection Impact Assessment (DPIA) - Record of processing activities (RoPA)

55.3 3. Record of Processing Activities (RoPA)

55.3.1 3.1 Mandatory Information (Art. 30 GDPR)

For Each Processing: - Name and contact details of controller - Purposes of processing - Categories of data subjects - Categories of personal data - Categories of recipients - Third country transfers - Deletion periods - Technical and organizational measures (TOMs)

55.3.2 3.2 RoPA Maintenance

Responsibility: - Data Protection Officer coordinates - Departments provide information - Annual update (minimum)

Tool: {{ meta.dpo.vvt_tool }}

55.4 4. Data Protection Impact Assessment (DPIA)

55.4.1 4.1 When Required?

Mandatory for (Art. 35 GDPR): - Systematic extensive evaluation of personal aspects (profiling) - Extensive processing of special categories (Art. 9) - Systematic extensive monitoring of public areas

Examples: - New CRM systems with profiling - Video surveillance - Biometric authentication

55.4.2 4.2 DPIA Process

Steps: 1. Description of processing 2. Assessment of necessity and proportionality 3. Risk assessment for data subjects 4. Remedial measures 5. Consultation with Data Protection Officer 6. Documentation

For High Risk: - Consultation with supervisory authority before processing

55.5 5. Data Subject Rights

55.5.1 5.1 Right of Access (Art. 15 GDPR)

Process: 1. Request via email to {{ meta.dpo.email }} 2. Identity verification 3. Compilation of information 4. Response within 1 month

Information to Provide: - Processing purposes - Categories of personal data - Recipients - Storage duration - Data subject rights - Copy of data

55.5.2 5.2 Right to Rectification (Art. 16 GDPR)

Process: 1. Request for rectification 2. Verification of accuracy 3. Correction within 1 month 4. Notification to recipients (if required)

55.5.3 5.3 Right to Erasure (Art. 17 GDPR)

Deletion Grounds: - Purpose fulfilled - Consent withdrawn - Objection to processing - Unlawful processing

Exceptions: - Legal retention obligations - Assertion of legal claims

55.5.4 5.4 Right to Restriction (Art. 18 GDPR)

Restriction Instead of Deletion: - When accuracy is contested - For unlawful processing (data subject does not want deletion) - For objection (during review)

55.5.5 5.5 Right to Data Portability (Art. 20 GDPR)

Prerequisites: - Processing based on consent or contract - Automated processing

Format: - Structured, commonly used, machine-readable (e.g., CSV, JSON)

55.5.6 5.6 Right to Object (Art. 21 GDPR)

For Legitimate Interest: - Data subject can object - Balancing required - Stop processing (unless compelling grounds)

For Direct Marketing: - Objection possible at any time - Stop processing immediately

55.6 6. Data Processing

55.6.1 6.1 Data Processing Agreement (DPA)

Mandatory for: - Service provider processes personal data on behalf - Cloud providers, IT service providers, etc.

Mandatory Contents (Art. 28 GDPR): - Subject matter and duration - Nature and purpose of processing - Categories of personal data - Obligations and rights of controller - Technical and organizational measures (TOMs) - Sub-processors - Support obligations

55.6.2 6.2 Technical and Organizational Measures (TOMs)

Categories: - Physical access control - System access control - Data access control - Disclosure control - Input control - Job control - Availability control - Separation control

Documentation: - TOMs for each processing - Regular review and adjustment

55.7 7. Data Breaches

55.7.1 7.1 Notification Obligation (Art. 33 GDPR)

To Supervisory Authority: - Within 72 hours of becoming aware - If risk to data subjects

Exceptions: - No risk to data subjects (e.g., encrypted data)

55.7.2 7.2 Notification to Data Subjects (Art. 34 GDPR)

Mandatory for: - High risk to data subjects - Without undue delay

Content: - Nature of breach - Contact point (Data Protection Officer) - Likely consequences - Measures taken

55.7.3 7.3 Documentation

Register of Data Breaches: - Document all breaches (including non-notifiable) - Facts, impacts, remedial measures - Proof for supervisory authority

55.8 8. International Data Transfers

55.8.1 8.1 Third Country Transfer

Permitted with: - EU Commission adequacy decision - Standard Contractual Clauses (SCCs) - Binding Corporate Rules (BCRs) - Consent

55.8.2 8.2 Schrems II Compliance

Transfer Impact Assessment (TIA): - Review legal situation in third country - Implement additional measures (e.g., encryption) - Documentation

55.9 9. Compliance and Audit

55.9.1 9.1 Metrics (KPIs)

Metric	Target Value
Data subject requests (response time)	$<$ 1 month
RoPA currency	$<$ 12 months
DPIA completion (new systems)	100%
Data breaches (notification)	$<$ 72 hours

55.9.2 9.2 Audit Evidence

- Record of processing activities (RoPA)
- Data Protection Impact Assessments (DPIA)
- Data Processing Agreements (DPA)
- Data subject requests and responses
- Register of data breaches

55.10 10. References

55.10.1 Internal Documents

- `0560_Policy_Data_Protection_Interfaces.md`
- `0590_Guideline_Records_Retention_and_Secure_Deletion.md`

55.10.2 External Standards

- **ISO/IEC 27001:2022 Annex A.5.34** - Privacy and protection of PII
- **GDPR (EU 2016/679)** - General Data Protection Regulation
- **BDSG** - German Federal Data Protection Act

Approved by: {{ meta.dpo.name }}, Data Protection Officer
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 56

Policy: Retention and Deletion

Document ID: 0580
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.5.33, A.5.34, A.8.10 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

56.1 1. Purpose

This policy defines the requirements for retention and deletion of information and data at **AdminSend GmbH**. It ensures compliance with legal retention obligations and adherence to data protection principles (data minimization, storage limitation).

56.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Data:** All information and data (structured and unstructured)
- **Systems:** All IT systems, databases, backup systems, archives
- **Media:** Digital and physical media
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

56.3 3. Principles (Policy Statements)

56.3.1 3.1 Retention Periods

Retention periods are defined for all information. Retention periods are based on legal, regulatory, and business requirements.

56.3.2 3.2 Retention Schedule

A retention schedule is created and maintained. The retention schedule defines for each information category: - Retention period - Legal basis - Deletion procedure - Responsible role

56.3.3 3.3 Data Minimization and Storage Limitation

Data is retained only as long as necessary (GDPR Art. 5(1)(e)). After expiration of the retention period, data is deleted or anonymized.

56.3.4 3.4 Secure Deletion

Data is securely and irrevocably deleted. Deletion procedures ensure that data cannot be recovered.

56.3.5 3.5 Deletion Concept

A deletion concept defines: - Deletion procedures for different media - Deletion periods and triggers - Responsibilities - Evidence documentation

56.3.6 3.6 Backup Retention

Backups are subject to the same retention periods as production data. Backups are deleted after expiration of the retention period.

56.3.7 3.7 Legal Hold

For legal proceedings or investigations, data may be exempted from deletion (Legal Hold). Legal Hold is documented and monitored.

56.3.8 3.8 Physical Media

Physical media (hard drives, USB drives, paper) are securely disposed of: - Digital media: Secure deletion or physical destruction - Paper: Shredding or certified disposal

56.4 4. Roles and Responsibilities

56.4.1 RACI Matrix: Retention and Deletion

Activity	CISO	DPO	IT Operations	Business Owner	Records Manager
Policy Creation	R/A	C	C	C	C
Retention Schedule	C	C	C	R	R/A

Activity	CISO	DPO	IT Operations	Business Owner	Records Manager
Deletion Concept	R/A	C	R	C	C
Deletion Execution	I	I	R/A	C	C
Legal Hold	C	C	I	C	R/A
Backup Deletion	C	I	R/A	I	C
Physical Disposal	C	I	R/A	I	C

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

56.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **Records Manager:** {{ meta.records.manager }}
- **Data Protection Officer:** {{ meta.dpo.name }}
- **Implementation Responsible:** IT Operations, Business Owner
- **Control/Audit Function:** ISMS, Internal Audit, Legal

56.5 5. Derivatives (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

56.5.1 Associated Guidelines

- **0590_Guideline_Records_Retention_and_Secure_Deletion.md** - Detailed implementation guideline
- `0280_Policy_Data_Classification_and_Information_Handling.md` - Data Classification Policy
- `0560_Policy_Data_Protection_Interfaces.md` - Privacy Policy
- `0420_Policy_Backup_and_Recovery.md` - Backup Policy

56.5.2 Associated Standards/Baselines

- Retention schedule
- Deletion concept
- Secure deletion procedures (NIST SP 800-88, BSI TL-03423)
- Legal Hold process

56.5.3 Associated Processes

- Retention management process
- Deletion process (automated and manual)
- Legal Hold process
- Physical disposal process

56.6 6. Compliance, Monitoring and Enforcement

56.6.1 Metrics and KPIs

- Retention schedule coverage (Target: 100% of information categories)
- Number of deletions performed (planned vs. performed)
- Average time to deletion after expiration (Target: < 30 days)
- Number of legal holds and duration
- Backup deletion compliance (Target: 100%)
- Number of securely disposed physical media

56.6.2 Evidence and Proof

- Retention schedule
- Deletion logs and evidence
- Legal Hold documentation
- Backup deletion logs
- Disposal certificates
- Audit logs for deletions

56.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Non-deleted Data:** Completion, compliance investigation - **Missing Retention Schedule:** Creation, risk assessment - **Insecure Deletion:** Incident response, risk assessment - **Repeated Violations:** Employment consequences, fines

56.7 7. Exceptions

Exceptions to this policy are only permitted in justified exceptional cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and DPO
- **Documentation:** All exceptions are documented in the risk register
- **Time Limitation:** Exceptions are generally time-limited

56.8 8. References

56.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0590_Guideline_Records_Retention_and_Secure_Deletion.md` - Detailed Guideline
- `0280_Policy_Data_Classification_and_Information_Handling.md` - Data Classification Policy
- `0080_ISMS_Risk_Register_Template.md` - Risk Register

56.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.5.33** - Protection of records
- **ISO/IEC 27001:2022 Annex A.5.34** - Privacy and protection of PII

- **ISO/IEC 27001:2022 Annex A.8.10** - Information deletion
- **GDPR Art. 5(1)(e)** - Storage limitation
- **GDPR Art. 17** - Right to erasure
- **NIST SP 800-88** - Guidelines for Media Sanitization
- **BSI TL-03423** - Guide to Deletion and Destruction

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 57

Guideline: Records Retention and Secure Deletion

Document ID: 0590
Document Type: Guideline (detailed)
Associated Policy: 0580_Policy_Retention_and_Deletion.md
Standard Reference: ISO/IEC 27001:2022 Annex A.5.33
Owner: {{ meta.compliance.manager }}
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}

57.1 1. Purpose and Scope

This guideline specifies the `0580_Policy_Retention_and_Deletion.md` and defines: - Retention periods for different data types - Secure deletion procedures - Records management processes

Scope: All data and documents at **AdminSend GmbH**

57.2 2. Retention Periods

57.2.1 2.1 Business Documents

Document Type	Retention Period	Legal Basis
Annual financial statements	10 years	HGB §257
Accounting records	10 years	HGB §257
Invoices	10 years	HGB §257, AO §147
Contracts	10 years after end	HGB §257
Business correspondence	6 years	HGB §257
Quotes	6 years	HGB §257

57.2.2 2.2 Personnel Documents

Document Type	Retention Period	Legal Basis
Personnel files	10 years after departure	GDPR Art. 17
Payroll records	10 years	AO §147
Employment references	3 years	BGB §195
Application documents (rejected)	6 months	AGG §15
Time tracking data	2 years	ArbZG §16

57.2.3 2.3 IT Data

Data Type	Retention Period	Justification
Emails (business)	{{ meta.retention.email_years }} years	Business correspondence
Logs (security)	{{ meta.retention.log_years }} years	Forensics, compliance
Logs (system)	1 year	Troubleshooting
Backups	Per backup policy	Recovery
Audit trails	{{ meta.retention.audit_years }} years	Compliance

57.2.4 2.4 Customer Data

Data Type	Retention Period	Legal Basis
Customer master data	Until contract end + 3 years	Statute of limitations
Order data	10 years	HGB §257
Payment data	10 years	AO §147
Communication	6 years	HGB §257

57.3 3. Retention Management

57.3.1 3.1 Retention Policies

Automation: - Retention labels in Microsoft 365 - Lifecycle policies in cloud storage - Automatic deletion after expiration

Manual Processes: - For physical documents - For legacy systems

57.3.2 3.2 Legal Hold

For Legal Proceedings: - Suspension of deletion - Preservation order - Documentation of legal hold - Lifting after proceedings end

57.3.3 3.3 Retention Register

Documentation: - Data type, retention period, legal basis - Storage location, responsible person - Deletion date - Regular reviews (annually)

57.4 4. Secure Deletion

57.4.1 4.1 Digital Data

Methods per DIN 66399:

Media	Method	Standard
HDD	Software deletion (3-pass) or degaussing	DIN 66399 H-3/H-4
SSD	Secure Erase (ATA) or cryptographic deletion	DIN 66399 H-3
Cloud data	Logical deletion + confirmation	Provider-dependent
Backups	Cryptographic deletion (destroy keys)	DIN 66399 H-4

Tools: - DBAN, Blancco (software deletion) - Degausser (magnetic deletion) - Shredder (physical destruction)

57.4.2 4.2 Physical Documents

Methods per DIN 66399:

Protection Level	Particle Size	Application
P-3	320 mm²	Internal documents
P-4	160 mm²	Confidential documents
P-5	30 mm²	Highly confidential documents

Process: - Shredders in offices (P-3) - Certified disposal partners (P-4, P-5) - Disposal certificate

57.4.3 4.3 Deletion Log

Documentation: - Date of deletion - Deleted data/documents - Deletion method - Person performing deletion - Confirmation of deletion

Retention: {{ meta.retention.deletion_log_years }} years

57.5 5. Email Archiving

57.5.1 5.1 Archiving Obligation

Business Emails: - Automatic archiving - Immutability (WORM) - Retention: {{ meta.retention.email_years }} years

Private Emails: - No archiving - Marking by user (Subject: [PRIVATE])

57.5.2 5.2 Archiving System

System: {{ meta.email.archive_system }}

Functions: - Automatic archiving - Full-text search - eDiscovery - Legal hold

57.5.3 5.3 Archive Access

Permissions: - Users: Own emails - Supervisors: With legitimate interest (with approval) - Legal/Compliance: For audits and investigations - IT admins: Only for technical administration

57.6 6. Data Minimization

57.6.1 6.1 Privacy by Design

Principles: - Collect only necessary data - Choose shortest retention period - Implement automatic deletion

57.6.2 6.2 Regular Reviews

Quarterly: - Identify unused data - Review deletion - Adjust retention policies

57.7 7. Cloud Data Deletion

57.7.1 7.1 SaaS Applications

Process: 1. Logical deletion in application 2. Wait for retention period (provider-dependent) 3. Request confirmation of final deletion 4. Documentation

57.7.2 7.2 IaaS/PaaS

Process: 1. Delete data 2. Delete volumes/disks 3. Delete snapshots 4. Destroy cryptographic keys 5. Confirmation of deletion

57.8 8. Compliance and Audit

57.8.1 8.1 Metrics (KPIs)

Metric	Target Value
Automatic deletion (after expiration)	100%
Deletion log completeness	100%
Retention policy compliance	$> 95\%$
Disposal certificates	100%

57.8.2 8.2 Audit Evidence

- Retention register
- Deletion logs
- Disposal certificates
- Email archiving reports

57.9 9. References

57.9.1 Internal Documents

- `0580_Policy_Retention_and_Deletion.md`
- `0570_Guideline_Data_Protection_Requirements_and_Data_Processing.md`

57.9.2 External Standards

- **ISO/IEC 27001:2022 Annex A.5.33** - Protection of records
- **DIN 66399** - Destruction of data carriers
- **HGB §257** - Retention of documents
- **AO §147** - Regulations for retention of documents

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 58

Policy: Network Security

Document ID: 0600
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.8.20-A.8.23 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

58.1 1. Purpose

This policy defines the requirements for network security at **AdminSend GmbH**. It ensures that networks are properly secured, segmented, and monitored to protect the confidentiality, integrity, and availability of information.

58.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Networks:** All internal and external networks, LAN, WLAN, WAN, VPN
- **Systems:** Firewalls, routers, switches, load balancers, IDS/IPS
- **Connections:** All network connections (internal, external, partner, cloud)
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

58.3 3. Principles (Policy Statements)

58.3.1 3.1 Network Segmentation

Networks are segmented by protection requirements and function. Segmentation is achieved through firewalls, VLANs, and zones (e.g., DMZ, production network, management network).

58.3.2 3.2 Defense in Depth

Network security follows the defense-in-depth principle. Multiple security layers protect against attacks (perimeter, segmentation, host-based).

58.3.3 3.3 Least Privilege Network Access

Network access follows the least privilege principle. Only required connections are permitted (default deny, whitelist approach).

58.3.4 3.4 Firewall Management

Firewalls protect network boundaries. Firewall rules are documented, regularly reviewed, and changed according to change management process.

58.3.5 3.5 Network Access Control (NAC)

Access to networks is controlled. NAC ensures that only authorized and compliant devices gain access.

58.3.6 3.6 Intrusion Detection/Prevention (IDS/IPS)

Networks are monitored for attacks. IDS/IPS systems detect and block suspicious activities.

58.3.7 3.7 VPN and Remote Access

Remote access occurs via secure VPN connections. VPN connections are encrypted and authenticated (MFA).

58.3.8 3.8 Wireless Security

WLAN networks are secured (WPA3, 802.1X). Guest WLANs are separated from production network.

58.3.9 3.9 Network Monitoring and Logging

Network activities are monitored and logged. Logs are centrally collected and analyzed (SIEM).

58.4 4. Roles and Responsibilities

58.4.1 RACI Matrix: Network Security

Activity	CISO	Network Security	IT Operations	SOC	Network Admin
Policy Creation	R/A	R	C	C	C
Network Segmentation	R	R/A	R	C	R
Firewall Management	C	R/A	R	C	R
NAC Implementation	C	R/A	R	C	R
IDS/IPS Operations	C	R	C	R/A	C
VPN Management	C	R/A	R	C	R
WLAN Security	C	R/A	R	C	R
Network Monitoring	C	R	C	R/A	C

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

58.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **Network Security Manager:** {{ meta.network.security_manager }}
- **Network Administrator:** {{ meta.network.admin }}
- **SOC Manager:** {{ meta.soc.manager }}
- **Implementation Responsible:** IT Operations, Network Team
- **Control/Audit Function:** ISMS, Internal Audit, SOC

58.5 5. Derivatives (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

58.5.1 Associated Guidelines

- **0610_Guideline_Segmentation_Firewalling_and_Network_Access_Control.md** - Detailed implementation guideline
- `0220_Policy_Access_Control_and_Identity_Management.md` - Access Control Policy
- `0320_Policy_Logging_and_Monitoring.md` - Logging and Monitoring Policy
- `0500_Policy_Mobile_Device_and_Remote_Work.md` - Remote Work Policy

58.5.2 Associated Standards/Baselines

- Network segmentation concept

- Firewall ruleset
- NAC configuration
- IDS/IPS signatures and rules
- VPN configuration
- WLAN security baseline

58.5.3 Associated Processes

- Firewall change management
- NAC onboarding/offboarding
- IDS/IPS alert response
- VPN access request
- Network security monitoring

58.6 6. Compliance, Monitoring and Enforcement

58.6.1 Metrics and KPIs

- Network segmentation coverage (Target: 100% of critical systems)
- Firewall rule review frequency (Target: quarterly)
- NAC coverage (Target: 100% production network)
- IDS/IPS alert response time (Target: $<$ 15 minutes for critical alerts)
- VPN availability (Target: 99.5%)
- WLAN security compliance (Target: 100% WPA3)
- Number of blocked attacks (IDS/IPS)

58.6.2 Evidence and Proof

- Network diagrams and segmentation concept
- Firewall ruleset and change logs
- NAC configuration and device inventory
- IDS/IPS logs and alert reports
- VPN logs and access logs
- WLAN configuration and security scans
- Network monitoring dashboards

58.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Unauthorized Firewall Changes:** Incident response, rollback, disciplinary action - **Missing Segmentation:** Completion, risk assessment - **Insecure WLAN Configuration:** Immediate correction, incident response - **Repeated Violations:** Employment consequences, access revocation

58.7 7. Exceptions

Exceptions to this policy are only permitted in justified exceptional cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and Network Security Manager

- **Documentation:** All exceptions are documented in the risk register
- **Time Limitation:** Exceptions are generally time-limited

58.8 8. References

58.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0610_Guideline_Segmentation_Firewalling_and_Network_Access_Control.md` - Detailed Guideline
- `0220_Policy_Access_Control_and_Identity_Management.md` - Access Control Policy
- `0080_ISMS_Risk_Register_Template.md` - Risk Register

58.8.2 External Standards and Requirements

- **ISO/IEC 27001:2022 Annex A.8.20** - Networks security
- **ISO/IEC 27001:2022 Annex A.8.21** - Security of network services
- **ISO/IEC 27001:2022 Annex A.8.22** - Segregation of networks
- **ISO/IEC 27001:2022 Annex A.8.23** - Web filtering
- **NIST SP 800-41** - Guidelines on Firewalls and Firewall Policy
- **NIST SP 800-97** - Establishing Wireless Robust Security Networks
- **BSI IT-Grundschutz** - NET.1.1, NET.1.2, NET.3.2

Approved by:
{{ meta.management.ceo }}, Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 59

Guideline: Segmentation, Firewalling and Network Access Control

Document ID: 0610
Document Type: Guideline (detailed)
Associated Policy: 0600_Policy_Network_Security.md
Standard Reference: ISO/IEC 27001:2022 Annex A.8.20, A.8.21, A.8.22
Owner: {{ meta.network.manager }}
Version: 1.0
Status: Approved
Classification: Confidential
Last Updated: {{ meta.document.date }}

59.1 1. Purpose and Scope

This guideline specifies the `0600_Policy_Network_Security.md` and defines: - Network segmentation and zone model - Firewall rules and management - Network Access Control (NAC)

Scope: All networks at **AdminSend GmbH**

59.2 2. Network Segmentation

59.2.1 2.1 Zone Model

Zone 1: Internet (Untrusted) - Public internet - No trust relationship

Zone 2: DMZ (Demilitarized Zone) - Internet-facing services (web servers, email gateway) - Restricted access to internal resources

Zone 3: Corporate Network - Internal office networks - Workstations, printers - Standard security controls

Zone 4: Server Network - Internal servers (file servers, application servers) - Enhanced security controls

Zone 5: Management Network - Management interfaces (IPMI, iLO, iDRAC) - Out-of-band management - Highest security controls

Zone 6: Production Network - Critical production systems - Databases, ERP - Highest security controls

59.2.2 2.2 VLAN Segmentation

VLAN Schema: - VLAN 10: Management - VLAN 20: Servers - VLAN 30: Workstations - VLAN 40: Guest/BYOD - VLAN 50: IoT/OT - VLAN 60: DMZ

Inter-VLAN Routing: - Via firewall (not Layer 3 switch) - Explicit firewall rules required

59.2.3 2.3 Micro-Segmentation

For Critical Systems: - Segmentation at workload level - Software-Defined Networking (SDN) - Zero Trust Network Access (ZTNA)

59.3 3. Firewall Management

59.3.1 3.1 Firewall Architecture

Perimeter Firewall: - Internet DMZ - Internet Corporate Network - High availability (Active/Active or Active/Passive)

Internal Firewalls: - Between zones - Micro-segmentation

Firewall Platform: {{ meta.network.firewall }}

59.3.2 3.2 Firewall Rules

Default Deny: - All connections blocked by default - Only explicitly allowed connections

Rule Structure: - Source (IP/network) - Destination (IP/network) - Service (port/protocol) - Action (Allow/Deny) - Logging (Enabled) - Justification (business justification)

Rule Order: 1. Deny rules (specific) 2. Allow rules (specific to general) 3. Default deny (implicit)

59.3.3 3.3 Firewall Change Process

Request: - Change request via ticket system - Justification (business justification) - Source and destination IP/port - Time limitation (where possible)

Approval: - IT Security: Mandatory - Network team: Technical feasibility - Application owner: Business justification

Implementation: - Testing in dev/test (where possible) - Implementation in maintenance window - Verification - Documentation

Details: See `0370_Guideline_Change_Management_with_Security_Approvals`

59.3.4 3.4 Firewall Review

Regular Reviews: - Quarterly: Review all firewall rules - Identify unused rules - Extend or delete temporary rules - Update documentation

59.4 4. Network Access Control (NAC)

59.4.1 4.1 NAC System

Platform: {{ meta.network.nac_solution }} (e.g., Cisco ISE, Aruba ClearPass)

Functions: - 802.1X authentication - MAC address authentication (MAB) - Guest access - Posture assessment

59.4.2 4.2 802.1X Authentication

For Workstations: - Computer authentication (machine auth) - User authentication (user auth) - Certificate-based or EAP-TLS

For Servers: - Certificate-based authentication - Dedicated VLANs

59.4.3 4.3 Posture Assessment

Compliance Checks: - Antivirus active and current? - Firewall enabled? - OS patches current? - Disk encryption enabled?

For Non-Compliance: - Quarantine VLAN - Restricted access (patch servers only) - Notification to user

59.4.4 4.4 Guest Access

Guest VLAN: - Isolated from corporate network - Internet access only - Captive portal for registration

Process: 1. Guest registers (self-service or sponsor) 2. Credentials via SMS/email 3. Time-limited access (max. 24 hours) 4. Automatic deactivation

59.5 5. Intrusion Detection/Prevention (IDS/IPS)

59.5.1 5.1 IDS/IPS Placement

Perimeter: - Before firewall (IDS) - Behind firewall (IPS)

Internal: - Between critical zones - IPS mode

IDS/IPS System: {{ meta.security.ids_ips }}

59.5.2 5.2 Signatures and Policies

Signature Updates: - Automatic, daily - Critical signatures: Immediate

IPS Policies: - Balanced (standard) - Connectivity (less aggressive) - Security (more aggressive)

59.5.3 5.3 Alerting

SIEM Integration: - All IDS/IPS alerts to SIEM - Correlation with other events - Automatic response (for critical alerts)

59.6 6. VPN and Remote Access

59.6.1 6.1 VPN Types

Site-to-Site VPN: - Between locations - IPsec - Always-on

Remote Access VPN: - For remote employees - SSL-VPN or IPsec - MFA mandatory

Details: See `0510_Guideline_MDM_BringYourOwnDevice_and_Remote_Access.md`

59.6.2 6.2 VPN Segmentation

VPN Users in Separate VLAN: - Not directly in corporate network - Firewall rules for access - Posture assessment before access

59.7 7. Wireless Security

59.7.1 7.1 WLAN Segmentation

Corporate WLAN: - 802.1X authentication - WPA3-Enterprise - Access to corporate resources

Guest WLAN: - Captive portal - WPA2/WPA3-Personal - Internet access only

IoT WLAN: - Separate VLAN - MAC address whitelist - Restricted access

59.7.2 7.2 WLAN Security

Encryption: - WPA3-Enterprise (corporate) - WPA2/WPA3-Personal (guest) - No WEP, WPA

Rogue AP Detection: - Automatic scans - Alerts for unauthorized APs

59.8 8. Network Monitoring

59.8.1 8.1 Flow Monitoring

NetFlow/sFlow: - Collection of flow data - Analysis of traffic patterns - Anomaly detection

Tools: {{ meta.network.flow_tool }}

59.8.2 8.2 Packet Capture

For Forensics: - Packet capture at critical points - Retention: 7 days - Access only for security team

59.9 9. Compliance and Audit

59.9.1 9.1 Metrics (KPIs)

Metric	Target Value
Firewall rule review completion	100% quarterly
Unused firewall rules	$< 10\%$
NAC compliance rate	$> 95\%$
IPS false positive rate	$< 5\%$

59.9.2 9.2 Audit Evidence

- Firewall configurations
- Firewall change logs
- NAC compliance reports
- IDS/IPS alerts and responses

59.10 10. References

59.10.1 Internal Documents

- `0600_Policy_Network_Security.md`
- `0370_Guideline_Change_Management_with_Security_Approvals.md`

59.10.2 External Standards

- **ISO/IEC 27001:2022 Annex A.8.20** - Networks security
- **ISO/IEC 27001:2022 Annex A.8.21** - Security of network services
- **ISO/IEC 27001:2022 Annex A.8.22** - Segregation of networks
- **NIST SP 800-41** - Guidelines on Firewalls and Firewall Policy

---

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 60

Policy: Endpoint Security

Document ID: 0620
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.8.1-A.8.3, A.6.7 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

60.1 1. Purpose

This policy defines the endpoint security requirements of **AdminSend GmbH**. It ensures that all endpoint devices (workstations, laptops, mobile devices) are appropriately secured and protected against threats.

60.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Devices:** All endpoint devices (workstations, laptops, tablets, smartphones)
- **Operating Systems:** Windows, macOS, Linux, iOS, Android
- **Ownership:** Company-owned and BYOD devices (with corporate access)
- **Locations:** {{ netbox.site.name }} and all other operational sites, remote work

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

60.3 3. Policy Statements

60.3.1 3.1 Endpoint Protection Platform (EPP)

All endpoint devices are equipped with endpoint protection. EPP includes antivirus, anti-malware, host firewall, and application control.

60.3.2 3.2 Endpoint Detection and Response (EDR)

Critical endpoint devices are equipped with EDR solution. EDR enables advanced threat detection, incident response, and forensics.

60.3.3 3.3 Device Compliance

Endpoint devices must meet compliance requirements: - Current operating system version - Current security patches - EPP/EDR installed and active - Disk encryption enabled - Screen lock configured

60.3.4 3.4 Disk Encryption

All endpoint devices with corporate data are encrypted (full disk encryption). Encryption protects against data loss in case of theft or loss.

60.3.5 3.5 Host-based Firewall

All endpoint devices have an enabled host firewall. Firewall rules follow the least privilege principle.

60.3.6 3.6 Application Control

Unauthorized applications are blocked (application whitelisting or blacklisting). Application control reduces malware risk.

60.3.7 3.7 Patch Management

Endpoint devices are patched regularly. Security patches are installed promptly (see `0340_Policy_Vulnerability_and_Patch_Management.md`).

60.3.8 3.8 Remote Wipe

Lost or stolen devices can be remotely wiped. Remote wipe protects against data loss.

60.3.9 3.9 BYOD (Bring Your Own Device)

BYOD devices with corporate access must meet minimum security requirements. BYOD is managed via MDM/MAM (see `0500_Policy_Mobile_Device_and_Remote_Work.md`).

60.4 4. Roles and Responsibilities

60.4.1 RACI Matrix: Endpoint Security

Activity	CISO	Endpoint Security	IT Operations	SOC	End User
Policy Creation	R/A	R	C	C	I
EPP/EDR Deployment	C	R/A	R	C	I
Device Compliance	C	R/A	R	C	R
Disk Encryption	C	R/A	R	I	C
Patch Management	C	R	R/A	I	C
Remote Wipe	C	R/A	C	C	I
BYOD Management	C	R/A	R	I	R
Incident Response	C	R	C	R/A	I

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

60.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **Endpoint Security Manager:** {{ meta.endpoint.security_manager }}
- **IT Operations Manager:** {{ meta.it.operations_manager }}
- **SOC Manager:** {{ meta.soc.manager }}
- **Implementation Responsible:** IT Operations, End Users
- **Control/Audit Function:** ISMS, Internal Audit, SOC

60.5 5. Derived Documents (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

60.5.1 Related Guidelines

- **0630_Guideline_EDR_AV_Host_Firewall_and_Device_Compliance.md** - Detailed implementation guideline
- `0500_Policy_Mobile_Device_and_Remote_Work.md` - Mobile Device Policy
- `0340_Policy_Vulnerability_and_Patch_Management.md` - Patch Management Policy
- `0260_Policy_Cryptography_and_Key_Management.md` - Encryption Policy

60.5.2 Related Standards/Baselines

- Endpoint Security Baseline (Windows, macOS, Linux)
- EPP/EDR Configuration
- Device Compliance Requirements
- Disk Encryption Standards
- Application Whitelist/Blacklist

60.5.3 Related Processes

- Endpoint Onboarding/Offboarding
- Device Compliance Monitoring
- EPP/EDR Alert Response

- Remote Wipe Process
- BYOD Enrollment

60.6 6. Compliance, Monitoring and Enforcement

60.6.1 Metrics and KPIs

- EPP/EDR Coverage (Target: 100% of all endpoints)
- Device Compliance Rate (Target: >95%)
- Disk Encryption Coverage (Target: 100%)
- Patch Compliance (Target: >95% within SLA)
- EPP/EDR Detection Rate
- Average Incident Response Time (Target: < 30 minutes)
- Number of Remote Wipes

60.6.2 Evidence and Proof

- Endpoint Inventory
- EPP/EDR Deployment Status
- Device Compliance Reports
- Disk Encryption Status
- Patch Compliance Reports
- EPP/EDR Logs and Alerts
- Remote Wipe Logs

60.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Non-compliant Devices:** Network access blocked until compliance is established - **Disabled EPP/EDR:** Immediate reactivation, incident response - **Missing Disk Encryption:** Remediation, access restriction - **Repeated Violations:** Employment consequences, device usage prohibited

60.7 7. Exceptions

Exceptions to this policy are only permitted in justified exceptional cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and Endpoint Security Manager
- **Documentation:** All exceptions are documented in the risk register
- **Time Limitation:** Exceptions are generally time-limited

60.8 8. References

60.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0630_Guideline_EDR_AV_Host_Firewall_and_Device_Compliance.md` - Detailed Guideline
- `0500_Policy_Mobile_Device_and_Remote_Work.md` - Mobile Device Policy

- `0080_ISMS_Risk_Register_Template.md` - Risk Register

60.8.2 External Standards and Regulations

- **ISO/IEC 27001:2022 Annex A.8.1** - User endpoint devices
- **ISO/IEC 27001:2022 Annex A.8.2** - Privileged access rights
- **ISO/IEC 27001:2022 Annex A.8.3** - Information access restriction
- **ISO/IEC 27001:2022 Annex A.6.7** - Remote working
- **NIST SP 800-124** - Guidelines for Managing the Security of Mobile Devices
- **NIST SP 800-171** - Protecting Controlled Unclassified Information
- **CIS Controls v8** - Control 4 (Secure Configuration of Enterprise Assets)

Approved by:
{{ meta.management.ceo }}, Executive Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 61

Guideline: EDR, Antivirus, Host Firewall and Device Compliance

Document ID: 0630
Document Type: Guideline (detailed)
Related Policy: 0620_Policy_Endpoint_Security.md
Standard Reference: ISO/IEC 27001:2022 Annex A.8.7
Owner: {{ meta.it_operations.manager }}
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}

61.1 1. Purpose and Scope

This guideline implements `0620_Policy_Endpoint_Security.md` and defines: - Endpoint Detection and Response (EDR) requirements - Antivirus configuration and management - Host firewall policies - Device compliance requirements

Scope: All endpoints at **AdminSend GmbH**

61.2 2. Endpoint Detection and Response (EDR)

61.2.1 2.1 EDR System

Platform: {{ meta.security.edr_solution }} (e.g., CrowdStrike, SentinelOne, Microsoft Defender for Endpoint)

Functions: - Real-time Threat Detection - Behavioral Analysis - Automated Response - Forensic Capabilities - Threat Hunting

61.2.2 2.2 EDR Deployment

Mandatory Installation: - All workstations (Windows, macOS, Linux) - All servers - No exceptions (except via exception process)

Deployment Methods: - Group Policy (Windows) - MDM (macOS, Mobile) - Configuration Management (Linux)

61.2.3 2.3 EDR Policies

Detection Modes: - **Prevent:** Automatic blocking (default) - **Detect:** Alerting only (for legacy systems)

Behavioral Policies: - Ransomware Protection - Credential Theft Protection - Exploit Protection - Script Control (PowerShell, CMD)

61.2.4 2.4 EDR Response

Automated Actions: - Malware Quarantine - Process Termination - Network Isolation (for critical threats)

Manual Actions: - Remote Shell for forensics - File Retrieval - Memory Dump

61.2.5 2.5 Tamper Protection

Protection Against Deactivation: - EDR agent cannot be disabled (without admin password) - Uninstall password required - Alerts on tamper attempts

61.3 3. Antivirus (AV)

61.3.1 3.1 AV System

Platform: {{ meta.security.av_solution }} (often integrated in EDR)

Scan Types: - Real-time Scanning (On-Access) - Scheduled Full Scans (weekly) - Quick Scans (daily)

61.3.2 3.2 AV Configuration

Scan Settings: - Scan all file types - Scan archives - Scan email attachments - Scan removable media

Exclusions: - Only after approval by IT Security - Documentation required - Regular review (quarterly)

61.3.3 3.3 Signature Updates

Automatic Updates: - Multiple times daily - Via internal update servers (WSUS, etc.) - Fallback to cloud updates

Monitoring: - Alerts for outdated signatures (> 7 days)

61.3.4 3.4 Malware Handling

Upon Malware Detection: 1. Automatic quarantine 2. Alert to security team 3. Create incident ticket 4. Forensic analysis (if needed) 5. Remediation 6. Lessons learned

61.4 4. Host Firewall

61.4.1 4.1 Windows Firewall

Configuration via GPO: - Firewall enabled (all profiles: Domain, Private, Public) - Inbound: Default Deny - Outbound: Default Allow (with exceptions)

Allowed Inbound Connections: - Remote Desktop (only from management VLAN) - File Sharing (only in corporate network) - Monitoring Agents

61.4.2 4.2 macOS Firewall

Configuration via MDM: - Application Firewall enabled - Stealth Mode enabled - Only signed apps allowed

61.4.3 4.3 Linux Firewall

iptables/firewalld: - Default Deny for inbound - Only required services allowed - Logging enabled

61.5 5. Device Compliance

61.5.1 5.1 Compliance Requirements

Mandatory Requirements: - EDR/AV installed and active - OS patches current (< 30 days old) - Disk encryption enabled - Host firewall enabled - Screen lock configured (max. 15 minutes) - No jailbreak/root (mobile)

61.5.2 5.2 Compliance Checks

Automatic Verification: - At every network access (NAC) - At VPN connection - Daily (endpoint management)

Upon Non-Compliance: - Warning to user (24-hour grace period) - Restricted network access - Complete blocking after 7 days

61.5.3 5.3 Compliance Reporting

Weekly Report: - Compliance rate per department - Top non-compliance items - Trend analysis

Target: > 95% compliance

61.6 6. Patch Management

61.6.1 6.1 OS Patches

Windows: - WSUS for patch distribution - Automatic installation (outside business hours) - Reboot window: Weekend

macOS: - Automatic updates via MDM - Deferred updates (7-day test period)

Linux: - Automatic security updates (unattended-upgrades) - Manual updates for kernel

61.6.2 6.2 Application Patches

Third-Party Applications: - Ninite, Chocolatey for automatic updates - Manual updates for critical apps

Patch SLA: - Critical: 7 days - High: 30 days - Medium: 90 days

Details: See `0350_Guideline_Vulnerability_Scans_Patching`

61.7 7. Application Control

61.7.1 7.1 Application Whitelisting

For Critical Systems: - Only signed, approved applications - Blocking of unapproved software - Exceptions via ticketing system

Tools: - Windows Defender Application Control (WDAC) - AppLocker

61.7.2 7.2 Script Control

PowerShell: - Constrained Language Mode - Script signing required - Logging enabled

CMD/Batch: - Blocked for standard users - Only for admins

61.8 8. USB and Removable Media

61.8.1 8.1 USB Control

Policies: - USB storage blocked (standard users) - Only approved USB devices (whitelist) - Automatic scanning upon connection

Exceptions: - Request via ticketing system - Time-limited - Encrypted USB drives

61.8.2 8.2 DLP for Removable Media

Data Loss Prevention: - Blocking of confidential data on USB - Alerts on copy attempts - Logging of all USB activities

61.9 9. Monitoring and Alerting

61.9.1 9.1 Endpoint Monitoring

Monitored Metrics: - EDR/AV status - Patch level - Compliance status - Malware detections - Anomalies (CPU, network)

61.9.2 9.2 SIEM Integration

Events to SIEM: - Malware detections - EDR alerts - Compliance violations - Tamper attempts

61.9.3 9.3 Automated Response

SOAR Integration: - Automatic isolation upon malware - Automatic ticket creation - Automatic notifications

61.10 10. Compliance and Audit

61.10.1 10.1 Metrics (KPIs)

Metric	Target Value
EDR Deployment Rate	100%
AV Signature Currency	100%
Device Compliance Rate	> 95%
Malware Detection Rate	Baseline
Patch Compliance (30 days)	> 90%

61.10.2 10.2 Audit Evidence

- EDR Deployment Status
- Compliance Reports
- Malware Incident Reports
- Patch Compliance Reports

61.11 11. References

61.11.1 Internal Documents

- `0620_Policy_Endpoint_Security.md`
- `0350_Guideline_Vulnerability_Scans_Patching_and_Exploitation_Response.md`

61.11.2 External Standards

- **ISO/IEC 27001:2022 Annex A.8.7** - Protection against malware
- **NIST SP 800-83** - Guide to Malware Incident Prevention and Handling
- **CIS Controls** - Malware Defenses

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 62

Policy: Exceptions and Risk Waivers

Document ID: 0640
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.5.1, A.6.1.2 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

62.1 1. Purpose

This policy defines the process for exceptions and risk waivers from security policies of **AdminSend GmbH**. It ensures that exceptions are appropriately justified, approved, documented, and monitored.

62.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Policies:** All security policies and standards
- **Systems:** All IT systems and applications
- **Processes:** All security-relevant processes
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: This policy itself is not subject to an exception process.

62.3 3. Policy Statements

62.3.1 3.1 Exceptions as Exception

Exceptions to security policies are the exception, not the rule. Policies must generally be complied with.

62.3.2 3.2 Formal Exception Process

Exceptions must be requested through a formal process. Informal or verbal exceptions are not permitted.

62.3.3 3.3 Justification Requirement

Every exception must be justified: - Business necessity - Technical impossibility - Disproportionate effort - Time limitation

62.3.4 3.4 Risk Assessment

A risk assessment is conducted for every exception. Risks are identified, evaluated, and documented.

62.3.5 3.5 Compensating Controls

Exceptions require compensating controls. Compensating controls reduce residual risk to an acceptable level.

62.3.6 3.6 Approval Requirement

Exceptions must be approved by authorized persons: - **Low Risk:** CISO or deputy - **Medium Risk:** CISO + Business Owner - **High Risk:** CISO + CIO + Management

62.3.7 3.7 Time Limitation

Exceptions are generally time-limited. Maximum duration: 12 months. Extensions require renewed approval.

62.3.8 3.8 Documentation

All exceptions are centrally documented (exception register). Documentation includes: - Requester and date - Affected policy/standard - Justification - Risk assessment - Compensating controls - Approver and date - Duration and review date

62.3.9 3.9 Monitoring and Review

Exceptions are reviewed regularly (at least quarterly). Exceptions no longer needed are withdrawn.

62.4 4. Roles and Responsibilities

62.4.1 RACI Matrix: Exceptions and Risk Waivers

Activity	CISO	CIO	Business Owner	Risk Manager	ISMS Team
Policy Creation	R/A	C	C	C	C
Exception Request	I	I	R	I	C
Risk Assessment	R/A	C	C	R	C
Compensating Controls	R/A	C	R	C	C
Approval (Low)	R/A	I	I	I	I
Approval (Medium)	R/A	I	R/A	C	I
Approval (High)	R/A	R/A	R/A	C	I
Exception Register	C	I	I	C	R/A
Monitoring & Review	R/A	C	C	C	R

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

62.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **CIO:** Anna Schmidt
- **Risk Manager:** {{ meta.risk.manager }}
- **ISMS Team:** {{ meta.isms.team }}
- **Requester:** Business Owner, IT Operations
- **Control/Audit Function:** ISMS, Internal Audit

62.5 5. Derived Documents (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

62.5.1 Related Guidelines

- **0650_Guideline_Exception_Process.md** - Detailed implementation guideline
- `0060_ISMS_Risk_Management_Methodology.md` - Risk Management Methodology
- `0080_ISMS_Risk_Register_Template.md` - Risk Register

62.5.2 Related Standards/Baselines

- Exception Request Template
- Risk Assessment Template
- Compensating Controls Catalog
- Exception Register

62.5.3 Related Processes

- Exception Request Process
- Risk Assessment Process
- Approval Process
- Monitoring and Review Process

62.6 6. Compliance, Monitoring and Enforcement

62.6.1 Metrics and KPIs

- Number of active exceptions
- Average duration of exceptions
- Number of expired exceptions (Target: 0)
- Number of extended exceptions
- Exceptions by risk category (Low/Medium/High)
- Review compliance (Target: 100% quarterly)
- Number of withdrawn exceptions

62.6.2 Evidence and Proof

- Exception Register
- Exception requests and approvals
- Risk assessments
- Compensating controls documentation
- Review protocols
- Audit logs for exceptions

62.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Unapproved Exceptions:** Immediate compliance establishment or system shutdown - **Missing Documentation:** Remediation, compliance investigation - **Expired Exceptions:** Immediate compliance establishment or extension request - **Repeated Violations:** Employment consequences, escalation to management

62.7 7. Exceptions

This policy itself is not subject to an exception process. Changes to this policy require management approval.

62.8 8. References

62.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0650_Guideline_Exception_Process.md` - Detailed Guideline
- `0060_ISMS_Risk_Management_Methodology.md` - Risk Management Methodology
- `0080_ISMS_Risk_Register_Template.md` - Risk Register

62.8.2 External Standards and Regulations

- **ISO/IEC 27001:2022 Annex A.5.1** - Policies for information security
- **ISO/IEC 27001:2022 Annex A.6.1.2** - Segregation of duties
- **ISO/IEC 27005** - Information security risk management
- **NIST SP 800-37** - Risk Management Framework

- **COBIT 2019** - APO12 (Managed Risk)

Approved by:
{{ meta.management.ceo }}, Executive Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 63

Guideline: Exception Process

Document ID: 0650
Document Type: Guideline (detailed)
Related Policy: 0640_Policy_Exceptions_and_Risk_Waivers.md
Standard Reference: ISO/IEC 27001:2022 Annex A.5.1
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}

63.1 1. Purpose and Scope

This guideline implements `0640_Policy_Exceptions_and_Risk_Waivers.md` and defines: - Exception process for security policies - Risk waiver procedures - Compensating controls

Scope: All security policies at **AdminSend GmbH**

63.2 2. Exception Categories

63.2.1 2.1 Temporary Exceptions

Definition: Time-limited deviation from policy

Examples: - Delayed patching (due to compatibility issues) - Temporary firewall rule for project - Delayed compliance (during migration)

Maximum Duration: 12 months

63.2.2 2.2 Permanent Exceptions

Definition: Permanent deviation from policy

Examples: - Legacy systems that cannot meet baseline - Special business requirements - Technical impossibility

Review Frequency: Annually

63.2.3 2.3 Emergency Exceptions

Definition: Immediate exception in emergencies

Examples: - Critical business requirement - System outage remediation - Security incident response

Retroactive Approval: Within 48 hours

63.3 3. Exception Process

63.3.1 3.1 Request Submission

Request via: {{ meta.itsm.portal }} (ticketing system)

Mandatory Information: - Affected policy/guideline - Description of deviation - Justification (business justification) - Affected systems/processes - Risk assessment - Proposed compensating controls - Desired duration

Requester: System owner or department head

63.3.2 3.2 Risk Assessment

Conducted by: IT Security Team

Assessment Criteria: - Likelihood of security incident - Potential impact - Affected assets and data - Existing controls - Proposed compensating controls

Risk Matrix: | Likelihood | Low Impact | Medium Impact | High Impact | |————|————|————|————-| | Low | Low | Low | Medium | | Medium | Low | Medium | High | | High | Medium | High | Critical |

63.3.3 3.3 Compensating Controls

Definition: Alternative security measures to minimize risk

Examples: - Network isolation (for missing patches) - Increased monitoring (for weaker authentication) - Manual processes (for missing automation) - Additional access restrictions

Requirement: - Compensating controls must reduce risk to acceptable level - Documentation of effectiveness

63.3.4 3.4 Approval

Approval Levels:

Risk	Approver	SLA
Low	IT Security Manager	3 business days
Medium	CISO	5 business days
High	CISO + CIO	7 business days
Critical	CISO + CIO + Executive Management	10 business days

Approval Criteria: - Business justification comprehensible - Risk acceptable (with compensating controls) - No alternative available - Time-limited (for temporary exceptions)

Rejection: - Justification required - Propose alternative solutions

63.3.5 3.5 Documentation

Exception Register: - All approved exceptions - Requester, approver, date - Risk assessment - Compensating controls - Expiration date - Review date

Storage Location: {{ meta.compliance.exception_register }}

63.4 4. Monitoring and Review

63.4.1 4.1 Ongoing Monitoring

Responsibility: IT Security Team

Activities: - Verify effectiveness of compensating controls - Compliance with exception conditions - Incidents related to exceptions

Frequency: Monthly (for critical exceptions), quarterly (for others)

63.4.2 4.2 Regular Review

Temporary Exceptions: - Review 30 days before expiration - Decision: Extend, terminate, make permanent

Permanent Exceptions: - Annual review - Verify necessity - Update risk assessment

Emergency Exceptions: - Review within 7 days after approval - Regularization or termination

63.4.3 4.3 Escalation

In Case of Problems: - Compensating controls ineffective - Risk increased - Incidents related to exception

Escalate to: - CISO (immediately) - Risk Committee (for critical exceptions)

63.5 5. Exception Termination

63.5.1 5.1 Planned Termination

Upon Expiration: 1. Notification to requester (30 days in advance) 2. Create remediation plan 3. Implement remediation 4. Verification 5. Close exception

63.5.2 5.2 Early Termination

Reasons: - Risk no longer acceptable - Compensating controls ineffective - Alternative solution available - Business requirement no longer exists

Process: 1. Decision by CISO 2. Notification to requester 3. Immediate remediation (or system shutdown) 4. Documentation

63.6 6. Reporting

63.6.1 6.1 Monthly Exception Report

Contents: - Number of active exceptions (by risk) - New exceptions in month - Expired exceptions - Overdue reviews - Top exceptions by risk

Recipients: CISO, CIO, Risk Committee

63.6.2 6.2 Quarterly Management Report

Contents: - Trend analysis - Exceptions by category/department - Risk posture - Improvement measures

Recipients: Executive Management, Audit Committee

63.7 7. Compliance and Audit

63.7.1 7.1 Metrics (KPIs)

Metric	Target Value
Exceptions with current review	100%
Overdue exceptions	0
Exceptions with compensating controls	100%
Average exception duration	$<$ 6 months

63.7.2 7.2 Audit Evidence

- Exception Register
- Requests and approvals
- Risk assessments
- Review protocols
- Monitoring reports

63.8 8. Examples

63.8.1 8.1 Example: Delayed Patching

Scenario: Critical patch causes compatibility issues with business application

Request: - Policy: Patch Management (critical patches within 7 days) - Deviation: Delay by 30 days - Justification: Compatibility issue, vendor working on fix - Risk: High (known exploit)

Compensating Controls: - Network isolation of affected system - IPS signature activated - Increased monitoring - Access restrictions

Approval: CISO + CIO
Duration: 30 days
Review: Weekly

63.8.2 8.2 Example: Legacy System

Scenario: Legacy system cannot meet security baseline

Request: - Policy: Security Baseline (CIS Benchmark Level 1) - Deviation: Outdated OS, no patches available - Justification: Critical business application, no migration possible (short-term) - Risk: High

Compensating Controls: - Dedicated VLAN (isolated) - Firewall rules (only required connections) - No internet access - Read-only access for standard users - Increased monitoring and logging - Annual penetration tests

Approval: CISO + CIO + Executive Management
Duration: Permanent (until migration)
Review: Annually

63.9 9. References

63.9.1 Internal Documents

- `0640_Policy_Exceptions_and_Risk_Waivers.md`
- All security policies and guidelines

63.9.2 External Standards

- **ISO/IEC 27001:2022 Annex A.5.1** - Policies for information security
- **NIST SP 800-53** - Security and Privacy Controls (Tailoring)

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 64

Policy: Information Transfer and Communication

Document ID: 0660
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.5.14, A.8.24, A.8.26 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

64.1 1. Purpose

This policy defines the requirements for secure information transfer and communication of **AdminSend GmbH**. It ensures that information is appropriately protected during transmission and that communication channels are secure.

64.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Communication Channels:** Email, messaging, file sharing, collaboration tools
- **Data:** All information (especially confidential and personal data)
- **Transmission Paths:** Internal, external, cloud, partners
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

64.3 3. Policy Statements

64.3.1 3.1 Encrypted Transmission

Confidential information is transmitted encrypted. Encryption occurs in transit (TLS/SSL) and at rest.

64.3.2 3.2 Email Security

Email communication is secured: - **Inbound:** SPF, DKIM, DMARC, anti-spam, anti-malware - **Outbound:** TLS encryption, S/MIME or PGP for confidential content - **Phishing Protection:** User awareness, technical protection measures

64.3.3 3.3 Secure File Sharing

File sharing occurs via approved platforms. Confidential files are shared encrypted. Public file sharing (e.g., WeTransfer) is prohibited for confidential data.

64.3.4 3.4 Collaboration Tools

Collaboration tools (Teams, Slack, etc.) must meet security requirements: - Encrypted communication - Access control - Data Loss Prevention (DLP) - Audit logging

64.3.5 3.5 Messaging and Chat

Instant messaging for business communication occurs via approved tools. Private messaging apps are prohibited for confidential business information.

64.3.6 3.6 Data Loss Prevention (DLP)

DLP systems prevent unintentional or malicious data exfiltration. DLP monitors email, file sharing, and collaboration tools.

64.3.7 3.7 External Communication

Communication with external parties (customers, partners, suppliers) occurs via secure channels. Confidentiality agreements (NDAs) are concluded as needed.

64.3.8 3.8 Mobile Communication

Mobile communication (smartphones, tablets) occurs via secure channels. Mobile devices are managed with MDM/MAM (see `0500_Policy_Mobile_Device_and_Remote_Work.md`).

64.3.9 3.9 Social Media

Business social media use follows social media guidelines. Confidential information is not shared via social media.

64.4 4. Roles and Responsibilities

64.4.1 RACI Matrix: Information Transfer and Communication

Activity	CISO	IT Operations	Communication Security	End User	DPO
Policy Creation	R/A	C	R	I	C
Email Security	C	R/A	R	I	C
File Sharing	C	R/A	R	R	C
Collaboration Tools	C	R/A	R	R	C
DLP Implementation	R/A	R	R	I	C
External Communication	C	C	C	R	C
Mobile Communication	C	R/A	C	R	I
Social Media	C	I	R/A	R	I

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

64.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **Communication Security Manager:** {{ meta.communication.security_manager }}
- **IT Operations Manager:** {{ meta.it.operations_manager }}
- **Data Protection Officer:** {{ meta.dpo.name }}
- **Implementation Responsible:** IT Operations, End Users
- **Control/Audit Function:** ISMS, Internal Audit, DPO

64.5 5. Derived Documents (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

64.5.1 Related Guidelines

- **0670_Guideline_Email_Sharing_and_Collaboration_Tools.md** - Detailed implementation guideline
- `0280_Policy_Data_Classification_and_Information_Handling.md` - Data Classification Policy
- `0260_Policy_Cryptography_and_Key_Management.md` - Encryption Policy
- `0500_Policy_Mobile_Device_and_Remote_Work.md` - Mobile Device Policy

64.5.2 Related Standards/Baselines

- Email Security Configuration (SPF, DKIM, DMARC)
- Approved File Sharing Platforms
- Approved Collaboration Tools
- DLP Rules and Policies
- Social Media Guidelines

64.5.3 Related Processes

- Email Encryption Process (S/MIME, PGP)
- File Sharing Approval Process
- DLP Incident Response
- External Communication (NDA Process)

64.6 6. Compliance, Monitoring and Enforcement

64.6.1 Metrics and KPIs

- Email Encryption Rate (Target: 100% for confidential emails)
- SPF/DKIM/DMARC Compliance (Target: 100%)
- DLP Incident Rate
- Number of blocked phishing emails
- File Sharing Compliance (Target: 100% approved platforms)
- Collaboration Tool Compliance
- Number of social media violations

64.6.2 Evidence and Proof

- Email Security Configuration (SPF, DKIM, DMARC)
- Email Encryption Logs
- DLP Logs and Incident Reports
- File Sharing Logs
- Collaboration Tool Configuration
- Phishing Simulation Results
- Social Media Monitoring

64.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Unencrypted Confidential Emails:** Incident response, user awareness training - **Unapproved File Sharing Tools:** Access blocked, disciplinary measures - **DLP Violations:** Incident response, investigation, disciplinary measures if applicable - **Repeated Violations:** Employment consequences, access revocation

64.7 7. Exceptions

Exceptions to this policy are only permitted in justified exceptional cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`

- **Approval:** Exceptions must be approved by CISO and Communication Security Manager
- **Documentation:** All exceptions are documented in the risk register
- **Time Limitation:** Exceptions are generally time-limited

64.8 8. References

64.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0670_Guideline_Email_Sharing_and_Collaboration_Tools.md` - Detailed Guideline
- `0280_Policy_Data_Classification_and_Information_Handling.md` - Data Classification Policy
- `0080_ISMS_Risk_Register_Template.md` - Risk Register

64.8.2 External Standards and Regulations

- **ISO/IEC 27001:2022 Annex A.5.14** - Information transfer
- **ISO/IEC 27001:2022 Annex A.8.24** - Use of cryptography
- **ISO/IEC 27001:2022 Annex A.8.26** - Application security requirements
- **NIST SP 800-177** - Trustworthy Email
- **RFC 7208** - Sender Policy Framework (SPF)
- **RFC 6376** - DomainKeys Identified Mail (DKIM)
- **RFC 7489** - Domain-based Message Authentication, Reporting, and Conformance (DMARC)

Approved by:
{{ meta.management.ceo }}, Executive Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 65

Guideline: Email, Sharing and Collaboration Tools

Document ID: 0670
Document Type: Guideline (detailed)
Related Policy: 0660_Policy_Information_Transfer_and_Communication.md
Standard Reference: ISO/IEC 27001:2022 Annex A.5.14
Owner: {{ meta.it_operations.manager }}
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}

65.1 1. Purpose and Scope

This guideline implements `0660_Policy_Information_Transfer_and_Communication.md` and defines: - Email security and usage - File sharing and collaboration tools - Secure communication channels

Scope: All communication tools at **AdminSend GmbH**

65.2 2. Email Security

65.2.1 2.1 Email System

Platform: {{ meta.email.system }} (e.g., Microsoft 365, Google Workspace)

Security Features: - SPF, DKIM, DMARC configured - TLS for transport encryption - Anti-spam and anti-malware - DLP (Data Loss Prevention) - Email archiving

65.2.2 2.2 Email Usage

Permitted Use: - Business communication - Limited private use (max. 10 emails/day) - Registration for business online services

Prohibited Activities: - Sending confidential data without encryption - Spam, chain emails - Using private email for business purposes - Automatic forwarding to external addresses

Details: See `0210_Guideline_Acceptable_Use_of_IT.md`

65.2.3 2.3 Email Encryption

S/MIME: - Mandatory for confidential emails - Certificates for all employees - Automatic encryption with "Confidential" label

Opportunistic TLS: - For all outgoing emails - MTA-STS for known partners

Details: See `0270_Guideline_Key_Management_and_Encryption.md`

65.2.4 2.4 Phishing Protection

Technical Controls: - Email gateway with anti-phishing - Link rewriting and sandbox - Attachment scanning - DMARC enforcement

User Training: - Phishing awareness training (annually) - Phishing simulations (quarterly) - Reporting button in email client

Upon Phishing Suspicion: 1. Do not open/click email 2. Report via reporting button 3. Delete email 4. IT Security reviews and responds

65.2.5 2.5 Email Archiving

Automatic Archiving: - All business emails - Retention: {{ meta.retention.email_years }} years - Immutability (WORM)

Access: - Users: Own emails - Legal/Compliance: For eDiscovery - Supervisors: With approval

Details: See `0590_Guideline_Records_Retention`

65.3 3. File Sharing

65.3.1 3.1 Approved Platforms

Internal: - **File Server:** {{ netbox.device.fileserver }} - **SharePoint/OneDrive:** {{ meta.collaboration.sharepoint }} - **Teams/Slack:** {{ meta.collaboration.teams }}

External (with customers/partners): - **Secure File Transfer:** {{ meta.filesharing.secure_platform }} - **Only with encryption and password protection**

Prohibited: - Private cloud services (private Dropbox, private Google Drive) - WeTransfer, Filemail (without approval) - USB drives for confidential data

65.3.2 3.2 Permissions

Least Privilege: - Only required permissions - Read-only where possible - Time-limited shares

External Shares: - Approval by data owner - Password protection mandatory - Set expiration date (max. 90 days) - Logging of all access

65.3.3 3.3 DLP for File Sharing

Automatic Controls: - Blocking confidential data on external shares - Warning for large data volumes - Alerts for unusual sharing patterns

65.4 4. Collaboration Tools

65.4.1 4.1 Microsoft Teams / Slack

Approved Use: - Internal communication - Project collaboration - Video conferences

Security Settings: - External guests only with approval - DLP policies activated - Retention policies configured - Audit logging activated

Prohibited Activities: - Sharing confidential data in public channels - Using private accounts for business purposes - Installing unapproved apps/bots

65.4.2 4.2 Video Conferences

Approved Platforms: - **Internal:** {{ meta.collaboration.video }} (e.g., Teams, Zoom) - **External:** Only approved platforms

Security Settings: - Waiting room activated - Password protection for meetings - No recording without consent - Screen sharing only for moderator

Best Practices: - Use background blur - Mute microphone when not speaking - No confidential information in public meetings

65.4.3 4.3 Instant Messaging

Approved Tools: - Microsoft Teams Chat - Slack (Enterprise)

Prohibited: - WhatsApp, Telegram for business communication - Private messaging apps

Retention: - Chat history: {{ meta.retention.chat_years }} years - Compliance archiving

65.5 5. External Communication

65.5.1 5.1 Communication with Customers

Channels: - Email (preferred) - Phone - Video conference - Customer portal (if available)

Confidential Information: - Encryption mandatory - Use secure file transfer - No confidential data via SMS/WhatsApp

65.5.2 5.2 Communication with Suppliers

Requirements: - NDA before exchanging confidential information - Approved communication channels - Documentation of important communication

65.5.3 5.3 Social Media

Business Use: - Only authorized accounts - Follow social media guidelines - No confidential information

Private Use: - No impersonation of official company opinion - Disclaimer for opinions - No negative statements about company

Details: See `0210_Guideline_Acceptable_Use_of_IT.md`

65.6 6. Mobile Communication

65.6.1 6.1 Business Smartphones

Configuration: - MDM enrollment mandatory - Encryption enabled - Remote wipe capability - Approved apps only

Usage: - Business emails and calendar - Teams/Slack - Business calls

65.6.2 6.2 BYOD

Requirements: - Containerization (work profile) - Separate apps for business/private - MDM enrollment

Details: See `0510_Guideline_MDM_BringYourOwnDevice`

65.7 7. Data Loss Prevention (DLP)

65.7.1 7.1 DLP Policies

For Email: - Blocking credit card numbers - Warning for "Confidential" label external - Blocking large attachments (> 25 MB)

For File Sharing: - Blocking confidential data on external shares - Warning for sharing with many people

For Collaboration Tools: - Warning for posting confidential data in public channels

65.7.2 7.2 DLP Incidents

Upon DLP Blocking: 1. User receives warning 2. Incident ticket created 3. Security team reviews 4. If needed: Training or disciplinary measures

65.8 8. Compliance and Audit

65.8.1 8.1 Metrics (KPIs)

Metric	Target Value
Email Encryption (confidential)	100%
Phishing Click Rate (simulation)	< 5%
DLP Incidents	< 10 per month

Metric	Target Value
External Shares with Password	100%

65.8.2 8.2 Audit Evidence

- Email Archive
- File Sharing Logs
- DLP Incident Reports
- Phishing Simulation Results

65.9 9. References

65.9.1 Internal Documents

- `0660_Policy_Information_Transfer_and_Communication.md`
- `0210_Guideline_Acceptable_Use_of_IT.md`
- `0270_Guideline_Key_Management_and_Encryption.md`

65.9.2 External Standards

- **ISO/IEC 27001:2022 Annex A.5.14** - Information transfer
- **NIST SP 800-177** - Trustworthy Email

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 66

Policy: Security in Projects

Document ID: 0680
Document Type: Policy (abstract)
Standard Reference: ISO/IEC 27001:2022 Annex A.5.8, A.8.25, A.8.32 (incl. Amendment 1:2024)
Owner: Thomas Weber
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}
Next Review: {{ meta.document.next_review }}

66.1 1. Purpose

This policy defines the requirements for integrating information security into projects of **AdminSend GmbH**. It ensures that security requirements are considered throughout the entire project lifecycle.

66.2 2. Scope

This policy applies to:

- **Organizational Units:** All departments and locations of AdminSend GmbH
- **Projects:** All IT projects, infrastructure projects, software development projects
- **Project Phases:** Initiation, planning, implementation, closure
- **Project Types:** Internal projects, external projects, partner projects
- **Locations:** {{ netbox.site.name }} and all other operational sites

Exceptions: Exceptions are only permitted through the defined exception process (`0640_Policy_Exceptions_and`

66.3 3. Policy Statements

66.3.1 3.1 Security by Design

Security is integrated into projects from the beginning (security by design). Security requirements are defined during project initiation.

66.3.2 3.2 Security Requirements

Security requirements are defined for each project: - Confidentiality, integrity, availability - Compliance requirements - Data protection requirements - Technical security requirements

66.3.3 3.3 Security Risk Assessment

A security risk assessment is conducted for each project. Risks are identified, evaluated, and treated.

66.3.4 3.4 Security Architecture Review

Project architectures are reviewed for security. Security architecture review occurs before implementation.

66.3.5 3.5 Security Testing

Projects are tested for security: - Security testing (penetration tests, vulnerability scans) - Code reviews (SAST, DAST) for software projects - Configuration reviews for infrastructure projects

66.3.6 3.6 Security Sign-Off

Projects receive security sign-off before go-live. Security sign-off confirms that security requirements are met.

66.3.7 3.7 Change Management Integration

Security-relevant changes follow the change management process (see `0360_Policy_Change_and_Release_Managem`

66.3.8 3.8 Third-Party Security

For projects with third parties (suppliers, partners), security requirements are contractually agreed (see `0460_Policy_Supplier_and_Cloud_Security.md`).

66.3.9 3.9 Security Documentation

Security-relevant project documentation is created: - Security Requirements Specification - Security Architecture Document - Security Test Report - Security Sign-Off Document

66.4 4. Roles and Responsibilities

66.4.1 RACI Matrix: Security in Projects

Activity	CISO	Project Manager	Security Architect	IT Operations	Business Owner
Policy Creation	R/A	C	R	C	C
Security Requirements	R	R/A	R	C	R
Security Risk Assessment	R/A	R	R	C	C
Security Architecture Review	R/A	C	R/A	C	C
Security Testing	R	R/A	R	R	C
Security Sign-Off	R/A	C	C	C	C
Change Management	C	R	C	R/A	C
Third-Party Security	R/A	R	C	C	R

Legend: R = Responsible (Execution), A = Accountable (Ownership), C = Consulted, I = Informed

66.4.2 Key Roles

- **Policy Owner:** Thomas Weber (CISO)
- **Security Architect:** {{ meta.security.architect }}
- **Project Manager:** Project responsible persons
- **IT Operations Manager:** {{ meta.it.operations_manager }}
- **Business Owner:** Department responsible persons
- **Control/Audit Function:** ISMS, Internal Audit

66.5 5. Derived Documents (Guidelines/Standards/Processes)

Implementation details are defined in subordinate documents:

66.5.1 Related Guidelines

- **0690_Guideline_Security_Requirements_in_Project_Lifecycle.md** - Detailed implementation guideline
- `0380_Policy_Secure_Development.md` - Secure Development Policy
- `0360_Policy_Change_and_Release_Management.md` - Change Management Policy
- `0460_Policy_Supplier_and_Cloud_Security.md` - Supplier Security Policy

66.5.2 Related Standards/Baselines

- Security Requirements Template
- Security Risk Assessment Template
- Security Architecture Review Checklist
- Security Testing Standards
- Security Sign-Off Template

66.5.3 Related Processes

- Project Security Review Process
- Security Risk Assessment Process
- Security Architecture Review Process
- Security Testing Process
- Security Sign-Off Process

66.6 6. Compliance, Monitoring and Enforcement

66.6.1 Metrics and KPIs

- Number of projects with security requirements (Target: 100%)
- Number of security risk assessments conducted (Target: 100% of all projects)
- Number of security architecture reviews (Target: 100% of critical projects)
- Number of security tests (Target: 100% before go-live)
- Number of security sign-offs (Target: 100% before go-live)
- Average time for security review (Target: < 5 days)
- Number of projects without security sign-off (Target: 0)

66.6.2 Evidence and Proof

- Security Requirements Specifications
- Security Risk Assessments
- Security Architecture Review Reports
- Security Test Reports (Penetration Tests, Vulnerability Scans)
- Security Sign-Off Documents
- Project Security Checklists
- Change Management Records

66.6.3 Consequences of Violations

Violations of this policy are handled according to applicable HR and compliance processes: - **Projects Without Security Requirements:** Project stop until requirements defined - **Missing Security Risk Assessments:** Remediation before continuation - **Go-Live Without Security Sign-Off:** Project stop, escalation to management - **Repeated Violations:** Employment consequences, project responsibility removed

66.7 7. Exceptions

Exceptions to this policy are only permitted in justified exceptional cases:

- **Exception Process:** See `0640_Policy_Exceptions_and_Risk_Waivers.md`
- **Approval:** Exceptions must be approved by CISO and CIO
- **Documentation:** All exceptions are documented in the risk register
- **Time Limitation:** Exceptions are generally time-limited

66.8 8. References

66.8.1 Internal Documents

- `0010_ISMS_Information_Security_Policy.md` - ISMS Policy
- `0690_Guideline_Security_Requirements_in_Project_Lifecycle.md` - Detailed Guideline
- `0380_Policy_Secure_Development.md` - Secure Development Policy
- `0080_ISMS_Risk_Register_Template.md` - Risk Register

66.8.2 External Standards and Regulations

- **ISO/IEC 27001:2022 Annex A.5.8** - Information security in project management
- **ISO/IEC 27001:2022 Annex A.8.25** - Secure development life cycle
- **ISO/IEC 27001:2022 Annex A.8.32** - Change management
- **NIST SP 800-64** - Security Considerations in the System Development Life Cycle
- **OWASP SAMM** - Software Assurance Maturity Model
- **BSIMM** - Building Security In Maturity Model
- **ISO/IEC 27034** - Application Security

Approved by:
{{ meta.management.ceo }}, Executive Management
Date: {{ meta.document.approval_date }}

Next Review: {{ meta.document.next_review }} (annually or as needed)

ewpage

Chapter 67

Guideline: Security Requirements in Project Lifecycle

Document ID: 0690
Document Type: Guideline (detailed)
Related Policy: 0680_Policy_Security_in_Projects.md
Standard Reference: ISO/IEC 27001:2022 Annex A.5.8
Owner: {{ meta.pmo.manager }}
Version: 1.0
Status: Approved
Classification: Internal
Last Updated: {{ meta.document.date }}

67.1 1. Purpose and Scope

This guideline implements `0680_Policy_Security_in_Projects.md` and defines: - Security requirements in all project phases - Security reviews and gateways - Security-by-design principles

Scope: All IT projects at **AdminSend GmbH**

67.2 2. Project Classification

67.2.1 2.1 Project Categories

Category A (Critical): - New systems with confidential data - Internet-facing applications - Critical infrastructure - **Security Involvement:** Comprehensive

Category B (High): - Internal applications with sensitive data - Changes to critical systems - **Security Involvement:** Detailed

Category C (Standard): - Standard IT projects - Infrastructure upgrades - **Security Involvement:** Standard

Category D (Low): - Small changes - Non-critical systems - **Security Involvement:** Minimal

67.2.2 2.2 Classification Criteria

Assessment: - Data classification (Confidential/Highly Confidential = higher category) - Internet exposure (Yes = higher category) - Number of users (> 100 = higher category) - Compliance requirements (GDPR, PCI-DSS = higher category)

67.3 3. Project Phases and Security Activities

67.3.1 3.1 Initiation

Security Activities: - Project classification - Identify security stakeholders - Initial security budget

Deliverables: - Project classification - Security contact person

Security Gateway: None (Informational)

67.3.2 3.2 Planning

Security Activities: - Define security requirements - Threat modeling (Category A/B) - Data Protection Impact Assessment (DPIA) if needed - Security architecture review - Security testing plan

Deliverables: - Security Requirements Document - Threat Model (Category A/B) - DPIA (if required) - Security Test Plan

Security Gateway 1: - **Category A/B:** Mandatory - **Approver:** CISO or Security Architect - **Criteria:** Security requirements complete, threat model acceptable

67.3.3 3.3 Design

Security Activities: - Security architecture review - Apply secure design patterns - Authentication/authorization design - Encryption design - Logging/monitoring design

Deliverables: - Security Architecture Document - Data Flow Diagrams - Authentication/Authorization Design

Security Gateway 2: - **Category A:** Mandatory - **Approver:** CISO and Security Architect - **Criteria:** Security architecture acceptable, no critical vulnerabilities in design

67.3.4 3.4 Development/Procurement

Security Activities (Development): - Follow secure coding standards - Code reviews (incl. security review) - SAST (Static Application Security Testing) - Dependency scanning - Secrets management

Security Activities (Procurement): - Vendor security assessment - Contract review (security clauses) - Data Processing Agreement (DPA) if needed

Deliverables: - Code review reports - SAST reports - Vendor assessment (for procurement)

Details: See `0390_Guideline_Secure_SDLC` and `0470_Guideline_Third_Party_Risk_Assessment`

67.3.5 3.5 Testing

Security Testing: - DAST (Dynamic Application Security Testing) - Penetration testing (Category A/B) - Security test cases - Vulnerability scanning

Deliverables: - DAST reports - Penetration test report (Category A/B) - Security test results

Security Gateway 3: - **Category A/B:** Mandatory - **Approver:** CISO - **Criteria:** No critical/high vulnerabilities, all security tests passed

67.3.6 3.6 Deployment

Security Activities: - Security configuration review - Hardening according to baseline - Configure firewall rules - Set up monitoring/alerting - Configure backup

Deliverables: - Security Configuration Checklist - Firewall Rules Documentation - Monitoring Setup Documentation

Security Gateway 4 (Go-Live): - **Category A/B:** Mandatory - **Approver:** CISO - **Criteria:** Security configuration correct, monitoring active, no open critical findings

67.3.7 3.7 Operations and Maintenance

Security Activities: - Regular vulnerability scans - Patch management - Security incident monitoring - Annual security review (Category A)

Deliverables: - Vulnerability scan reports - Patch compliance reports - Incident reports

67.3.8 3.8 Decommissioning

Security Activities: - Data backup (if required) - Secure data deletion - Revoke access - Remove firewall rules - Archive documentation

Deliverables: - Deletion log - Decommissioning checklist

67.4 4. Security-by-Design Principles

67.4.1 4.1 Least Privilege

Principle: Minimum required permissions

Implementation: - Role-based access control (RBAC) - No default admin accounts - Just-in-Time (JIT) access for privileged operations

67.4.2 4.2 Defense in Depth

Principle: Multiple security layers

Implementation: - Network segmentation - Firewall + IDS/IPS - Endpoint protection + EDR - Application security + WAF

67.4.3 4.3 Fail Secure

Principle: Fail to secure state

Implementation: - Default deny (firewall, access control) - Errors lead to access denial (not access) - Graceful degradation

67.4.4 4.4 Privacy by Design

Principle: Data protection from the beginning

Implementation: - Data minimization - Purpose limitation - Encryption - Anonymization/pseudonymization

Details: See `0570_Guideline_Data_Protection_Requirements`

67.5 5. Security Requirements

67.5.1 5.1 Functional Security Requirements

Authentication: - Multi-factor authentication (MFA) for external access - Strong passwords or certificates - Session management

Authorization: - Role-based access control (RBAC) - Least privilege - Segregation of duties

Encryption: - TLS 1.2+ for data transmission - AES-256 for data at rest - Secure key management

Logging: - Authentication events - Access to confidential data - Administrative actions - Errors and exceptions

67.5.2 5.2 Non-Functional Security Requirements

Performance: - Security controls must not significantly impact performance ($< 10\%$)

Availability: - Security controls highly available - Failover mechanisms

Maintainability: - Security configuration documented - Automated security tests

67.6 6. Threat Modeling

67.6.1 6.1 Methodology

STRIDE: - **S**poofing (identity spoofing) - **T**ampering (manipulation) - **R**epudiation (deniability) - **I**nformation Disclosure (information disclosure) - **D**enial of Service (denial of service) - **E**levation of Privilege (privilege escalation)

67.6.2 6.2 Process

Steps: 1. Document system architecture (data flow diagrams) 2. Identify threats (STRIDE) 3. Assess threats (risk) 4. Define mitigation measures 5. Documentation

Tool: {{ meta.security.threat_modeling_tool }} (e.g., Microsoft Threat Modeling Tool)

67.7 7. Security Testing

67.7.1 7.1 Test Types

SAST (Static Application Security Testing): - During development - Automated in CI/CD - Focus: Code vulnerabilities

DAST (Dynamic Application Security Testing): - During testing phase - Automated or manual - Focus: Runtime vulnerabilities

Penetration Testing: - Before go-live (Category A/B) - Manual by experts - Focus: Realistic attack scenarios

Details: See `0390_Guideline_Secure_SDLC`

67.7.2 7.2 Remediation

Process: 1. Prioritize findings (by CVSS) 2. Create remediation plan 3. Implement fixes 4. Re-test 5. Documentation

SLA: - Critical: Before go-live - High: Before go-live or with compensating controls - Medium: Within 30 days after go-live - Low: Within 90 days after go-live

67.8 8. Compliance and Audit

67.8.1 8.1 Metrics (KPIs)

Metric	Target Value
Security Gateway Compliance (Category A/B)	100%
Penetration Test Before Go-Live (Category A/B)	100%
Critical Findings Before Go-Live	0
Security Requirements Completeness	100%

67.8.2 8.2 Audit Evidence

- Security Requirements Documents
- Threat Models
- Security Test Reports
- Security Gateway Approvals
- DPIA (if required)

67.9 9. References

67.9.1 Internal Documents

- `0680_Policy_Security_in_Projects.md`
- `0390_Guideline_Secure_SDLC_Coding_Review_and_Secrets.md`
- `0470_Guideline_Third_Party_Risk_Assessment_and_Cloud_Controls.md`
- `0570_Guideline_Data_Protection_Requirements_and_Data_Processing.md`

67.9.2 External Standards

- **ISO/IEC 27001:2022 Annex A.5.8** - Information security in project management
- **NIST SP 800-64** - Security Considerations in the System Development Life Cycle
- **OWASP SAMM** - Software Assurance Maturity Model

Approved by: Thomas Weber, CISO
Next Review: {{ meta.document.next_review }}

ewpage

Chapter 68

Appendix A: Annex A Control Mapping

Document Type: Appendix
Version: 1.0.0
Date: {{ meta.document.date }}
Classification: internal

68.1 Purpose

This document provides the complete mapping of ISO/IEC 27001:2022 Annex A controls to the implemented policies and guidelines of the ISMS. It serves as a central reference for compliance evidence and demonstrates how each Annex A control is implemented in the organization.

The mapping considers the changes from Amendment 1:2024 and ensures that all 93 controls of the current Annex A version are covered.

68.2 Scope

Organization: AdminSend GmbH
ISMS Scope: {{ meta.isms.scope }}
Responsible: Thomas Weber (thomas.weber@adminsend.de)

68.3 ISO/IEC 27001:2022 Annex A Structure

The Annex A controls are organized into four main categories:

- **Organizational Controls (5.1-5.37):** 37 controls
- **People Controls (6.1-6.8):** 8 controls
- **Physical Controls (7.1-7.14):** 14 controls
- **Technological Controls (8.1-8.34):** 34 controls

Total: 93 controls

68.4 Annex A Control Mapping

68.4.1 5. Organizational Controls

68.4.1.1 5.1 Policies for Information Security

Control Statement: Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Implementation Status: Implemented
Implementation in ISMS: - Policy: 0010_ISMS_Information_Security_Policy.md - Policy: 0200-0680 (All Topic-Specific Policies) - Process: 0050_ISMS_Document_Control.md

Responsible: Thomas Weber
Evidence: Approved and published policies, training records

---

ewpage

Chapter 69

Appendix B: Asset and System Inventory

Document Type: Appendix
Version: 1.0.0
Date: {{ meta.document.date }}
Classification: internal

69.1 Purpose

This document represents the central asset and system inventory of the organization. It fulfills the requirements of ISO/IEC 27001:2022 Annex A 5.9 (Inventory of Information and Other Associated Assets) and serves as the foundation for:

- Asset management and lifecycle management
- Risk assessment and protection needs determination
- Incident response and business continuity planning
- Compliance evidence and audits

The inventory is continuously maintained and reviewed at least quarterly.

69.2 Scope

Organization: AdminSend GmbH
ISMS Scope: {{ meta.isms.scope }}
Responsible: Asset Management Team, Thomas Weber

69.3 Asset Categories

The inventory includes the following asset categories:

1. **Hardware Assets:** Servers, network devices, endpoints, storage
2. **Software Assets:** Operating systems, applications, licenses
3. **Data Assets:** Databases, file systems, repositories
4. **Network Assets:** VLANs, subnets, connections
5. **Cloud Assets:** Cloud services, SaaS applications
6. **Physical Assets:** Rooms, infrastructure, documentation

69.4 Asset Classification

Each asset is classified according to the following criteria:

69.4.1 Protection Requirements (Confidentiality, Integrity, Availability)

Level	Description	Example
High	Critical for business operations, high damage if compromised	Production databases, core banking systems
Medium	Important for business operations, medium damage if compromised	Internal applications, development systems
Low	Non-critical, low damage if compromised	Test systems, public information

69.4.2 Criticality

Level	RTO	RPO	Description
Tier 1	< 4h	< 1h	Business-critical, immediate recovery required
Tier 2	< 24h	< 4h	Important, recovery within one business day
Tier 3	< 72h	< 24h	Standard, recovery within 3 days
Tier 4	> 72h	> 24h	Non-critical, no time-critical recovery

69.5 Hardware Assets

69.5.1 Servers

Asset-ID	Hostname	Type	Location	Owner	Protection Req (C/I/A)	Criticality	Status
SRV-001	{{ net-box.device.primary_ip4 }}	Physical Server	{{ net-box.site.name }}	IT Operations	High/High/High	Tier 1	Production

Asset-ID	Hostname	Type	Location	Owner	Protection Req (C/I/A)	Criticality	Status
SRV-002	{{ net-box.device.name | default('') }}	Physical Server	{{ net-box.site.name | default('') }}	IT Operations	High/High/Medium	Tier 2	Production
[TODO]	[TODO: Hostname]	[TODO: Type]	[TODO: Location]	[TODO: Owner]	[TODO: C/I/A]	[TODO: Tier]	[TODO: Status]

Note: Import complete server list from NetBox/CMDB.

69.5.2 Network Devices

Asset-ID	Hostname	Type	Location	Owner	Protection Req (C/I/A)	Criticality	Status
NET-001	{{ net-box.device.name | default('') }}	Core Switch	{{ net-box.site.name | default('') }}	Network Team	Medium/High/High	Tier 1	Production
NET-002	{{ net-box.device.name | default('') }}	Firewall	{{ net-box.site.name | default('') }}	Security Team	High/High/High	Tier 1	Production
[TODO]	[TODO: Hostname]	[TODO: Type]	[TODO: Location]	[TODO: Owner]	[TODO: C/I/A]	[TODO: Tier]	[TODO: Status]

Note: Import complete network device list from NetBox.

69.5.3 Endpoints

Asset-ID	Hostname	Type	User	Owner	Protection Req (C/I/A)	Status
WS-001	{{ meta.ciso.workstation }}	Laptop	Thomas Weber	IT Operations	High/Medium/Medium	Production
[TODO]	[TODO: Hostname]	[TODO: Type]	[TODO: User]	[TODO: Owner]	[TODO: C/I/A]	[TODO: Status]

Note: Import endpoint inventory from MDM/Endpoint Management System.

69.5.4 Storage Systems

Asset-ID	Name	Type	Capacity	Location	Owner	Protection Req (C/I/A)	Criticality
STO-001	{{ netbox.device.storage }}	SAN	[TODO: Capacity]	{{ netbox.site.name }}	IT Operations	High/High/High	Tier 1
[TODO]	[TODO: Name]	[TODO: Type]	[TODO: Capacity]	[TODO: Location]	[TODO: Owner]	[TODO: C/I/A]	[TODO: Tier]

69.6 Software Assets

69.6.1 Operating Systems

Asset-ID	Name	Version	License Type	License Count	Owner	Criticality
OS-001	Windows Server	2022	Volume License	[TODO: Count]	IT Operations	Tier 1
OS-002	Red Hat Enterprise Linux	9.x	Subscription	[TODO: Count]	IT Operations	Tier 1
OS-003	Ubuntu Server	22.04 LTS	Open Source	Unlimited	IT Operations	Tier 2
[TODO]	[TODO: Name]	[TODO: Version]	[TODO: License Type]	[TODO: Count]	[TODO: Owner]	[TODO: Tier]

69.6.2 Business Applications

Asset-ID	Name	Version	Vendor	License Type	Owner	Protection Req (C/I/A)	Criticality
APP-001	[TODO: ERP System]	[TODO: Version]	[TODO: Vendor]	[TODO: License Type]	Business Owner	High/High/High	Tier 1
APP-002	[TODO: CRM System]	[TODO: Version]	[TODO: Vendor]	[TODO: License Type]	Sales	High/Medium/Medium	Tier 2

Asset-ID	Name	Version	Vendor	License Type	Owner	Protection Req (C/I/A)	Criticality
[TODO]	[TODO: Name]	[TODO: Version]	[TODO: Vendor]	[TODO: License Type]	[TODO: Owner]	[TODO: C/I/A]	[TODO: Tier]

69.6.3 Security Software

Asset-ID	Name	Version	Type	Coverage	Owner	Criticality
SEC-001	[TODO: EDR Solution]	[TODO: Version]	Endpoint Detection & Response	All Endpoints	Security Team	Tier 1
SEC-002	[TODO: SIEM]	[TODO: Version]	Security Information & Event Management	All Systems	Security Team	Tier 1
SEC-003	[TODO: Firewall]	[TODO: Version]	Next-Gen Firewall	Perimeter	Security Team	Tier 1
[TODO]	[TODO: Name]	[TODO: Version]	[TODO: Type]	[TODO: Coverage]	[TODO: Owner]	[TODO: Tier]

69.7 Data Assets

69.7.1 Databases

Asset-ID	Name	Type	Version	Server	Owner	Protection Req (C/I/A)	Criticality	Backup
DB-001	[TODO: Production DB]	[TODO: PostgreSQL/MySQL/Oracle]	[TODO: Version]	SRV-001	DBA Team	High/High/High	Tier 1	Daily
DB-002	[TODO: Test DB]	[TODO: Type]	[TODO: Version]	[TODO: Server]	DBA Team	Low/Medium/Low	Tier 3	Weekly

Asset-ID	Name	Type	Version	Server	Owner	Protection Req (C/I/A)	Criticality	Backup
[TODO]	[TODO: Name]	[TODO: Type]	[TODO: Version]	[TODO: Server]	[TODO: Owner]	[TODO: C/I/A]	[TODO: Tier]	[TODO: Backup]

69.7.2 File Systems and Shares

Asset-ID	Name	Type	Path	Server	Owner	Protection Req (C/I/A)	Backup
FS-001	[TODO: Department Share]	SMB Share	[TODO: Path]	[TODO: Server]	IT Operations	Medium/Medium/Medium	Daily
FS-002	[TODO: Project Share]	SMB Share	[TODO: Path]	[TODO: Server]	Project Management	High/Medium/Medium	Daily
[TODO]	[TODO: Name]	[TODO: Type]	[TODO: Path]	[TODO: Server]	[TODO: Owner]	[TODO: C/I/A]	[TODO: Backup]

69.7.3 Code Repositories

Asset-ID	Name	Type	URL	Owner	Protection Req (C/I/A)	Backup
REPO-001	[TODO: Main Repository]	Git	[TODO: URL]	Development Team	High/High/Medium	Daily
[TODO]	[TODO: Name]	[TODO: Type]	[TODO: URL]	[TODO: Owner]	[TODO: C/I/A]	[TODO: Backup]

69.8 Network Assets

69.8.1 VLANs

VLAN-ID	Name	Subnet	Purpose	Security Zone	Owner
{{ net-box.vlan.management.vid }}	{{ net-box.vlan.management.name }}	{{ net-box.management.subnet }}	Management	Restricted	Network Team
{{ net-box.vlan.production.vid }}	{{ net-box.vlan.production.name }}	{{ net-box.production.subnet }}	Production	Internal	Network Team
[TODO]	[TODO: Name]	[TODO: Subnet]	[TODO: Purpose]	[TODO: Zone]	[TODO: Owner]

Note: Import complete VLAN list from NetBox.

69.8.2 External Connections

Connection-ID	Type	Provider	Bandwidth	Purpose	Owner	Criticality
WAN-001	Internet	[TODO: Provider]	[TODO: Bandwidth]	Internet Access	Network Team	Tier 1
WAN-002	MPLS	[TODO: Provider]	[TODO: Bandwidth]	Site-to-Site	Network Team	Tier 1
[TODO]	[TODO: Type]	[TODO: Provider]	[TODO: Bandwidth]	[TODO: Purpose]	[TODO: Owner]	[TODO: Tier]

69.9 Cloud Assets

69.9.1 Cloud Services (IaaS/PaaS)

Asset-ID	Service Name	Provider	Type	Region	Owner	Protection Req (C/I/A)	Criticality
CLOUD-001	[TODO: VM Instances]	[TODO: AWS/Azure/GCP]	IaaS	[TODO: Region]	Cloud Team	High/High/High	Tier 1
CLOUD-002	[TODO: Database Service]	[TODO: Provider]	PaaS	[TODO: Region]	DBA Team	High/High/High	Tier 1
[TODO]	[TODO: Service]	[TODO: Provider]	[TODO: Type]	[TODO: Region]	[TODO: Owner]	[TODO: C/I/A]	[TODO: Tier]

69.9.2 SaaS Applications

Asset-ID	Service Name	Provider	Purpose	User Count	Owner	Protection Req (C/I/A)
SAAS-001	Microsoft 365	Microsoft	Productivity	[TODO: Count]	IT Operations	High/Medium/High
SAAS-002	[TODO: CRM SaaS]	[TODO: Provider]	Customer Management	[TODO: Count]	Sales	High/Medium/Medium
[TODO]	[TODO: Service]	[TODO: Provider]	[TODO: Purpose]	[TODO: Count]	[TODO: Owner]	[TODO: C/I/A]

69.10 Physical Assets

69.10.1 Sites and Rooms

Site-ID	Name	Address	Type	Security Level	Owner
SITE-001	{{ netbox.site.name }}	{{ netbox.site.address }}	Main Site	High	Facility Management
SITE-002	[TODO: Branch Office]	[TODO: Address]	Branch Office	Medium	Facility Management
[TODO]	[TODO: Name]	[TODO: Address]	[TODO: Type]	[TODO: Security]	[TODO: Owner]

69.10.2 Server Rooms and Data Centers

Room-ID	Name	Site	Type	Size	Air Conditioning	Fire Suppression	Access Control
ROOM-001	Server Room 1	SITE-001	Server Room	[TODO: m^2]	Redundant	FM-200	Biometric
[TODO]	[TODO: Name]	[TODO: Site]	[TODO: Type]	[TODO: Size]	[TODO: AC]	[TODO: Fire]	[TODO: Access]

69.10.3 Critical Infrastructure

Asset-ID	Name	Type	Site	Capacity	Redundancy	Owner	Criticality
INFRA-001	UPS System 1	UPS	SITE-001	[TODO: kVA]	N+1	Facility Management	Tier 1
INFRA-002	AC Unit 1	Air Conditioning	SITE-001	[TODO: kW]	N+1	Facility Management	Tier 1
INFRA-003	Emergency Generator	Generator	SITE-001	[TODO: kW]	N	Facility Management	Tier 1
[TODO]	[TODO: Name]	[TODO: Type]	[TODO: Site]	[TODO: Capacity]	[TODO: Redundancy]	[TODO: Owner]	[TODO: Tier]

69.11 Asset Lifecycle Management

69.11.1 Lifecycle Phases

Phase	Description	Responsible	Process
Planning	Requirements determination, budgeting	Business Owner	Requirements Management
Procurement	Selection, ordering, delivery	Procurement	Procurement Process
Deployment	Installation, configuration, testing	IT Operations	Change Management
Operation	Usage, maintenance, monitoring	IT Operations	Operations Processes
Maintenance	Updates, patches, repairs	IT Operations	Patch Management
Decommissioning	Decommissioning, data deletion	IT Operations	Decommissioning Process
Disposal	Secure disposal or reuse	IT Operations	Disposal Process

---

69.11.2 Asset Owners and Responsibilities

Role	Responsibilities	Contact
Asset Owner	Business responsibility, approvals, budget	[TODO: Name/Department]

Role	Responsibilities	Contact
Technical Owner	Technical responsibility, operations, maintenance	IT Operations
Security Owner	Security requirements, risk assessment	Thomas Weber
Data Owner	Data classification, access control	[TODO: Name/Department]

69.12 Asset Tagging and Labeling

69.12.1 Tagging Schema

All assets are tagged with the following tags:

Tag Category	Description	Example
Environment	Environment	Production, Development, Test, QA
Criticality	Criticality	Tier1, Tier2, Tier3, Tier4
Owner	Responsible	IT-Ops, Security, Development
CostCenter	Cost Center	[TODO: Cost Centers]
Project	Project	[TODO: Project Name]
Compliance	Compliance Requirements	PCI-DSS, GDPR, ISO27001

Note: Tagging is maintained in CMDB/Asset Management System.

69.13 Inventory Process

69.13.1 Regular Review

Activity	Frequency	Responsible	Documentation
Complete Inventory	Annually	Asset Management Team	Inventory Report
Quarterly Review	Quarterly	Asset Owners	Review Protocol
Automatic Discovery	Daily	IT Operations	Discovery Logs
Change Tracking	Continuous	Change Management	Change Records

69.13.2 Discovery Tools

Tool	Purpose	Coverage	Owner
NetBox	Network and Infrastructure Inventory	Network Devices, Servers, VLANs	Network Team
CMDB	Configuration Management Database	All IT Assets	IT Operations
MDM	Mobile Device Management	Endpoints, Mobile Devices	IT Operations
Cloud Asset Inventory	Cloud Resources	Cloud Services	Cloud Team
[TODO: Tool]	[TODO: Purpose]	[TODO: Coverage]	[TODO: Owner]

69.14 Compliance and Audit

69.14.1 Audit Requirements

This inventory fulfills the following compliance requirements:

- **ISO/IEC 27001:2022 Annex A 5.9:** Inventory of Information and Other Associated Assets
- **ISO/IEC 27001:2022 Annex A 5.10:** Acceptable Use of Information and Other Associated Assets
- **ISO/IEC 27001:2022 Annex A 8.9:** Configuration Management
- **[TODO: Additional Compliance Requirements]**

69.14.2 Audit Trail

Date	Change	Performed By	Approved By	Reason
{{ meta.document.creation }}	Initial creation	{{ meta.document.author }}	Thomas Weber	ISMS Implementation
[TODO: Date]	[TODO: Change]	[TODO: Name]	[TODO: Name]	[TODO: Reason]

69.15 References

- Policy: 0300_Policy_Asset_Management.md
- Guideline: 0310_Guideline_Asset_Inventory_Tagging_and_Disposal.md
- Document: 0100_ISMS_Statement_of_Applicability_SoA_Template.md
- Appendix: 0730_Appendix_Data_Flow_and_Interfaces_Template.md

---

Document Owner: Asset Management Team
Approved By: Thomas Weber
Next Review: Quarterly

ewpage

Chapter 70

Appendix C: Data Flow and Interfaces

Document Type: Appendix
Version: 1.0.0
Date: {{ meta.document.date }}
Classification: internal

70.1 Purpose

This document documents all data flows and interfaces within the organization as well as to external partners and service providers. It fulfills the requirements of:

- ISO/IEC 27001:2022 Annex A 5.14 (Information Transfer)
- ISO/IEC 27001:2022 Annex A 5.19-5.23 (Supplier Relationships)
- ISO/IEC 27001:2022 Annex A 8.20-8.22 (Network Security)

The documentation serves as the foundation for:

- Risk assessment of data transfers
- Security requirements for interfaces
- Data Protection Impact Assessments (DPIA)
- Incident response and forensics

70.2 Scope

Organization: AdminSend GmbH
ISMS Scope: {{ meta.isms.scope }}
Responsible: Thomas Weber, Data Protection Officer

70.3 Data Flow Categories

70.3.1 Internal Data Flows

Data transfers within the organization between different systems and sites.

70.3.2 External Data Flows

Data transfers between the organization and external partners, customers, suppliers, or cloud services.

70.3.3 Cross-Border Data Flows

Data transfers across country borders that must meet special data protection requirements (GDPR Art. 44-50).

70.4 Data Classification

All data flows are assessed according to the following classifications:

Classification	Description	Examples	Protection Measures
Public	Intended for public	Marketing materials, public website	No special measures
Internal	For internal use only	Internal documents, operations manuals	Access control
Confidential	Sensitive business information	Contracts, financial reports	Encryption, strict access control
Strictly Confidential	Highly sensitive data	Personal data, trade secrets	End-to-end encryption, MFA, audit logging

---

70.5 Internal Data Flows

70.5.1 Application-to-Application Communication

Data Flow-ID	Source	Destination	Protocol	Port	Data Type	Classification	Encryption	Frequency
DF-INT-001	[TODO: ERP System]	[TODO: CRM System]	HTTPS	443	Customer Data	Confidential	TLS 1.3	Real-time
DF-INT-002	[TODO: App Server]	[TODO: Database]	PostgreSQL	5432	Transaction Data	Strictly Confidential	TLS 1.2+	Continuous
DF-INT-003	[TODO: Backup System]	[TODO: Storage]	iSCSI	3260	Backup Data	Confidential	IPSec	Daily
[TODO]	[TODO: Source]	[TODO: Destination]	[TODO: Protocol]	[TODO: Port]	[TODO: Data Type]	[TODO: Classification]	[TODO: Encryption]	[TODO: Frequency]

Security Measures: - Network segmentation between application and database layers - Firewall rules with least privilege principle - Encrypted connections (TLS 1.2+) - Authentication via certificates or service accounts

---

70.5.2 Site-to-Site Connections

Data Flow-ID	Source Site	Destination Site	Connection Type	Bandwidth	Data Type	Encryption	Redundancy
DF-S2S-001	{{ netbox.site.name }}	[TODO: Branch Office]	MPLS	[TODO: Mbps]	All Business Data	IPSec	Yes
DF-S2S-002	{{ netbox.site.name }}	[TODO: DR Site]	Dedicated Line	[TODO: Mbps]	Replication Data	AES-256	Yes
[TODO]	[TODO: Source]	[TODO: Destination]	[TODO: Type]	[TODO: Bandwidth]	[TODO: Data Type]	[TODO: Encryption]	[TODO: Redundancy]

Security Measures: - VPN tunnels with IPSec or WireGuard - Redundant connections for critical sites - Monitoring and alerting for connection failures - Regular security audits

---

70.5.3 Database Replication

Data Flow-ID	Primary DB	Secondary DB	Replication Type	Data Type	Classification	Encryption	RPO
DF-REP-001	[TODO: Prod DB]	[TODO: DR DB]	Asynchronous	All Production Data	Strictly Confidential	TLS 1.3	< 1h
DF-REP-002	[TODO: Prod DB]	[TODO: Reporting DB]	Synchronous	Reporting Data	Confidential	TLS 1.2	< 5min
[TODO]	[TODO: Primary]	[TODO: Secondary]	[TODO: Type]	[TODO: Data Type]	[TODO: Classification]	[TODO: Encryption]	[TODO: RPO]

70.6 External Data Flows

70.6.1 Cloud Services

Data Flow-ID	Internal System	Cloud Service	Provider	Data Type	Classification	Encryption	Data Location
DF-EXT-001	[TODO: File Server]	Microsoft 365	Microsoft	Documents, Emails	Confidential	TLS 1.3, At-Rest AES-256	EU
DF-EXT-002	[TODO: App Server]	AWS S3	Amazon	Backup Data	Confidential	TLS 1.3, SSE-S3	EU (Frankfurt)
DF-EXT-003	[TODO: Monitoring]	Azure Monitor	Microsoft	Logs, Metrics	Internal	TLS 1.3	EU
[TODO]	[TODO: System]	[TODO: Service]	[TODO: Provider]	[TODO: Data Type]	[TODO: Classification]	[TODO: Encryption]	[TODO: Location]

Security Measures: - Cloud Security Posture Management (CSPM) - Identity and Access Management (IAM) with least privilege - Encryption in transit and at rest - Regular security assessments of cloud providers - Data residency compliance (GDPR)

70.6.2 Partner Interfaces

Data Flow-ID	Internal System	Partner	Interface Type	Data Type	Classification	Encryption	Contract
DF-PART-001	[TODO: ERP]	[TODO: Supplier A]	REST API	Order Data	Confidential	TLS 1.3, API Key	[TODO: Contract No.]

Data Flow-ID	Internal System	Partner	Interface Type	Data Type	Classification	Encryption	Contract
DF-PART-002	[TODO: CRM]	[TODO: Partner B]	SFTP	Customer Data	Strictly Confidential	SSH, PGP	[TODO: Contract No.]
[TODO]	[TODO: System]	[TODO: Partner]	[TODO: Type]	[TODO: Data Type]	[TODO: Classification]	[TODO: Encryption]	[TODO: Contract]

Security Measures: - Supplier security assessments before contract signing - Data Processing Agreements (DPA) according to GDPR Art. 28 - Mutual TLS (mTLS) for API communication - API rate limiting and monitoring - Regular security audits

---

70.6.3 Customer Interfaces

Data Flow-ID	Internal System	Interface	Protocol	Data Type	Classification	Encryption	Authentication
DF-CUST-001	[TODO: Web App]	Customer Portal	HTTPS	Customer Data	Strictly Confidential	TLS 1.3	OAuth 2.0 + MFA
DF-CUST-002	[TODO: API Gateway]	Mobile App	HTTPS	Transaction Data	Confidential	TLS 1.3	JWT + Biometrics
[TODO]	[TODO: System]	[TODO: Interface]	[TODO: Protocol]	[TODO: Data Type]	[TODO: Classification]	[TODO: Encryption]	[TODO: Auth]

Security Measures: - Web Application Firewall (WAF) - DDoS Protection - Rate limiting and throttling - Input validation and output encoding - Security headers (HSTS, CSP, etc.)

70.7 Cross-Border Data Flows

70.7.1 EU-Third Country Transfers

Data Flow-ID	Source (EU)	Destination (Third Country)	Country	Data Type	Legal Basis	Protection Measures
DF-CROSS-001	{{ net-box.site.name }}	[TODO: US Data Center]	USA	Cloud Data	Standard Contractual Clauses (SCC)	Encryption, Access Controls
[TODO]	[TODO: Source]	[TODO: Destination]	[TODO: Country]	[TODO: Data Type]	[TODO: Legal Basis]	[TODO: Measures]

GDPR Compliance: - Art. 44-50 GDPR: Data transfer to third countries - Standard Contractual Clauses (SCC) according to Art. 46 para. 2 lit. c GDPR - Transfer Impact Assessment (TIA) conducted - Additional protection measures implemented

---

70.8 Interface Documentation

70.8.1 API Interfaces

API-ID	Name	Type	Version	Authentication	Authorization	Rate Limit	Documentation
API-001	[TODO: Customer API]	REST	v2.0	OAuth 2.0	RBAC	1000 req/min	[TODO: URL]
API-002	[TODO: Partner API]	REST	v1.5	API Key + mTLS	API Key Scopes	500 req/min	[TODO: URL]
API-003	[TODO: Internal API]	GraphQL	v1.0	JWT	ABAC	Unlimited	[TODO: URL]
[TODO]	[TODO: Name]	[TODO: Type]	[TODO: Version]	[TODO: Auth]	[TODO: Authz]	[TODO: Limit]	[TODO: Docs]

Security Requirements: - API gateway with authentication and authorization - Input validation and schema validation - Output filtering (no sensitive data in error messages) - Logging and monitoring of all API access - Versioning and deprecation policy

---

70.8.2 File Transfer Interfaces

Interface-ID	Type	Protocol	Source	Destination	Data Type	Encryption	Authentication
FT-001	SFTP	SSH	[TODO: System]	[TODO: Partner]	Files	SSH, PGP	SSH Key
FT-002	FTPS	FTP over TLS	[TODO: System]	[TODO: System]	Backup Files	TLS 1.3	Certificate
FT-003	MFT	Managed File Transfer	[TODO: System]	[TODO: Partner]	Business Data	AES-256	OAuth 2.0
[TODO]	[TODO: Type]	[TODO: Protocol]	[TODO: Source]	[TODO: Destination]	[TODO: Data Type]	[TODO: Encryption]	[TODO: Auth]

70.8.3 Messaging Interfaces

Interface-ID	Type	Protocol	Source	Destination	Message Type	Encryption	Persistence
MSG-001	Message Queue	AMQP	[TODO: Producer]	[TODO: Consumer]	Events	TLS 1.3	7 Days
MSG-002	Event Stream	Kafka	[TODO: Producer]	[TODO: Consumer]	Logs	TLS 1.3	30 Days
[TODO]	[TODO: Type]	[TODO: Protocol]	[TODO: Source]	[TODO: Destination]	[TODO: Message Type]	[TODO: Encryption]	[TODO: Persistence]

70.8.4 Email Communication

Communication Type	Sender	Recipient	Data Type	Classification	Encryption	Archiving
Business Email	{{ meta.organization.domain }}	External	Business Correspondence	Confidential	TLS (Opportunistic)	7 Years
Confidential Email	{{ meta.organization.domain }}	External	Contract Documents	Strictly Confidential	S/MIME or PGP	10 Years
Internal Email	{{ meta.organization.domain }}	{{ meta.organization.domain }}	Internal Communication	Internal	TLS (Enforced)	3 Years

Security Measures: - SPF, DKIM, DMARC for email authentication - Email gateway with anti-spam and anti-malware - Data Loss Prevention (DLP) for outgoing emails - Email encryption for confidential content - Email archiving according to legal requirements

---

70.9 Network Architecture

70.9.1 Network Zones

Zone	Description	Security Level	Access Control	Systems
DMZ	Demilitarized zone for publicly accessible services	High	Firewall, IDS/IPS	Web Servers, Mail Gateway
Internal	Internal network for business applications	Medium	Firewall, NAC	App Servers, File Servers
Management	Management network for administration	Very High	Firewall, MFA, Jump Host	Management Interfaces
Production	Production network for critical systems	Very High	Firewall, Segmentation	Database Servers, Core Systems
Development	Development and test network	Low	Firewall	Dev/Test Systems

---

70.9.2 Firewall Rules (Example)

Rule-ID	Source Zone	Destination Zone	Protocol	Port	Action	Logging	Description
FW-001	Internet	DMZ	HTTPS	443	Allow	Yes	Web traffic to web servers
FW-002	DMZ	Internal	HTTPS	443	Allow	Yes	Web server to app server
FW-003	Internal	Production	PostgreSQL	5432	Allow	Yes	App server to database
FW-004	Management	All	SSH	22	Allow	Yes	Admin access
FW-999	Any	Any	Any	Any	Deny	Yes	Default Deny

Note: Complete firewall rules in separate documentation.

70.10 Data Flow Diagrams

70.10.1 High-Level Architecture

```
[Internet]
    |
    | HTTPS (443)
    v
[Firewall/WAF]
    |
    | HTTPS (443)
    v
[DMZ - Web Server]
    |
    | HTTPS (443)
    v
[Internal - App Server]
    |
    | PostgreSQL (5432)
    v
[Production - Database]
```

Note: Detailed network diagrams in separate files (e.g., Visio, Draw.io).

70.10.2 Data Flow for Critical Business Processes

70.10.2.1 Example: Customer Order

```
[Customer]
  -> HTTPS -> [Web Portal (DMZ)]
  -> HTTPS -> [Order Service (Internal)]
  -> PostgreSQL -> [Order DB (Production)]
  -> HTTPS -> [Payment Gateway (External)]
  -> HTTPS -> [ERP System (Internal)]
  -> HTTPS -> [Warehouse System (Internal)]
```

Security Measures: - End-to-end encryption - Authentication at each level - Input validation - Audit logging of all transactions

---

70.11 Risk Assessment Data Flows

70.11.1 Risk Matrix

Data Flow-ID	Threat	Likelihood	Impact	Risk	Measures	Residual Risk
DF-EXT-001	Data loss during cloud transfer	Low	High	Medium	Encryption, DLP	Low
DF-PART-001	Unauthorized access by partner	Medium	High	High	mTLS, API Gateway, Monitoring	Medium
DF-CROSS-001	Third country access to EU data	Medium	Very High	High	SCC, Encryption, Access Controls	Medium
[TODO]	[TODO: Threat]	[TODO: Likelihood]	[TODO: Impact]	[TODO: Risk]	[TODO: Measures]	[TODO: Residual Risk]

70.12 Monitoring and Logging

70.12.1 Data Flow Monitoring

Monitoring Type	Tool	Metrics	Alerting	Retention
Network Traffic	[TODO: NetFlow/sFlow]	Bandwidth, Connections, Anomalies	Yes	90 Days
API Traffic	[TODO: API Gateway]	Request Rate, Latency, Errors	Yes	90 Days
Firewall Logs	[TODO: SIEM]	Blocked Connections, Rule Hits	Yes	1 Year
Application Logs	[TODO: Log Management]	Transactions, Errors, Security Events	Yes	1 Year

---

70.12.2 Security Events

The following security events are monitored for data flows:

- Unusual data transfer volumes
- Connections to unknown destinations
- Failed authentication attempts

- Protocol violations
- Encryption errors
- DLP violations

70.13 Compliance and Data Protection

70.13.1 GDPR Requirements

Requirement	Article	Implementation	Evidence
Lawfulness of processing	Art. 6	Legal basis documented	Processing register
Data minimization	Art. 5 para. 1 lit. c	Only necessary data transferred	Data flow documentation
Integrity and confidentiality	Art. 5 para. 1 lit. f	Encryption, access control	Security measures
Third country transfer	Art. 44-50	SCC, TIA	Transfer documentation

---

70.13.2 Processing Register Reference

All data flows are documented in the processing register according to Art. 30 GDPR.

Reference: [TODO: Link to processing register]

70.14 Change Management

70.14.1 Change Control

All changes to data flows and interfaces are subject to the change management process:

1. **Change Request:** Request with justification and risk assessment
2. **Security Review:** Assessment by security team
3. **Approval:** Approval by Change Advisory Board
4. **Implementation:** Implementation with documentation
5. **Verification:** Testing and validation
6. **Documentation Update:** Update of this document

Reference: 0360_Policy_Change_and_Release_Management.md

70.15 References

- Policy: 0660_Policy_Information_Transfer_and_Communication.md
- Guideline: 0670_Guideline_Email_Sharing_and_Collaboration_Tools.md

- Policy: 0460_Policy_Supplier_and_Cloud_Security.md
- Guideline: 0470_Guideline_Third_Party_Risk_Assessment_and_Cloud_Controls.md
- Policy: 0600_Policy_Network_Security.md
- Guideline: 0610_Guideline_Segmentation_Firewalling_and_Network_Access_Control.md
- Appendix: 0720_Appendix_Asset_and_System_Inventory_Template.md

---

Document Owner: Thomas Weber
Approved By: {{ meta.management.name }}
Next Review: Semi-annually

ewpage

Chapter 71

Appendix D: Terms and Abbreviations

Document Type: Appendix
Version: 1.0.0
Date: {{ meta.document.date }}
Classification: internal

71.1 Purpose

This document defines all terms and abbreviations used in the ISMS. It serves as a central reference for consistent terminology and facilitates understanding of ISMS documentation.

71.2 Scope

Organization: AdminSend GmbH
ISMS Scope: {{ meta.isms.scope }}
Responsible: Thomas Weber

71.3 Abbreviations

71.3.1 A

Abbreviation	Meaning	Explanation
ABAC	Attribute-Based Access Control	Attribute-based access control
ACL	Access Control List	Access control list
AES	Advanced Encryption Standard	Symmetric encryption standard

Abbreviation	Meaning	Explanation
API	Application Programming Interface	Application programming interface
APT	Advanced Persistent Threat	Advanced persistent threat
AV	Antivirus	Antivirus software

71.3.2 B

Abbreviation	Meaning	Explanation
BC	Business Continuity	Business continuity
BCP	Business Continuity Plan	Business continuity plan
BIA	Business Impact Analysis	Business impact analysis
BYOD	Bring Your Own Device	Use of personal devices for business purposes

71.3.3 C

Abbreviation	Meaning	Explanation
CA	Certificate Authority	Certificate authority
CAB	Change Advisory Board	Change advisory board
CIA	Confidentiality, Integrity, Availability	Confidentiality, integrity, availability
CISO	Chief Information Security Officer	Chief information security officer
CIS	Center for Internet Security	Center for Internet Security
CMDB	Configuration Management Database	Configuration management database
CRM	Customer Relationship Management	Customer relationship management
CSP	Content Security Policy	Content security policy
CSPM	Cloud Security Posture Management	Cloud security posture management
CVE	Common Vulnerabilities and Exposures	Common vulnerabilities and exposures
CVSS	Common Vulnerability Scoring System	Common vulnerability scoring system

71.3.4 D

Abbreviation	Meaning	Explanation
DAST	Dynamic Application Security Testing	Dynamic application security testing
DDoS	Distributed Denial of Service	Distributed denial of service attack
DLP	Data Loss Prevention	Data loss prevention
DMZ	Demilitarized Zone	Demilitarized zone
DNS	Domain Name System	Domain name system
DoS	Denial of Service	Denial of service attack
DPA	Data Processing Agreement	Data processing agreement
DPIA	Data Protection Impact Assessment	Data protection impact assessment
DPO	Data Protection Officer	Data protection officer
DR	Disaster Recovery	Disaster recovery
DRP	Disaster Recovery Plan	Disaster recovery plan

71.3.5 E

Abbreviation	Meaning	Explanation
EDR	Endpoint Detection and Response	Endpoint detection and response
ERP	Enterprise Resource Planning	Enterprise resource planning

71.3.6 F

Abbreviation	Meaning	Explanation
FQDN	Fully Qualified Domain Name	Fully qualified domain name
FTP	File Transfer Protocol	File transfer protocol
FTPS	FTP Secure	Secure FTP over TLS

71.3.7 G

Abbreviation	Meaning	Explanation
GDPR	General Data Protection Regulation	General Data Protection Regulation

71.3.8 H

Abbreviation	Meaning	Explanation
HIDS	Host-based Intrusion Detection System	Host-based intrusion detection system
HIPS	Host-based Intrusion Prevention System	Host-based intrusion prevention system
HSTS	HTTP Strict Transport Security	HTTP strict transport security
HTTP	Hypertext Transfer Protocol	Hypertext transfer protocol
HTTPS	HTTP Secure	Secure HTTP over TLS

71.3.9 I

Abbreviation	Meaning	Explanation
IaaS	Infrastructure as a Service	Infrastructure as a service
IAM	Identity and Access Management	Identity and access management
ICMP	Internet Control Message Protocol	Internet control message protocol
ICT	Information and Communication Technology	Information and communication technology
IDS	Intrusion Detection System	Intrusion detection system
IG	Implementation Group	Implementation group (CIS Controls)
IoC	Indicator of Compromise	Indicator of compromise
IP	Internet Protocol	Internet protocol
IPS	Intrusion Prevention System	Intrusion prevention system
IPSec	Internet Protocol Security	Internet protocol security
ISMS	Information Security Management System	Information security management system
ISO	International Organization for Standardization	International Organization for Standardization
ISP	Internet Service Provider	Internet service provider
IT	Information Technology	Information technology

71.3.10 J

Abbreviation	Meaning	Explanation
JWT	JSON Web Token	JSON web token

71.3.11 K

Abbreviation	Meaning	Explanation
KPI	Key Performance Indicator	Key performance indicator

71.3.12 L

Abbreviation	Meaning	Explanation
LDAP	Lightweight Directory Access Protocol	Lightweight directory access protocol

71.3.13 M

Abbreviation	Meaning	Explanation
MAC	Media Access Control / Mandatory Access Control	MAC address / Mandatory access control
MDM	Mobile Device Management	Mobile device management
MFA	Multi-Factor Authentication	Multi-factor authentication
MFT	Managed File Transfer	Managed file transfer
MPLS	Multiprotocol Label Switching	Multiprotocol label switching
mTLS	Mutual TLS	Mutual TLS

71.3.14 N

Abbreviation	Meaning	Explanation
NAC	Network Access Control	Network access control
NDA	Non-Disclosure Agreement	Non-disclosure agreement
NIDS	Network-based Intrusion Detection System	Network-based intrusion detection system
NIPS	Network-based Intrusion Prevention System	Network-based intrusion prevention system

Abbreviation	Meaning	Explanation
NTP	Network Time Protocol	Network time protocol

71.3.15 O

Abbreviation	Meaning	Explanation
OAuth	Open Authorization	Open authorization protocol
OWASP	Open Web Application Security Project	Open Web Application Security Project

71.3.16 P

Abbreviation	Meaning	Explanation
PaaS	Platform as a Service	Platform as a service
PAM	Privileged Access Management	Privileged access management
PCI DSS	Payment Card Industry Data Security Standard	Payment Card Industry Data Security Standard
PGP	Pretty Good Privacy	Pretty Good Privacy (encryption)
PII	Personally Identifiable Information	Personally identifiable information
PKI	Public Key Infrastructure	Public key infrastructure

71.3.17 R

Abbreviation	Meaning	Explanation
RACI	Responsible, Accountable, Consulted, Informed	Responsibility assignment matrix
RBAC	Role-Based Access Control	Role-based access control
REST	Representational State Transfer	Representational state transfer
RPO	Recovery Point Objective	Recovery point objective
RTO	Recovery Time Objective	Recovery time objective

71.3.18 S

Abbreviation	Meaning	Explanation
SaaS	Software as a Service	Software as a service
SAML	Security Assertion Markup Language	Security Assertion Markup Language
SAN	Storage Area Network	Storage area network
SAST	Static Application Security Testing	Static application security testing
SCC	Standard Contractual Clauses	Standard contractual clauses
SDLC	Software Development Life Cycle	Software development life cycle
SFTP	SSH File Transfer Protocol	SSH file transfer protocol
SIEM	Security Information and Event Management	Security information and event management
SLA	Service Level Agreement	Service level agreement
S/MIME	Secure/Multipurpose Internet Mail Extensions	Secure email encryption
SMB	Server Message Block	Server message block
SMTP	Simple Mail Transfer Protocol	Simple mail transfer protocol
SoA	Statement of Applicability	Statement of applicability
SOAP	Simple Object Access Protocol	Simple object access protocol
SOC	Security Operations Center	Security operations center
SOP	Standard Operating Procedure	Standard operating procedure
SPF	Sender Policy Framework	Sender policy framework
SQL	Structured Query Language	Structured query language
SSH	Secure Shell	Secure shell
SSL	Secure Sockets Layer	Secure sockets layer (deprecated, see TLS)
SSO	Single Sign-On	Single sign-on

71.3.19 T

Abbreviation	Meaning	Explanation
TCP	Transmission Control Protocol	Transmission control protocol
TIA	Transfer Impact Assessment	Transfer impact assessment
TLS	Transport Layer Security	Transport layer security
TTP	Tactics, Techniques, and Procedures	Tactics, techniques, and procedures

71.3.20 U

Abbreviation	Meaning	Explanation
UDP	User Datagram Protocol	User datagram protocol
UPS	Uninterruptible Power Supply	Uninterruptible power supply
URL	Uniform Resource Locator	Uniform resource locator

71.3.21 V

Abbreviation	Meaning	Explanation
VLAN	Virtual Local Area Network	Virtual local area network
VPN	Virtual Private Network	Virtual private network

71.3.22 W

Abbreviation	Meaning	Explanation
WAF	Web Application Firewall	Web application firewall
WAN	Wide Area Network	Wide area network

71.3.23 X

Abbreviation	Meaning	Explanation
XSS	Cross-Site Scripting	Cross-site scripting

71.3.24 Z

Abbreviation	Meaning	Explanation
ZTA	Zero Trust Architecture	Zero trust architecture

71.4 Term Definitions

71.4.1 A

Acceptable Use Policy (AUP)
Policy that defines acceptable use of IT resources.

Access Control
Mechanisms to control access to resources.

Accountability
Responsibility for actions and decisions.

Advanced Persistent Threat (APT)
Targeted, long-term cyber attacks.

Annex A
Annex A of ISO/IEC 27001, which defines 93 security controls.

Asset
Any resource with value to the organization (hardware, software, data, etc.).

Audit
Systematic, independent review to determine conformity.

Authentication
Proof of identity of a user or system.

Authorization
Granting of access rights after successful authentication.

Availability
Property that information and systems are accessible when needed.

71.4.2 B

Backup
Copy of data for recovery in case of failure.

Baseline
Defined state as reference for changes.

Business Continuity
Ability to maintain business processes during disruptions.

Business Impact Analysis (BIA)
Assessment of the impact of disruptions on business processes.

71.4.3 C

Change Management
Controlled process for implementing changes.

CIA Triad
Fundamental principles of information security (Confidentiality, Integrity, Availability).

Cloud Computing
Provision of IT resources over the internet.

Compliance
Adherence to laws, regulations, and standards.

Confidentiality
Protection of information from unauthorized disclosure.

Configuration Management
Management and control of system configurations.

Control
Security measure to reduce risk.

Cryptography
Science of encrypting and decrypting information.

Cyber Security
Protection of computer systems and networks from attacks.

71.4.4 D

Data Breach
Unauthorized access to or disclosure of data.

Data Classification
Categorization of data according to protection requirements.

Data Loss Prevention (DLP)
Technologies to protect against data loss.

Data Protection
Protection of personal data.

Disaster Recovery
Recovery of IT systems after a failure.

71.4.5 E

Encryption
Conversion of data into unreadable format.

Endpoint
Device at the end of a network connection (PC, laptop, smartphone).

Event
Identifiable change of state in a system.

71.4.6 F

Firewall
Security system to control network traffic.

Forensics
Investigation of security incidents.

71.4.7 G

Gap Analysis
Comparison between current and desired state.

Governance
Framework for leadership and control.

71.4.8 H

Hardening
Securing systems by removing unnecessary functions.

Hash
Unique checksum for integrity assurance.

71.4.9 I

Incident
Event that affects information security.

Incident Response
Process for handling security incidents.

Information Security
Protection of information from threats.

Integrity
Property that information is complete and unchanged.

Intrusion Detection
Detection of attacks on systems.

71.4.10 K

Key Management
Management of cryptographic keys.

71.4.11 L

Least Privilege
Principle of granting only necessary access rights.

Logging
Recording of events and activities.

71.4.12 M

Malware
Software with malicious intent.

Management Review
Regular review of the ISMS by management.

Monitoring
Continuous observation of systems and processes.

Multi-Factor Authentication (MFA)
Authentication with multiple factors.

71.4.13 N

Network Segmentation
Division of a network into separate areas.

Non-Conformity
Deviation from requirements.

71.4.14 P

Patch Management
Process for managing software updates.

Penetration Testing
Simulated attack to identify vulnerabilities.

Phishing
Attempt to obtain sensitive data through fake messages.

Policy
Formal rule or principle of the organization.

Privacy
Right to protection of personal data.

Privileged Access
Access with extended rights.

71.4.15 R

Ransomware
Malware that encrypts data and demands ransom.

Recovery Point Objective (RPO)
Maximum acceptable data loss.

Recovery Time Objective (RTO)
Maximum acceptable downtime.

Residual Risk
Remaining risk after implementation of measures.

Risk
Combination of likelihood and impact of a threat.

Risk Assessment
Process for identifying and assessing risks.

Risk Treatment
Measures to reduce risk.

71.4.16 S

Security Awareness
Knowledge and understanding of information security.

Security Control
Measure to reduce risk.

Security Incident
Event that affects information security.

Security Policy
Formal rule for information security.

Segregation of Duties
Division of tasks to avoid conflicts of interest.

Social Engineering
Manipulation of people to disclose information.

Statement of Applicability (SoA)
Document explaining the applicability of controls.

Supply Chain
Network of suppliers and service providers.

71.4.17 T

Threat
Potential cause of an unwanted event.

Threat Intelligence
Information about current threats.

Two-Factor Authentication (2FA)
Authentication with two factors.

71.4.18 V

Vulnerability
Weakness that can be exploited by a threat.

Vulnerability Assessment
Identification and assessment of vulnerabilities.

71.4.19 W

Whitelist
List of allowed elements (applications, IP addresses, etc.).

71.4.20 Z

Zero Day
Vulnerability for which no patch is yet available.

Zero Trust
Security model without implicit trust.

71.5 ISO/IEC 27001:2022 Specific Terms

Annex A Control
One of the 93 security controls from Annex A of ISO/IEC 27001:2022.

Context of the Organization
Understanding of internal and external factors (Clause 4).

Continual Improvement
Ongoing improvement of the ISMS (Clause 10).

Documented Information
Information that must be documented and retained.

Interested Party
Person or organization that can influence the ISMS.

Internal Audit
Systematic review of the ISMS (Clause 9.2).

ISMS Scope
Boundaries and applicability of the ISMS (Clause 4.3).

Leadership
Commitment and engagement of top management (Clause 5).

Management Review
Regular review by management (Clause 9.3).

Performance Evaluation
Monitoring, measurement, and evaluation of the ISMS (Clause 9).

Risk Assessment
Process for identifying and assessing risks (Clause 6.1.2).

Risk Treatment
Selection and implementation of measures (Clause 6.1.3).

Statement of Applicability (SoA)
Document with Annex A controls and their applicability (Clause 6.1.3).

71.6 References

- ISO/IEC 27000:2018 Information Security Management Systems - Overview and Vocabulary
- ISO/IEC 27001:2022 Information Security Management Systems - Requirements
- ISO/IEC 27002:2022 Information Security Controls
- NIST Glossary: https://csrc.nist.gov/glossary

Document Owner: Thomas Weber
Approved By: {{ meta.management.name }}
Next Review: Annually

ewpage