Contents

Chapter 1

NIST 800-53 Security and Privacy Controls Handbook

Document Metadata

- **Created on:** 2026-02-10
- **Author:** Andreas Huemmer [andreas.huemmer@adminsend.de]
- **Version:** 0.0.5
- **Type:** NIST 800-53 Handbook

---

ewpage

Chapter 2

System Categorization

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

2.1 1. Purpose

This document describes the categorization of the information system {{ meta.nist.system_name }} according to FIPS 199 and NIST SP 800-60.

2.1.1 1.1 Objectives

- **FIPS 199 Compliance:** Categorization by security objectives (confidentiality, integrity, availability)
- **Risk Assessment:** Determination of potential impacts from security breaches
- **Baseline Selection:** Foundation for security control selection
- **Compliance:** Meeting federal requirements

2.1.2 1.2 References

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

2.2 2. System Information

2.2.1 2.1 System Identification

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

2.2.2 2.2 System Description

Purpose: [TODO: Description of system purpose]

Functions: - [TODO: Main function 1] - [TODO: Main function 2] - [TODO: Main function 3]

Users: - **Internal Users:** [TODO: Number and roles] - **External Users:** [TODO: Number and roles] - **Privileged Users:** [TODO: Number and roles]

2.2.3 2.3 Information Types

Information Type	Description	Source (NIST 800-60)
[TODO: Type 1]	[TODO: Description]	[TODO: C.2.x.x]
[TODO: Type 2]	[TODO: Description]	[TODO: C.3.x.x]
[TODO: Type 3]	[TODO: Description]	[TODO: C.4.x.x]

2.3 3. FIPS 199 Categorization

2.3.1 3.1 Security Objectives and Impact Levels

Categorization is performed according to three security objectives:

2.3.1.1 3.1.1 Confidentiality

Definition: Protection from unauthorized disclosure of information.

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

Rationale: [TODO: Describe potential impacts of unauthorized disclosure]

Impact Examples: - **Low:** Limited adverse effects on organizational operations, assets, or individuals - **Moderate:** Serious adverse effects - **High:** Severe or catastrophic adverse effects

Specific Impacts for This System: - [TODO: Impact 1] - [TODO: Impact 2] - [TODO: Impact 3]

2.3.1.2 3.1.2 Integrity

Definition: Protection from unauthorized modification or destruction of information.

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

Rationale: [TODO: Describe potential impacts of unauthorized modification]

Specific Impacts for This System: - [TODO: Impact 1] - [TODO: Impact 2] - [TODO: Impact 3]

2.3.1.3 3.1.3 Availability

Definition: Ensuring timely and reliable access to information.

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

Rationale: [TODO: Describe potential impacts of availability loss]

Specific Impacts for This System: - [TODO: Impact 1] - [TODO: Impact 2] - [TODO: Impact 3]

2.3.2 3.2 Overall Categorization

FIPS 199 Security Category:

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

Example:

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

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

> **Note:** Overall categorization corresponds to the highest impact level of the three security objectives (High-Water Mark).

2.4 4. Categorization by Information Types

2.4.1 4.1 Information Type Analysis

For each information type, categorization is performed according to NIST SP 800-60:

2.4.1.1 Information Type 1: [TODO: Name]

Description: [TODO: Description of information type]

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

Security Objective	Provisional Impact	Adjusted Impact	Rationale
Confidentiality	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: Rationale]
Integrity	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: Rationale]
Availability	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: Rationale]

2.4.1.2 Information Type 2: [TODO: Name]

Description: [TODO: Description of information type]

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

Security Objective	Provisional Impact	Adjusted Impact	Rationale
Confidentiality	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: Rationale]
Integrity	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: Rationale]
Availability	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: Rationale]

2.4.2 4.2 Aggregated Categorization

Method: High-Water Mark (highest impact level across all information types)

Security Objective	Aggregated Impact
Confidentiality	[TODO: Low / Moderate / High]
Integrity	[TODO: Low / Moderate / High]
Availability	[TODO: Low / Moderate / High]

2.5 5. Baseline Selection

2.5.1 5.1 NIST 800-53 Baseline

Based on overall categorization, the following baseline is selected:

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

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

2.5.2 5.2 Tailoring

Tailoring Activities: - **Added Controls:** [TODO: List of additional controls] - **Removed Controls:** [TODO: List of removed controls with rationale] - **Modified Controls:** [TODO: List of modified controls]

2.6 6. Categorization Process

2.6.1 6.1 Process Steps

1. **System Identification:** Identify system to be categorized
2. **Information Type Identification:** Identify all processed information types
3. **Provisional Impact:** Determine provisional impact levels per NIST 800-60
4. **Impact Adjustment:** Adjust based on organization-specific factors

5. **Aggregation:** Aggregate to overall categorization
6. **Documentation:** Document categorization
7. **Approval:** Approval by Authorizing Official

2.6.2 6.2 Involved Roles

Role	Name	Responsibility
System Owner	[TODO: Name]	System responsibility
Information Owner	[TODO: Name]	Information responsibility
ISSO	{{ meta.roles.isso.name }}	Security assessment
ISSM	{{ meta.roles.issm.name }}	Security management
Authorizing Official (AO)	{{ meta.roles.ao.name }}	Approval

2.6.3 6.3 Categorization Date

Initial Categorization: [TODO: Date]
Last Review: [TODO: Date]
Next Review: [TODO: Date]

2.7 7. Impact Analysis

2.7.1 7.1 Confidentiality Loss

Potential impacts from unauthorized disclosure:

Area	Impact	Severity
Organizational Operations	[TODO: Description]	[TODO: L/M/H]
Organizational Assets	[TODO: Description]	[TODO: L/M/H]
Individuals	[TODO: Description]	[TODO: L/M/H]
National Security	[TODO: Description]	[TODO: L/M/H]

2.7.2 7.2 Integrity Loss

Potential impacts from unauthorized modification:

Area	Impact	Severity
Organizational Operations	[TODO: Description]	[TODO: L/M/H]
Organizational Assets	[TODO: Description]	[TODO: L/M/H]
Individuals	[TODO: Description]	[TODO: L/M/H]
National Security	[TODO: Description]	[TODO: L/M/H]

2.7.3 7.3 Availability Loss

Potential impacts from system failure:

Area	Impact	Severity
Organizational Operations	[TODO: Description]	[TODO: L/M/H]
Organizational Assets	[TODO: Description]	[TODO: L/M/H]
Individuals	[TODO: Description]	[TODO: L/M/H]
National Security	[TODO: Description]	[TODO: L/M/H]

2.8 8. Approval

2.8.1 8.1 Categorization Approval

Categorization approved by:

Name: {{ meta.roles.ao.name }}
Title: Authorizing Official (AO)
Date: [TODO: Date]
Signature: [TODO: Signature or electronic approval]

2.8.2 8.2 Review Interval

Review Frequency: [TODO: Annually / Upon significant changes]

Triggers for Recategorization: - Significant system changes - New information types - Changes in threat landscape - Organizational changes - Legal or regulatory changes

2.9 9. Appendix

2.9.1 9.1 FIPS 199 Impact Level Definitions

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

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

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

2.9.2 9.2 Categorization Matrix

Information Type	Confidentiality	Integrity	Availability	Overall
[TODO: Type 1]	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: L/M/H]
[TODO: Type 2]	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: L/M/H]

Information Type	Confidentiality	Integrity	Availability	Overall
[TODO: Type 3]	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: L/M/H]	[TODO: L/M/H]
System Overall	**[TODO: L/M/H]**	**[TODO: L/M/H]**	**[TODO: L/M/H]**	**[TODO: L/M/H]**

Document History:

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

ewpage

Chapter 3

Scope and System Boundaries

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

3.1 1. Purpose

This document defines the scope and authorization boundaries of the information system {{ meta.nist.system_name }}.

3.2 2. System Identification

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

3.3 3. Authorization Boundary

3.3.1 3.1 Boundary Definition

The authorization boundary includes all components under a single authorization decision.

Authorization Boundary: [TODO: Description of boundary]

Included Components: - [TODO: Component 1] - [TODO: Component 2]

Excluded Components: - [TODO: Component 1 - Rationale]

3.3.2 3.2 Network Diagram

[TODO: Insert network diagram showing authorization boundary]

3.4 4. System Components

3.4.1 4.1 Hardware Components

Component	Type	Location	Function	Criticality
[TODO: Server 1]	Server	[TODO: DC1]	[TODO: Function]	[TODO: H/M/L]

3.4.2 4.2 Software Components

Component	Version	Vendor	Function	License
[TODO: OS]	[TODO: Version]	[TODO: Vendor]	Operating System	[TODO: License]

3.4.3 4.3 Data Components

Data Type	Classification	Storage Location	Retention	Backup
[TODO: Data 1]	[TODO: Classification]	[TODO: Location]	[TODO: Time]	[TODO: Yes/No]

3.5 5. External Interfaces

3.5.1 5.1 System Connections

Connected System	Connection Type	Protocol	Purpose	Authorization
[TODO: System 1]	[TODO: Type]	[TODO: Protocol]	[TODO: Purpose]	[TODO: ATO Number]

3.6 6. Locations

3.6.1 6.1 Physical Locations

Location-ID	Location Name	Address	Components	Security Level
[TODO: LOC-01]	[TODO: Name]	[TODO: Address]	[TODO: List]	[TODO: Level]

3.7 7. Personnel

3.7.1 7.1 User Roles

Role	Count	Access Level	Rationale
[TODO: Admin]	[TODO: Count]	Privileged	Administration

Document History:

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

ewpage

Chapter 4

Roles and Responsibilities

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

4.1 1. Purpose

This document defines roles and responsibilities for the Risk Management Framework (RMF) and security of system {{ meta.nist.system_name }}.

4.2 2. RMF Roles

4.2.1 2.1 Authorizing Official (AO)

Name: {{ meta.roles.ao.name }}
Email: {{ meta.roles.ao.email }}

Responsibilities: - Authorization decision for the system - Acceptance of security risk - Approval of System Security Plan (SSP) - Monitoring of security status

4.2.2 2.2 Information System Security Officer (ISSO)

Name: {{ meta.roles.isso.name }}
Email: {{ meta.roles.isso.email }}

Responsibilities: - Daily security operations - Implementation of security controls - Incident response - Security monitoring

4.2.3 2.3 Information System Security Manager (ISSM)

Name: {{ meta.roles.issm.name }}
Email: {{ meta.roles.issm.email }}

Responsibilities: - Security program management - Policy development - Compliance monitoring - Risk management

4.2.4 2.4 System Owner

Name: [TODO: Name]
Email: [TODO: Email]

Responsibilities: - Overall system responsibility - Business process responsibility - Budget and resources - Approve system changes

4.2.5 2.5 Security Control Assessor (SCA)

Name: [TODO: Name/Company]
Email: [TODO: Email]

Responsibilities: - Independent assessment of security controls - Creation of Security Assessment Report (SAR) - Identification of weaknesses - Recommendations for improvements

4.3 3. RACI Matrix

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

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

---

Document History:

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

ewpage

Chapter 5

Risk Management Framework (RMF)

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

5.1 1. Purpose

This document describes the application of the NIST Risk Management Framework (RMF) to system {{ meta.nist.system_name }}.

5.2 2. RMF Overview

5.2.1 2.1 RMF Steps

The RMF consists of seven steps:

1. **Prepare:** Prepare for RMF activities
2. **Categorize:** System categorization per FIPS 199
3. **Select:** Select security controls
4. **Implement:** Implement controls
5. **Assess:** Assess controls
6. **Authorize:** Authorization decision
7. **Monitor:** Continuous monitoring

5.3 3. RMF Step 1: Prepare

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

Activities: - Organization-wide preparation - System-level preparation - Identification of Common Controls

Outputs: - [TODO: List of outputs]

5.4 4. RMF Step 2: Categorize

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

Document: See NIST-0010 System Categorization

Approved by: {{ meta.roles.ao.name }}
Date: [TODO: Date]

5.5 5. RMF Step 3: Select

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

Selected Controls: - Baseline controls: [TODO: Count] - Additional controls: [TODO: Count] - Total: [TODO: Count]

Tailoring: - Added controls: [TODO: List] - Removed controls: [TODO: List]

5.6 6. RMF Step 4: Implement

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

Implementation Status: - Implemented: [TODO: Count / Percent] - In Progress: [TODO: Count / Percent] - Planned: [TODO: Count / Percent]

Document: See NIST-0021 System Security Plan (SSP)

5.7 7. RMF Step 5: Assess

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

Assessment Information: - Assessor: [TODO: Name/Company] - Assessment Date: [TODO: Date] - Assessment Methods: [TODO: Interview, Examine, Test]

Results: - Satisfied controls: [TODO: Count / Percent] - Partially satisfied controls: [TODO: Count / Percent] - Not satisfied controls: [TODO: Count / Percent]

Document: See NIST-0810 Security Assessment Report (SAR)

5.8 8. RMF Step 6: Authorize

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

Authorization to Operate (ATO): - ATO Status: [TODO: Granted / Denied / Conditional] - ATO Date: [TODO: Date] - ATO Validity: [TODO: 3 years] - Next Reauthorization: [TODO: Date]

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

Risk Assessment: - Overall Risk: [TODO: Low / Moderate / High] - Accepted Risk: [TODO: Description]

Document: Authorization Decision Document

5.9 9. RMF Step 7: Monitor

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

Continuous Monitoring: - Monitoring Strategy: See NIST-0050 - Monitoring Frequency: [TODO: Continuous / Monthly / Quarterly] - Reporting: [TODO: Monthly to AO]

Activities: - Security status monitoring - Change management - Compliance review - Incident response

5.10 10. Timeline

RMF Step	Planned Start	Planned End	Actual End	Status
Prepare	[TODO: Date]	[TODO: Date]	[TODO: Date]	[TODO: Status]
Categorize	[TODO: Date]	[TODO: Date]	[TODO: Date]	[TODO: Status]
Select	[TODO: Date]	[TODO: Date]	[TODO: Date]	[TODO: Status]
Implement	[TODO: Date]	[TODO: Date]	[TODO: Date]	[TODO: Status]
Assess	[TODO: Date]	[TODO: Date]	[TODO: Date]	[TODO: Status]
Authorize	[TODO: Date]	[TODO: Date]	[TODO: Date]	[TODO: Status]
Monitor	[TODO: Date]	Continuous	N/A	[TODO: Status]

Document History:

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

ewpage

Chapter 6

Continuous Monitoring Strategy

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

6.1 1. Purpose

This document describes the continuous monitoring strategy for system {{ meta.nist.system_name }}.

6.2 2. Continuous Monitoring Overview

6.2.1 2.1 Objectives

- **Security Status:** Continuous monitoring of security status
- **Risk Management:** Early detection of risks
- **Compliance:** Ensuring ongoing compliance
- **Incident Detection:** Rapid detection of security incidents

6.2.2 2.2 References

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

6.3 3. Monitoring Strategy

6.3.1 3.1 Monitoring Areas

Area	Description	Frequency	Responsible
Vulnerabilities	Vulnerability Scanning	[TODO: Weekly]	[TODO: ISSO]
Configuration	Configuration Compliance	[TODO: Daily]	[TODO: ISSO]
Patches	Patch Status	[TODO: Weekly]	[TODO: System Admin]
Access	Access Control Review	[TODO: Monthly]	[TODO: ISSO]
Logs	Log Analysis	[TODO: Daily]	[TODO: SOC]
Incidents	Incident Tracking	[TODO: Continuous]	[TODO: ISSO]

6.3.2 3.2 Monitoring Tools

Tool	Purpose	Vendor	Version
[TODO: Vulnerability Scanner]	Vulnerability scans	[TODO: Vendor]	[TODO: Version]
[TODO: SIEM]	Log analysis	[TODO: Vendor]	[TODO: Version]
[TODO: Configuration Management]	Configuration monitoring	[TODO: Vendor]	[TODO: Version]

6.4 4. Metrics and Indicators

6.4.1 4.1 Security Metrics

Metric	Target Value	Measurement Method	Reporting Frequency
Critical Vulnerabilities	0	Vulnerability Scan	Weekly
Patch Compliance	$> 95\%$	Patch Management System	Monthly
Configuration Deviations	$< 5\%$	Configuration Scanner	Weekly
Incident Response Time	< 1 Hour	Incident Tracking	Monthly

6.4.2 4.2 Compliance Indicators

Indicator	Description	Threshold
Control Effectiveness	Percentage of effective controls	$> 90\%$
POA&M Completion	Completed POA&M items	$> 80\%$
Assessment Findings	Open assessment findings	< 10

6.5 5. Reporting

6.5.1 5.1 Reporting Structure

Monthly Reports to AO: - Security status summary - Metrics and trends - New risks and vulnerabilities - POA&M status - Recommendations

Quarterly Reports: - Comprehensive security assessment - Compliance status - System changes - Reauthorization preparation

6.5.2 5.2 Escalation

Escalation Criteria: - Critical vulnerabilities - Security incidents - Compliance violations - Significant system changes

Escalation Path: 1. ISSO → ISSM 2. ISSM → AO 3. AO → Senior Leadership

6.6 6. Change Management

6.6.1 6.1 Change Categories

Category	Description	Approval Required
Significant	Impact on authorization	AO
Moderate	Impact on security controls	ISSO
Minor	No security impact	System Owner

6.6.2 6.2 Change Process

1. Change request
2. Security assessment
3. Approval
4. Implementation
5. Verification
6. Documentation

6.7 7. Reauthorization

Reauthorization Interval: [TODO: 3 years]
Next Reauthorization: [TODO: Date]

Reauthorization Triggers: - ATO expiration - Significant system changes - New threats - Compliance requirements

---

Document History:

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

ewpage

Chapter 7

Access Control Policy

Document-ID: NIST-0100
Control Family: Access Control (AC)
Control: AC-1
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

7.1 1. Control Description

AC-1 Policy and Procedures

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

7.2 2. Control Implementation

7.2.1 2.1 Access Control Policy

Policy Statement: [TODO: Describe organization's access control policy]

Scope: [TODO: Scope]
Roles and Responsibilities: [TODO: Roles]
Compliance: [TODO: Compliance requirements]

7.2.2 2.2 Access Control Procedures

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

7.3 3. Control Enhancements

[TODO: List applicable control enhancements]

7.4 4. Implementation Status

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

7.5 5. Assessment

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

Document History:

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

ewpage

Chapter 8

Account Management

Document-ID: NIST-0110
Control Family: Access Control (AC)
Control: AC-2
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

8.1 1. Control Description

AC-2 Account Management

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

8.2 2. Control Implementation

8.2.1 2.1 Account Types

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

8.2.2 2.2 Account Management Process

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

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

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

8.2.3 2.3 Account Monitoring

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

8.3 3. Control Enhancements

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

8.4 4. Implementation Status

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

8.5 5. Assessment

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

Document History:

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

ewpage

Chapter 9

Access Enforcement

Document ID: NIST-0120
Control Family: Access Control (AC)
Control: AC-3
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

9.1 1. Control Description

AC-3 Access Enforcement

The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

9.2 2. Control Implementation

9.2.1 2.1 Access Enforcement Mechanisms

Enforcement Methods: - Role-Based Access Control (RBAC) - Mandatory Access Control (MAC) - Discretionary Access Control (DAC) - Attribute-Based Access Control (ABAC)

[TODO: Describe implemented access control mechanisms]

9.2.2 2.2 Authorization Policies

Policy Framework: [TODO: Describe authorization policies]

Access Decision Criteria: - [TODO: Criterion 1] - [TODO: Criterion 2] - [TODO: Criterion 3]

9.2.3 2.3 Technical Implementation

System Components: [TODO: List of systems with access control]

Enforcement Points: [TODO: Description of enforcement points]

9.3 3. Control Enhancements

- **AC-3(1):** Restricted Access to Privileged Functions
- **AC-3(2):** Dual Authorization
- **AC-3(3):** Mandatory Access Control
- **AC-3(4):** Discretionary Access Control
- **AC-3(7):** Role-Based Access Control
- **AC-3(8):** Revocation of Access Authorizations

[TODO: Mark applicable enhancements]

9.4 4. Implementation Status

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

9.5 5. Assessment

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

Document History:

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

ewpage

Chapter 10

Information Flow Enforcement

Document ID: NIST-0130
Control Family: Access Control (AC)
Control: AC-4
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

10.1 1. Control Description

AC-4 Information Flow Enforcement

The information system enforces approved authorizations for controlling the flow of information within the system and between connected systems.

10.2 2. Control Implementation

10.2.1 2.1 Information Flow Policies

Flow Control Policies: [TODO: Describe information flow policies]

10.2.2 2.2 Flow Control Mechanisms

Technical Controls: - Network segmentation - Firewalls and security gateways - Data loss prevention (DLP) - Content filtering

[TODO: Describe implemented mechanisms]

10.2.3 2.3 Inter-System Connections

Connected Systems: [TODO: List connected systems and flow controls]

10.3 3. Control Enhancements

- **AC-4(1):** Object Security and Privacy Attributes
- **AC-4(2):** Processing Domains
- **AC-4(3):** Dynamic Information Flow Control
- **AC-4(4):** Flow Control of Encrypted Information
- **AC-4(8):** Security and Privacy Policy Filters

[TODO: Mark applicable enhancements]

10.4 4. Implementation Status

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

10.5 5. Assessment

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

Document History:

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

ewpage

Chapter 11

Separation of Duties

Document ID: NIST-0140
Control Family: Access Control (AC)
Control: AC-5
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

11.1 1. Control Description

AC-5 Separation of Duties

The organization separates duties of individuals to prevent malevolent activity without collusion and reduces the risk of malevolent activity without detection.

11.2 2. Control Implementation

11.2.1 2.1 Duty Separation Policy

Policy Statement: [TODO: Describe duty separation policy]

11.2.2 2.2 Separated Duties

Critical Functions: | Function | Role A | Role B | Justification | |———-|———|———|———————| | [TODO] | [TODO] | [TODO] | [TODO] |

11.2.3 2.3 Implementation Mechanisms

Technical Controls: - Role-based access control (RBAC) - Workflow approvals - Dual authorization requirements

[TODO: Describe implemented mechanisms]

11.3 3. Control Enhancements

- **AC-5(1):** Automated Separation of Duties

[TODO: Mark applicable enhancements]

11.4 4. Implementation Status

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

11.5 5. Assessment

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

Document History:

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

ewpage

Chapter 12

Least Privilege

Document ID: NIST-0150
Control Family: Access Control (AC)
Control: AC-6
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

12.1 1. Control Description

AC-6 Least Privilege

The organization employs the principle of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

12.2 2. Control Implementation

12.2.1 2.1 Least Privilege Policy

Policy Statement: [TODO: Describe least privilege policy]

12.2.2 2.2 Privilege Assignment

Privilege Levels: | Role | Privileges | Justification | |——|————|————| | [TODO] | [TODO] | [TODO] |

12.2.3 2.3 Privileged Account Management

Privileged Accounts: [TODO: List privileged accounts and their usage]

Access Controls: - Just-in-time (JIT) access - Privileged access management (PAM) - Time-limited privileges

[TODO: Describe implemented controls]

12.3 3. Control Enhancements

- **AC-6(1):** Authorize Access to Security Functions
- **AC-6(2):** Non-Privileged Access for Nonsecurity Functions
- **AC-6(3):** Network Access to Privileged Commands
- **AC-6(5):** Privileged Accounts
- **AC-6(7):** Review of User Privileges
- **AC-6(9):** Log Use of Privileged Functions
- **AC-6(10):** Prohibit Non-Privileged Users from Executing Privileged Functions

[TODO: Mark applicable enhancements]

12.4 4. Implementation Status

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

12.5 5. Assessment

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

Document History:

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

ewpage

Chapter 13

Security Awareness and Training

Document-ID: NIST-0200
Control Family: Awareness and Training (AT)
Control: AT-1, AT-2, AT-3, AT-4
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

13.1 1. Control Description

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

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

13.2 2. Control Implementation

13.2.1 2.1 Security Awareness Program

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

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

13.2.2 2.2 Role-Based Training

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

13.2.3 2.3 Training Records

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

13.3 3. Implementation Status

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

Document History:

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

ewpage

Chapter 14

Role-Based Training

Document ID: NIST-0210
Control Family: Awareness and Training (AT)
Control: AT-3
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

14.1 1. Control Description

AT-3 Role-Based Training

The organization provides role-based security and privacy training to personnel with assigned security roles and responsibilities.

14.2 2. Control Implementation

14.2.1 2.1 Role-Based Training Program

Training Requirements by Role: | Role | Training Topics | Frequency | Duration | |——|————————-|————|————-| | System Administrators | Secure configuration, patch management, access control | Annual | [TODO] | | Security Personnel | Threat analysis, incident response, forensics | Annual | [TODO] | | Developers | Secure coding, SDLC security, code review | Annual | [TODO] | | Managers | Risk management, compliance, policy enforcement | Annual | [TODO] | | [TODO] | [TODO] | [TODO] | [TODO] |

14.2.2 2.2 Training Content

Core Topics: - Role-specific security responsibilities - Applicable security policies and procedures - Security technologies and tools - Threat landscape and attack vectors - Incident reporting procedures

[TODO: Detail training content for each role]

14.2.3 2.3 Training Delivery

Delivery Methods: - Instructor-led training - Online courses - Workshops and labs - On-the-job training - Certification programs

[TODO: Specify delivery methods]

14.2.4 2.4 Training Records

Documentation: - Training completion records - Assessment results - Certification tracking - Refresher training schedule

[TODO: Describe record-keeping procedures]

14.3 3. Control Enhancements

- **AT-3(1):** Environmental Controls
- **AT-3(2):** Physical Security Controls
- **AT-3(3):** Practical Exercises
- **AT-3(4):** Suspicious Communications and Anomalous System Behavior
- **AT-3(5):** Processing Personally Identifiable Information

[TODO: Mark applicable enhancements]

14.4 4. Implementation Status

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

14.5 5. Assessment

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

Document History:

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

ewpage

Chapter 15

Audit and Accountability Policy

Document-ID: NIST-0220
Control Family: Audit and Accountability (AU)
Control: AU-1, AU-2, AU-3
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

15.1 1. Control Description

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

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

15.2 2. Control Implementation

15.2.1 2.1 Auditable Events

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

15.2.2 2.2 Audit Record Content

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

15.2.3 2.3 Audit Log Management

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

15.3 3. Implementation Status

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

Document History:

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

ewpage

Chapter 16

Audit Events

Document ID: NIST-0230
Control Family: Audit and Accountability (AU)
Control: AU-2
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

16.1 1. Control Description

AU-2 Audit Events

The organization determines that the information system is capable of auditing specified events and coordinates the security audit function with other organizational entities.

16.2 2. Control Implementation

16.2.1 2.1 Auditable Events

Event Categories: - Account management events - Authentication and authorization events - Privilege escalation events - System and application access events - Configuration changes - Security policy changes - Data access and modification - Network activity - System startup and shutdown

[TODO: Specify auditable events for your organization]

16.2.2 2.2 Event Selection Criteria

Selection Rationale: | Event Type | Rationale | Frequency | |————|————|————| | Failed login attempts | Detect unauthorized access attempts | Real-time | | Privilege changes | Monitor elevation of privileges | Real-time | | Configuration changes | Track system modifications | Real-time | | Data access | Monitor sensitive data access | Real-time | | [TODO] | [TODO] | [TODO] |

16.2.3 2.3 Audit Coordination

Coordination Activities: - Review audit requirements with stakeholders - Coordinate with incident response team - Align with compliance requirements - Integrate with SIEM systems

[TODO: Describe coordination procedures]

16.2.4 2.4 Audit Review and Updates

Review Schedule: [TODO: e.g., Quarterly]
Update Triggers: - New threats identified - Compliance requirement changes - Incident lessons learned - Technology changes

[TODO: Define review and update procedures]

16.3 3. Control Enhancements

- **AU-2(1):** Compilation of Audit Records from Multiple Sources
- **AU-2(2):** Selection of Audit Events by Component
- **AU-2(3):** Reviews and Updates
- **AU-2(4):** Privileged Functions

[TODO: Mark applicable enhancements]

16.4 4. Implementation Status

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

16.5 5. Assessment

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

Document History:

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

ewpage

Chapter 17

Audit Log Storage and Protection

Document ID: NIST-0240
Control Family: Audit and Accountability (AU)
Controls: AU-4, AU-9
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

17.1 1. Control Description

This document covers audit log storage and protection controls: - **AU-4:** Audit Log Storage Capacity - **AU-9:** Protection of Audit Information

17.2 2. Control Implementation

17.2.1 2.1 Audit Log Storage Capacity (AU-4)

Storage Requirements: - Estimated log volume: [TODO: e.g., GB per day] - Retention period: [TODO: e.g., 90 days online, 1 year archive] - Storage allocation: [TODO: Total capacity]

Capacity Planning: [TODO: Describe capacity planning procedures]

Monitoring: - Storage utilization alerts - Threshold: [TODO: e.g., 80% capacity] - Alert recipients: [TODO: List]

Overflow Handling: - Oldest logs archived - Critical alerts generated - Emergency storage expansion

[TODO: Define overflow procedures]

17.2.2 2.2 Protection of Audit Information (AU-9)

Access Controls: - Read access: [TODO: Authorized roles] - Write access: System only (no manual modification) - Delete access: [TODO: Authorized roles with approval]

Protection Mechanisms: - Write-once storage - Cryptographic hashing - Digital signatures - Access logging - Backup and replication

[TODO: Specify protection mechanisms]

Physical Protection: [TODO: Describe physical security measures for audit storage]

Backup Procedures: - Backup frequency: [TODO: e.g., Daily] - Backup retention: [TODO: e.g., 1 year] - Backup location: [TODO: Off-site/cloud] - Backup verification: [TODO: Procedures]

17.3 3. Control Enhancements

- **AU-4(1):** Transfer to Alternate Storage
- **AU-9(1):** Hardware Write-Once Media
- **AU-9(2):** Store on Separate Physical Systems or Components
- **AU-9(3):** Cryptographic Protection
- **AU-9(4):** Access by Subset of Privileged Users
- **AU-9(5):** Dual Authorization
- **AU-9(6):** Read-Only Access
- **AU-9(7):** Store on Component with Different Operating System

[TODO: Mark applicable enhancements]

17.4 4. Implementation Status

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

17.5 5. Assessment

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

Document History:

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

ewpage

Chapter 18

Audit Review and Analysis

Document ID: NIST-0250
Control Family: Audit and Accountability (AU)
Controls: AU-6, AU-7
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

18.1 1. Control Description

This document covers audit review and analysis controls: - **AU-6:** Audit Record Review, Analysis, and Reporting - **AU-7:** Audit Record Reduction and Report Generation

18.2 2. Control Implementation

18.2.1 2.1 Audit Record Review, Analysis, and Reporting (AU-6)

Review Schedule: - Continuous automated monitoring - Daily review of critical systems - Weekly review of all systems - Monthly comprehensive analysis

[TODO: Define review schedule]

Review Responsibilities: | System/Application | Reviewer | Frequency | |———————-|———-|————| | [TODO] | [TODO] | [TODO] |

Analysis Activities: - Anomaly detection - Pattern recognition - Correlation analysis - Trend analysis - Compliance verification

[TODO: Describe analysis procedures]

Reporting: - Incident reports - Compliance reports - Trend reports - Executive summaries

[TODO: Define reporting requirements]

Response Procedures: [TODO: Describe procedures for responding to audit findings]

18.2.2 2.2 Audit Record Reduction and Report Generation (AU-7)

Reduction Capabilities: - Filtering by event type - Filtering by time period - Filtering by user/system - Filtering by severity - Custom queries

[TODO: Specify reduction capabilities]

Report Types: - Security incident reports - Compliance reports - User activity reports - System access reports - Configuration change reports

[TODO: Define report types and templates]

Automated Reporting: - Scheduled reports - Alert-triggered reports - On-demand reports

[TODO: Configure automated reporting]

18.3 3. Control Enhancements

- **AU-6(1):** Automated Process Integration
- **AU-6(3):** Correlate Audit Record Repositories
- **AU-6(4):** Central Review and Analysis
- **AU-6(5):** Integrated Analysis of Audit Records
- **AU-6(6):** Correlation with Physical Monitoring
- **AU-6(7):** Permitted Actions
- **AU-6(9):** Correlation with Information from Nontechnical Sources
- **AU-6(10):** Audit Level Adjustment
- **AU-7(1):** Automatic Processing
- **AU-7(2):** Automatic Sort and Search

[TODO: Mark applicable enhancements]

18.4 4. Implementation Status

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

18.5 5. Assessment

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

Document History:

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

ewpage

Chapter 19

Configuration Management Policy

Document-ID: NIST-0300
Control Family: Configuration Management (CM)
Control: CM-1, CM-2, CM-3
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

19.1 1. Control Description

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

The organization establishes and maintains baseline configurations and controls changes.

19.2 2. Control Implementation

19.2.1 2.1 Baseline Configuration

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

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

19.2.2 2.2 Configuration Change Control

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

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

19.2.3 2.3 Configuration Monitoring

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

Review Frequency: [TODO: Weekly / Monthly]

19.3 3. Implementation Status

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

Document History:

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

ewpage

Chapter 20

Configuration Baseline and Settings

Document ID: NIST-0310
Control Family: Configuration Management (CM)
Controls: CM-2, CM-6, CM-7
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

20.1 1. Control Description

This document covers configuration baseline and settings controls: - **CM-2:** Baseline Configuration - **CM-6:** Configuration Settings - **CM-7:** Least Functionality

20.2 2. Control Implementation

20.2.1 2.1 Baseline Configuration (CM-2)

Baseline Components: - Operating system configurations - Application configurations - Network device configurations - Security tool configurations - Database configurations

[TODO: Define baseline components]

Baseline Documentation: | System/Component | Baseline Version | Last Updated | Owner | |———————|———————|———————|——-| | [TODO] | [TODO] | [TODO] | [TODO] |

Baseline Review: - Review frequency: [TODO: e.g., Annually or upon significant changes] - Approval authority: [TODO: Role/Committee] - Update procedures: [TODO: Process]

20.2.2 2.2 Configuration Settings (CM-6)

Mandatory Configuration Settings: | Setting Category | Requirement | Rationale | |———————|———————|———————| | Password policy | Minimum 12 characters, complexity required | Security

best practice | | Session timeout | 15 minutes inactivity | Prevent unauthorized access | | Encryption | TLS 1.2 or higher | Data protection | | Logging | All security events | Audit trail | | [TODO] | [TODO] | [TODO] |

Configuration Standards: - CIS Benchmarks - DISA STIGs - Vendor hardening guides - Organization-specific standards

[TODO: Specify applicable standards]

Configuration Verification: - Automated scanning tools - Manual reviews - Compliance checks

[TODO: Define verification procedures]

20.2.3 2.3 Least Functionality (CM-7)

Prohibited Functions: - Unnecessary services - Unused protocols - Deprecated features - Development tools on production systems - Guest accounts

[TODO: List prohibited functions]

Allowed Functions: [TODO: Define allowed functions and justification]

Review Process: - Periodic functionality reviews - Exception approval process - Documentation requirements

[TODO: Define review process]

20.3 3. Control Enhancements

- **CM-2(1):** Reviews and Updates
- **CM-2(2):** Automation Support for Accuracy and Currency
- **CM-2(3):** Retention of Previous Configurations
- **CM-2(6):** Development and Test Environments
- **CM-2(7):** Configure Systems and Components for High-Risk Areas
- **CM-6(1):** Automated Management, Application, and Verification
- **CM-6(2):** Respond to Unauthorized Changes
- **CM-7(1):** Periodic Review
- **CM-7(2):** Prevent Program Execution
- **CM-7(5):** Authorized Software - Allow by Exception

[TODO: Mark applicable enhancements]

20.4 4. Implementation Status

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

20.5 5. Assessment

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

Findings: [TODO: Description]

Document History:

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

ewpage

Chapter 21

Configuration Change Control

Document ID: NIST-0320
Control Family: Configuration Management (CM)
Controls: CM-3, CM-4, CM-5
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

21.1 1. Control Description

This document covers configuration change control: - **CM-3:** Configuration Change Control - **CM-4:** Impact Analyses - **CM-5:** Access Restrictions for Change

21.2 2. Control Implementation

21.2.1 2.1 Configuration Change Control (CM-3)

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

[TODO: Detail change control process]

Change Types: | Change Type | Approval Authority | Timeline | |————-|————————-|————-| | Emergency | [TODO: Role] | Immediate with post-implementation review | | Standard | [TODO: Committee] | [TODO: e.g., 5 business days] | | Normal | [TODO: Role] | [TODO: e.g., 10 business days] |

Change Advisory Board (CAB): - Members: [TODO: List members] - Meeting frequency: [TODO: e.g., Weekly] - Responsibilities: [TODO: Define]

21.2.2 2.2 Impact Analyses (CM-4)

Analysis Requirements: - Security impact assessment - Operational impact assessment - Compliance impact assessment - Performance impact assessment - Rollback planning

[TODO: Define analysis requirements]

Impact Assessment Template: | Assessment Area | Impact Level | Mitigation | |———————-|———————|———————| | Security | [High/Medium/Low] | [TODO] | | Operations | [High/Medium/Low] | [TODO] | | Compliance | [High/Medium/Low] | [TODO] | | Performance | [High/Medium/Low] | [TODO] |

21.2.3 2.3 Access Restrictions for Change (CM-5)

Access Controls: - Production environment access limited to authorized personnel - Change implementation requires approval - Separation of duties enforced - All changes logged and audited

[TODO: Define access restrictions]

Authorized Personnel: | Name/Role | Systems | Change Types | Approval Required | |———————|———————|———————|———————-| | [TODO] | [TODO] | [TODO] | [TODO] |

Physical Access: [TODO: Define physical access restrictions for change implementation]

Logical Access: [TODO: Define logical access restrictions]

21.3 3. Control Enhancements

- **CM-3(1):** Automated Documentation, Notification, and Prohibition of Changes
- **CM-3(2):** Testing, Validation, and Documentation of Changes
- **CM-3(4):** Security and Privacy Representatives
- **CM-3(6):** Cryptography Management
- **CM-4(1):** Separate Test Environments
- **CM-4(2):** Verification of Controls
- **CM-5(1):** Automated Access Enforcement and Audit Records
- **CM-5(3):** Signed Components
- **CM-5(5):** Privilege Limitation for Production and Operation
- **CM-5(6):** Limit Library Privileges

[TODO: Mark applicable enhancements]

21.4 4. Implementation Status

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

21.5 5. Assessment

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

Findings: [TODO: Description]

Document History:

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

ewpage

Chapter 22

Contingency Planning Policy

Document-ID: NIST-0330
Control Family: Contingency Planning (CP)
Control: CP-1, CP-2, CP-9
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

22.1 1. Control Description

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

The organization develops and maintains contingency plans and backup procedures.

22.2 2. Control Implementation

22.2.1 2.1 Contingency Plan

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

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

22.2.2 2.2 Backup Procedures

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

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

Backup Testing: [TODO: Quarterly]

22.2.3 2.3 Contingency Plan Testing

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

22.3 3. Implementation Status

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

Document History:

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

ewpage

Chapter 23

Contingency Plan and Alternate Sites

Document ID: NIST-0340
Control Family: Contingency Planning (CP)
Controls: CP-2, CP-6, CP-7
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

23.1 1. Control Description

This document covers contingency planning and alternate site controls: - **CP-2:** Contingency Plan - **CP-6:** Alternate Storage Site - **CP-7:** Alternate Processing Site

23.2 2. Control Implementation

23.2.1 2.1 Contingency Plan (CP-2)

Plan Components: - Essential missions and business functions - Recovery objectives (RTO/RPO) - Restoration priorities - Roles and responsibilities - Contact information - Alternate facilities - Recovery procedures - Technical contingency operations

[TODO: Develop comprehensive contingency plan]

Plan Distribution: - Key personnel: [TODO: List] - Alternate storage location: [TODO: Location] - Access controls: [TODO: Define]

Plan Review and Updates: - Review frequency: [TODO: e.g., Annually] - Update triggers: [TODO: List triggers] - Approval authority: [TODO: Role]

Plan Testing: - Test frequency: [TODO: e.g., Annually] - Test types: Tabletop, functional, full-scale - Test documentation: [TODO: Requirements]

23.2.2 2.2 Alternate Storage Site (CP-6)

Storage Site Details: - Location: [TODO: Geographic location] - Type: Hot/Warm/Cold site - Distance from primary: [TODO: Miles/km] - Capacity: [TODO: Storage capacity]

Data Replication: - Replication method: [TODO: Synchronous/Asynchronous] - Replication frequency: [TODO: Real-time/Scheduled] - Data types replicated: [TODO: List]

Access and Security: - Physical security: [TODO: Measures] - Logical access controls: [TODO: Controls] - Environmental controls: [TODO: Requirements]

Agreements: - Service level agreements (SLAs) - Recovery time objectives - Testing requirements

[TODO: Document agreements]

23.2.3 2.3 Alternate Processing Site (CP-7)

Processing Site Details: - Location: [TODO: Geographic location] - Type: Hot/Warm/Cold site - Distance from primary: [TODO: Miles/km] - Capacity: [TODO: Processing capacity]

Site Capabilities: - Computing resources - Network connectivity - Environmental controls - Physical security - Support personnel

[TODO: Detail site capabilities]

Activation Procedures: 1. Declaration of disaster 2. Notification of personnel 3. Site activation 4. Data restoration 5. Service restoration 6. Verification and testing

[TODO: Define activation procedures]

Agreements: [TODO: Document agreements with alternate site provider]

23.3 3. Control Enhancements

- **CP-2(1):** Coordinate with Related Plans
- **CP-2(2):** Capacity Planning
- **CP-2(3):** Resume Mission and Business Functions
- **CP-2(4):** Resume All Mission and Business Functions
- **CP-2(5):** Continue Mission and Business Functions
- **CP-2(8):** Identify Critical Assets
- **CP-6(1):** Separation from Primary Site
- **CP-6(2):** Recovery Time and Recovery Point Objectives
- **CP-6(3):** Accessibility
- **CP-7(1):** Separation from Primary Site
- **CP-7(2):** Accessibility
- **CP-7(3):** Priority of Service
- **CP-7(4):** Preparation for Use
- **CP-7(6):** Inability to Return to Primary Site

[TODO: Mark applicable enhancements]

23.4 4. Implementation Status

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

23.5 5. Assessment

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

Document History:

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

ewpage

Chapter 24

System Backup and Recovery

Document ID: NIST-0350
Control Family: Contingency Planning (CP)
Controls: CP-9, CP-10
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

24.1 1. Control Description

This document covers system backup and recovery controls: - **CP-9:** System Backup - **CP-10:** System Recovery and Reconstitution

24.2 2. Control Implementation

24.2.1 2.1 System Backup (CP-9)

Backup Types: | Backup Type | Frequency | Retention | Storage Location | |————-|————–|————|————–| | Full backup | [TODO: e.g., Weekly] | [TODO: e.g., 4 weeks] | [TODO: Location] | | Incremental backup | [TODO: e.g., Daily] | [TODO: e.g., 1 week] | [TODO: Location] | | Differential backup | [TODO: e.g., Daily] | [TODO: e.g., 1 week] | [TODO: Location] |

Backup Scope: - User-level information - System-level information - System state information - Application data - Configuration files - Documentation

[TODO: Define backup scope]

Backup Procedures: 1. Initiate backup 2. Verify backup completion 3. Test backup integrity 4. Transfer to alternate storage 5. Document backup

[TODO: Detail backup procedures]

Backup Protection: - Encryption at rest - Encryption in transit - Access controls - Physical security - Integrity verification

[TODO: Specify protection measures]

Backup Testing: - Test frequency: [TODO: e.g., Quarterly] - Test procedures: [TODO: Define] - Success criteria: [TODO: Define]

24.2.2 2.2 System Recovery and Reconstitution (CP-10)

Recovery Procedures: 1. Assess damage 2. Activate recovery team 3. Restore from backup 4. Verify system integrity 5. Resume operations 6. Document recovery

[TODO: Detail recovery procedures]

Recovery Time Objectives (RTO): | System/Application | RTO | Priority | |———————-|———-| | [TODO] | [TODO] | [High/Medium/Low] |

Recovery Point Objectives (RPO): | System/Application | RPO | Data Loss Tolerance | |———————-|———-|———————| | [TODO] | [TODO] | [TODO] |

Reconstitution: - Deactivate alternate processing site - Restore primary site - Migrate operations back to primary - Verify full functionality - Document lessons learned

[TODO: Define reconstitution procedures]

Transaction Recovery: [TODO: Define procedures for recovering incomplete transactions]

24.3 3. Control Enhancements

- **CP-9(1):** Testing for Reliability and Integrity
- **CP-9(2):** Test Restoration Using Sampling
- **CP-9(3):** Separate Storage for Critical Information
- **CP-9(5):** Transfer to Alternate Storage Site
- **CP-9(6):** Redundant Secondary System
- **CP-9(7):** Dual Authorization for Deletion or Destruction
- **CP-9(8):** Cryptographic Protection
- **CP-10(2):** Transaction Recovery
- **CP-10(4):** Restore Within Time Period
- **CP-10(6):** Component Protection

[TODO: Mark applicable enhancements]

24.4 4. Implementation Status

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

24.5 5. Assessment

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

Document History:

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

ewpage

Chapter 25

Identification and Authentication Policy

Document-ID: NIST-0400
Control Family: Identification and Authentication (IA)
Control: IA-1, IA-2, IA-5
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

25.1 1. Control Description

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

The organization uniquely identifies and authenticates users.

25.2 2. Control Implementation

25.2.1 2.1 User Identification

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

25.2.2 2.2 Authentication Methods

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

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

25.2.3 2.3 Password Requirements

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

25.2.4 2.4 Authenticator Management

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

25.3 3. Implementation Status

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

Document History:

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

ewpage

Chapter 26

User and Device Authentication

Document ID: NIST-0410
Control Family: Identification and Authentication (IA)
Controls: IA-2, IA-3, IA-4, IA-6, IA-8
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

26.1 1. Control Description

This document covers user and device authentication controls: - **IA-2:** Identification and Authentication (Organizational Users) - **IA-3:** Device Identification and Authentication - **IA-4:** Identifier Management - **IA-6:** Authentication Feedback - **IA-8:** Identification and Authentication (Non-Organizational Users)

26.2 2. Control Implementation

26.2.1 2.1 User Authentication (IA-2)

Authentication Methods: - Username and password - Multi-factor authentication (MFA) - Biometric authentication - Smart cards/tokens - Certificate-based authentication

[TODO: Specify authentication methods by system/application]

MFA Requirements: | System/Application | MFA Required | MFA Type | |——————-|———-|———-| | [TODO] | Yes/No | [TODO: SMS, App, Hardware token] |

26.2.2 2.2 Device Authentication (IA-3)

Device Types: - Workstations - Servers - Mobile devices - Network devices - IoT devices

[TODO: Define device authentication requirements]

Authentication Mechanisms: - Device certificates - MAC address filtering - Network access control (NAC) - Device registration

[TODO: Specify mechanisms]

26.2.3 2.3 Identifier Management (IA-4)

Identifier Assignment: - Unique identifiers for each user - Naming conventions: [TODO: Define] - Identifier reuse policy: [TODO: Define]

Identifier Lifecycle: 1. Creation 2. Assignment 3. Modification 4. Suspension 5. Deletion

[TODO: Define lifecycle procedures]

Identifier Types: | Identifier Type | Format | Example | |———————-|———|———| | User ID | [TODO] | [TODO] | | Service Account | [TODO] | [TODO] | | Device ID | [TODO] | [TODO] |

26.2.4 2.4 Authentication Feedback (IA-6)

Feedback Restrictions: - No password display during entry - Generic error messages for failed authentication - No indication of which credential failed - Masking of authentication information

[TODO: Define feedback restrictions]

26.2.5 2.5 Non-Organizational User Authentication (IA-8)

External User Types: - Contractors - Partners - Customers - Vendors - Public users

[TODO: Define external user types]

Authentication Requirements: | User Type | Authentication Method | Access Level | |———— |———————-|————| | [TODO] | [TODO] | [TODO] |

Federated Authentication: - Supported identity providers: [TODO: List] - Federation protocols: SAML, OAuth, OpenID Connect - Trust relationships: [TODO: Define]

26.3 3. Control Enhancements

- **IA-2(1):** Multi-Factor Authentication to Privileged Accounts
- **IA-2(2):** Multi-Factor Authentication to Non-Privileged Accounts
- **IA-2(5):** Individual Authentication with Group Authentication
- **IA-2(6):** Access to Accounts - Separate Device
- **IA-2(8):** Access to Accounts - Replay Resistant
- **IA-2(12):** Acceptance of PIV Credentials
- **IA-3(1):** Cryptographic Bidirectional Authentication
- **IA-3(4):** Device Attestation
- **IA-4(4):** Identify User Status
- **IA-8(1):** Acceptance of PIV Credentials from Other Agencies
- **IA-8(2):** Acceptance of External Authenticators
- **IA-8(4):** Use of Defined Profiles

[TODO: Mark applicable enhancements]

26.4 4. Implementation Status

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

26.5 5. Assessment

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

Document History:

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

ewpage

Chapter 27

Authenticator Management

Document ID: NIST-0420
Control Family: Identification and Authentication (IA)
Controls: IA-5, IA-7
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

27.1 1. Control Description

This document covers authenticator management controls: - **IA-5:** Authenticator Management - **IA-7:** Cryptographic Module Authentication

27.2 2. Control Implementation

27.2.1 2.1 Authenticator Management (IA-5)

Password Requirements: - Minimum length: [TODO: e.g., 12 characters] - Complexity: [TODO: e.g., Upper, lower, number, special character] - Maximum age: [TODO: e.g., 90 days] - Password history: [TODO: e.g., Last 12 passwords] - Account lockout: [TODO: e.g., 5 failed attempts]

Initial Authenticator Distribution: - Secure delivery method - Temporary password requirements - Forced change on first use - Verification of recipient identity

[TODO: Define distribution procedures]

Authenticator Types: | Type | Use Case | Strength | Lifecycle | |——|———-|———-|———| | Password | Standard access | Medium | [TODO] | | MFA token | Privileged access | High | [TODO] | | Certificate | System-to-system | High | [TODO] | | Biometric | Physical access | High | N/A |

Authenticator Protection: - Encrypted storage - Secure transmission - Protection against replay attacks - Secure backup and recovery

[TODO: Define protection measures]

Authenticator Lifecycle: 1. Generation/issuance 2. Distribution 3. Activation 4. Renewal 5. Revocation 6. Destruction

[TODO: Detail lifecycle procedures]

Compromised Authenticators: - Reporting procedures - Immediate revocation - Investigation - Reissuance - Documentation

[TODO: Define procedures]

27.2.2 2.2 Cryptographic Module Authentication (IA-7)

Cryptographic Modules: - Hardware security modules (HSMs) - Trusted platform modules (TPMs) - Smart cards - USB tokens

[TODO: List cryptographic modules in use]

Authentication Requirements: - FIPS 140-2/140-3 validated modules - Certificate-based authentication - Strong cryptographic algorithms - Key management procedures

[TODO: Define requirements]

Module Management: - Procurement standards - Configuration requirements - Monitoring and logging - Decommissioning procedures

[TODO: Define management procedures]

27.3 3. Control Enhancements

- **IA-5(1):** Password-Based Authentication
- **IA-5(2):** Public Key-Based Authentication
- **IA-5(3):** In-Person or Trusted External Party Registration
- **IA-5(4):** Automated Support for Password Strength Determination
- **IA-5(6):** Protection of Authenticators
- **IA-5(7):** No Embedded Unencrypted Static Authenticators
- **IA-5(8):** Multiple System Accounts
- **IA-5(9):** Federated Credential Management
- **IA-5(10):** Dynamic Credential Binding
- **IA-5(13):** Expiration of Cached Authenticators
- **IA-5(15):** GSA-Approved Products and Services
- **IA-5(18):** Password Managers

[TODO: Mark applicable enhancements]

27.4 4. Implementation Status

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

27.5 5. Assessment

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

Document History:

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

ewpage

Chapter 28

Incident Response Policy

Document-ID: NIST-0430
Control Family: Incident Response (IR)
Control: IR-1, IR-4, IR-5, IR-6
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

28.1 1. Control Description

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

The organization implements incident response capabilities.

28.2 2. Control Implementation

28.2.1 2.1 Incident Response Process

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

28.2.2 2.2 Incident Categories

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

Category	Severity	Response Time	Escalation
Minor	Low	4 hours	ISSO

28.2.3 2.3 Incident Response Team

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

28.2.4 2.4 Incident Reporting

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

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

28.2.5 2.5 Incident Documentation

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

28.3 3. Implementation Status

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

Document History:

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

ewpage

Chapter 29

Incident Handling and Assistance

Document ID: NIST-0440
Control Family: Incident Response (IR)
Controls: IR-4, IR-7
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

29.1 1. Control Description

This document covers incident handling and assistance controls: - **IR-4:** Incident Handling - **IR-7:** Incident Response Assistance

29.2 2. Control Implementation

29.2.1 2.1 Incident Handling (IR-4)

Incident Handling Process: 1. **Preparation** - Incident response team established - Tools and resources available - Training completed

2. **Detection and Analysis**
   - Incident identification
   - Incident categorization
   - Incident prioritization
3. **Containment, Eradication, and Recovery**
   - Short-term containment
   - Long-term containment
   - Eradication of threat
   - System recovery
4. **Post-Incident Activity**
   - Lessons learned

- Evidence retention
- Documentation

[TODO: Detail incident handling procedures]

Incident Categories: | Category | Severity | Response Time | Escalation | |———-|———-|———-|———-| | Data breach | Critical | Immediate | [TODO] | | Malware infection | High | 1 hour | [TODO] | | Unauthorized access | High | 1 hour | [TODO] | | DoS attack | Medium | 4 hours | [TODO] | | Policy violation | Low | 24 hours | [TODO] |

Incident Response Team: | Role | Name | Contact | Responsibilities | |——|——|———|———-| | IR Manager | [TODO] | [TODO] | Overall coordination | | Security Analyst | [TODO] | [TODO] | Analysis and investigation | | System Administrator | [TODO] | [TODO] | System recovery | | Legal Counsel | [TODO] | [TODO] | Legal guidance | | Communications | [TODO] | [TODO] | Stakeholder communication |

Incident Tracking: - Incident ticketing system - Status tracking - Timeline documentation - Evidence collection

[TODO: Define tracking procedures]

Information Sharing: - Internal stakeholders - External partners - Law enforcement - Regulatory bodies - Information sharing organizations (ISAOs)

[TODO: Define sharing procedures]

29.2.2 2.2 Incident Response Assistance (IR-7)

Assistance Resources: - Internal security team - Managed security service provider (MSSP) - Incident response retainer - Forensics specialists - Legal counsel

[TODO: List available resources]

Contact Information: | Resource | Contact | Availability | Scope | |———-|———|————|——-| | [TODO] | [TODO] | [TODO] | [TODO] |

Assistance Procedures: 1. Assess need for assistance 2. Contact appropriate resource 3. Provide incident details 4. Coordinate response activities 5. Document assistance provided

[TODO: Define procedures]

External Coordination: - US-CERT - Industry ISACs - Law enforcement - Cloud service providers - Vendors

[TODO: Define coordination procedures]

29.3 3. Control Enhancements

- **IR-4(1):** Automated Incident Handling Processes
- **IR-4(2):** Dynamic Reconfiguration
- **IR-4(3):** Continuity of Operations
- **IR-4(4):** Information Correlation
- **IR-4(6):** Insider Threats
- **IR-4(8):** Correlation with External Organizations

- **IR-4(10):** Supply Chain Coordination
- **IR-7(1):** Automation Support for Availability of Information and Support
- **IR-7(2):** Coordination with External Providers

[TODO: Mark applicable enhancements]

29.4 4. Implementation Status

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

29.5 5. Assessment

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

Document History:

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

ewpage

Chapter 30

Incident Monitoring and Reporting

Document ID: NIST-0450
Control Family: Incident Response (IR)
Controls: IR-5, IR-6
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

30.1 1. Control Description

This document covers incident monitoring and reporting controls: - **IR-5:** Incident Monitoring - **IR-6:** Incident Reporting

30.2 2. Control Implementation

30.2.1 2.1 Incident Monitoring (IR-5)

Monitoring Capabilities: - Real-time security event monitoring - Automated incident detection - Threat intelligence integration - Anomaly detection - User behavior analytics

[TODO: Define monitoring capabilities]

Monitoring Tools: | Tool | Purpose | Coverage | |——|———|———-| | SIEM | Event correlation | Enterprise-wide | | IDS/IPS | Network intrusion detection | Network perimeter | | EDR | Endpoint threat detection | All endpoints | | [TODO] | [TODO] | [TODO] |

Monitoring Metrics: - Number of incidents detected - Mean time to detect (MTTD) - Mean time to respond (MTTR) - False positive rate - Incident trends

[TODO: Define metrics and targets]

Incident Tracking: - Incident ID assignment - Status tracking - Timeline documentation - Resource allocation - Resolution tracking

[TODO: Define tracking procedures]

30.2.2 2.2 Incident Reporting (IR-6)

Internal Reporting: - Incident response team - Management - Legal counsel - Human resources - Affected business units

[TODO: Define internal reporting procedures]

Reporting Timeline: | Incident Severity | Initial Report | Status Updates | Final Report | |———————|——————-|——————-|——————| | Critical | Immediate | Every 2 hours | Within 24 hours | | High | Within 1 hour | Daily | Within 3 days | | Medium | Within 4 hours | As needed | Within 7 days | | Low | Within 24 hours | As needed | Within 14 days |

External Reporting: - Regulatory requirements - Law enforcement - US-CERT - Affected parties - Business partners

[TODO: Define external reporting requirements]

Reporting Requirements by Incident Type: | Incident Type | Internal | External | Regulatory | Timeline | |———————|————-|————-|———————|————-| | Data breach | Yes | Yes | Yes | [TODO] | | Ransomware | Yes | Yes | Yes | [TODO] | | Insider threat | Yes | Maybe | Maybe | [TODO] | | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] |

Report Content: - Incident description - Impact assessment - Timeline of events - Response actions taken - Current status - Recommendations

[TODO: Define report templates]

Automated Reporting: - Automated alert generation - Report distribution - Escalation notifications - Status updates

[TODO: Configure automated reporting]

30.3 3. Control Enhancements

- **IR-5(1):** Automated Tracking, Data Collection, and Analysis
- **IR-6(1):** Automated Reporting
- **IR-6(2):** Vulnerabilities Related to Incidents
- **IR-6(3):** Supply Chain Coordination

[TODO: Mark applicable enhancements]

30.4 4. Implementation Status

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

30.5 5. Assessment

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

Document History:

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

ewpage

Chapter 31

System Maintenance

Document-ID: NIST-0500
Control Family: Maintenance (MA)
Control: MA-1, MA-2, MA-4, MA-5
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

31.1 1. Control Description

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

The organization performs system maintenance in a controlled manner.

31.2 2. Control Implementation

31.2.1 2.1 Maintenance Policy

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

Maintenance Schedule: [TODO: Schedule]

31.2.2 2.2 Maintenance Procedures

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

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

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

31.2.3 2.3 Remote Maintenance

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

31.3 3. Implementation Status

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

Document History:

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

ewpage

Chapter 32

Media Protection Policy

Document ID: NIST-0510
Control Family: Media Protection (MP)
Control: MP-1
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

32.1 1. Control Description

MP-1 Policy and Procedures

The organization develops, documents, and disseminates media protection policy and procedures.

32.2 2. Control Implementation

32.2.1 2.1 Media Protection Policy

Policy Statement: [TODO: Describe the organization's media protection policy]

Scope: [TODO: Scope]
Roles and Responsibilities: [TODO: Roles]
Compliance: [TODO: Compliance requirements]

32.2.2 2.2 Media Types

Protected Media: - Digital media (USB drives, external hard drives, SSDs) - Optical media (CDs, DVDs, Blu-ray) - Magnetic media (backup tapes) - Paper documents - Mobile devices

[TODO: Specify relevant media types]

32.2.3 2.3 Media Protection Procedures

Procedures: - Media access control - Media marking and labeling - Media storage and transport - Media sanitization and disposal

[TODO: Detail the procedures]

32.3 3. Control Enhancements

[TODO: List applicable control enhancements]

32.4 4. Implementation Status

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

32.5 5. Assessment

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

Document History:

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

ewpage

Chapter 33

Media Access and Sanitization

Document ID: NIST-0520
Control Family: Media Protection (MP)
Controls: MP-2, MP-3, MP-4, MP-5, MP-6, MP-7
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

33.1 1. Control Description

This document covers multiple media protection controls: - **MP-2:** Media Access - **MP-3:** Media Marking - **MP-4:** Media Storage - **MP-5:** Media Transport - **MP-6:** Media Sanitization - **MP-7:** Media Use

33.2 2. Control Implementation

33.2.1 2.1 Media Access (MP-2)

Access Controls: [TODO: Describe access control mechanisms for media]

Authorization Process: [TODO: Describe authorization process]

33.2.2 2.2 Media Marking (MP-3)

Marking Requirements: - Classification labels - Handling instructions - Distribution limitations

[TODO: Specify marking requirements]

33.2.3 2.3 Media Storage (MP-4)

Storage Requirements: - Physical security controls - Environmental controls - Access logging

[TODO: Describe storage requirements]

33.2.4 2.4 Media Transport (MP-5)

Transport Procedures: - Encryption requirements - Chain of custody - Approved carriers

[TODO: Detail transport procedures]

33.2.5 2.5 Media Sanitization (MP-6)

Sanitization Methods: | Media Type | Method | Standard | |————|——|———-| | Hard Drives | Cryptographic Erase / Physical Destruction | NIST SP 800-88 | | SSDs | Cryptographic Erase / Physical Destruction | NIST SP 800-88 | | USB Drives | Overwrite / Physical Destruction | NIST SP 800-88 | | Optical Media | Physical Destruction | NIST SP 800-88 | | Paper | Shredding / Pulping | Cross-cut P-4 or higher |

[TODO: Specify sanitization methods]

33.2.6 2.6 Media Use (MP-7)

Usage Restrictions: - Approved media types - Prohibited uses - Monitoring requirements

[TODO: Define usage restrictions]

33.3 3. Control Enhancements

- **MP-2(1):** Automated Restricted Access
- **MP-3(1):** Automated Marking
- **MP-4(1):** Cryptographic Protection
- **MP-5(4):** Cryptographic Protection
- **MP-6(1):** Review, Approve, Track, Document, and Verify
- **MP-6(2):** Equipment Testing
- **MP-6(3):** Nondestructive Techniques
- **MP-7(1):** Prohibit Use Without Owner

[TODO: Mark applicable enhancements]

33.4 4. Implementation Status

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

33.5 5. Assessment

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

Document History:

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

ewpage

Chapter 34

Physical and Environmental Protection Policy

Document ID: NIST-0530
Control Family: Physical and Environmental Protection (PE)
Control: PE-1
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

34.1 1. Control Description

PE-1 Policy and Procedures

The organization develops, documents, and disseminates physical and environmental protection policy and procedures.

34.2 2. Control Implementation

34.2.1 2.1 Physical Protection Policy

Policy Statement: [TODO: Describe the organization's physical protection policy]

Scope: [TODO: Scope - data centers, offices, etc.]
Roles and Responsibilities: [TODO: Roles]
Compliance: [TODO: Compliance requirements]

34.2.2 2.2 Protected Facilities

Facility Types: - Data centers - Server rooms - Network equipment rooms - Office spaces - Storage areas

[TODO: Specify protected facilities]

34.2.3 2.3 Physical Protection Procedures

Procedures: - Physical access control - Visitor management - Environmental monitoring - Emergency procedures

[TODO: Detail the procedures]

34.3 3. Control Enhancements

[TODO: List applicable control enhancements]

34.4 4. Implementation Status

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

34.5 5. Assessment

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

Document History:

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

ewpage

Chapter 35

Physical Access Control

Document ID: NIST-0540
Control Family: Physical and Environmental Protection (PE)
Controls: PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

35.1 1. Control Description

This document covers multiple physical access control controls: - **PE-2:** Physical Access Authorizations - **PE-3:** Physical Access Control - **PE-4:** Access Control for Transmission - **PE-5:** Access Control for Output Devices - **PE-6:** Monitoring Physical Access - **PE-8:** Visitor Access Records

35.2 2. Control Implementation

35.2.1 2.1 Physical Access Authorizations (PE-2)

Authorization Process: [TODO: Describe authorization process for physical access]

Authorized Personnel: | Name/Role | Facility | Access Level | Valid Until | |————|————-|————|————-| | [TODO] | [TODO] | [TODO] | [TODO] |

35.2.2 2.2 Physical Access Control (PE-3)

Access Control Mechanisms: - Badge readers - Biometric systems - Security guards - Mantrap/airlock entries - Turnstiles

[TODO: Describe implemented mechanisms]

Access Points: [TODO: List all controlled access points]

35.2.3 2.3 Access Control for Transmission (PE-4)

Transmission Medium Protection: - Cable conduits - Locked telecommunications rooms - Fiber optic cables - Wireless signal containment

[TODO: Describe protection measures for transmission media]

35.2.4 2.4 Access Control for Output Devices (PE-5)

Output Device Controls: - Printer access controls - Secure print release - Output device monitoring - Disposal procedures

[TODO: Specify controls for output devices]

35.2.5 2.5 Monitoring Physical Access (PE-6)

Monitoring Systems: - CCTV surveillance - Access logs - Intrusion detection systems - Security patrols

[TODO: Describe monitoring systems]

Log Retention: [TODO: Retention period]

35.2.6 2.6 Visitor Access Records (PE-8)

Visitor Management: - Sign-in/sign-out procedures - Escort requirements - Badge issuance - Access restrictions

[TODO: Detail visitor management procedures]

Visitor Log: | Date | Visitor Name | Company | Host | Purpose | Time In | Time Out | |——|——————|———|——|———|———|———-| | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] |

35.3 3. Control Enhancements

- **PE-2(1):** Access by Position or Role
- **PE-2(2):** Two Forms of Identification
- **PE-3(1):** System Access
- **PE-3(2):** Facility and Systems
- **PE-3(5):** Tamper Protection
- **PE-6(1):** Intrusion Alarms and Surveillance Equipment
- **PE-6(4):** Monitoring Physical Access to Information Systems

[TODO: Mark applicable enhancements]

35.4 4. Implementation Status

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

35.5 5. Assessment

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

Document History:

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

ewpage

Chapter 36

Environmental Controls

Document ID: NIST-0550
Control Family: Physical and Environmental Protection (PE)
Controls: PE-12, PE-13, PE-14, PE-15
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

36.1 1. Control Description

This document covers environmental protection controls: - **PE-12:** Emergency Lighting - **PE-13:** Fire Protection - **PE-14:** Environmental Controls (Temperature and Humidity) - **PE-15:** Water Damage Protection

36.2 2. Control Implementation

36.2.1 2.1 Emergency Lighting (PE-12)

Emergency Lighting Systems: - Battery-backed emergency lights - Exit signs - Pathway illumination - Critical area lighting

[TODO: Describe emergency lighting systems]

Testing Schedule: [TODO: Test intervals]

36.2.2 2.2 Fire Protection (PE-13)

Fire Detection Systems: - Smoke detectors - Heat detectors - Flame detectors - Manual pull stations

[TODO: Specify fire detection systems]

Fire Suppression Systems: - Sprinkler systems - Clean agent systems (FM-200, Novec 1230) - Pre-action systems - Fire extinguishers

[TODO: Describe fire suppression systems]

Inspection and Maintenance: [TODO: Maintenance schedule and procedures]

36.2.3 2.3 Environmental Controls (PE-14)

Temperature Control: - Target range: [TODO: e.g., 64-81°F / 18-27°C] - Monitoring systems - HVAC systems - Redundancy measures

[TODO: Describe temperature control systems]

Humidity Control: - Target range: [TODO: e.g., 40-60% relative humidity] - Monitoring systems - Humidification/dehumidification systems

[TODO: Describe humidity control systems]

Monitoring and Alerting: [TODO: Describe monitoring and alerting systems]

36.2.4 2.4 Water Damage Protection (PE-15)

Water Detection Systems: - Water sensors - Leak detection cables - Monitoring systems - Alert mechanisms

[TODO: Specify water detection systems]

Protection Measures: - Raised floors - Water-resistant materials - Drainage systems - Protective barriers

[TODO: Describe protection measures]

Emergency Response: [TODO: Emergency procedures for water damage]

36.3 3. Control Enhancements

- **PE-13(1):** Detection Systems - Automatic Activation and Notification
- **PE-13(2):** Suppression Systems - Automatic Activation and Notification
- **PE-13(3):** Automatic Fire Suppression
- **PE-14(1):** Automatic Controls
- **PE-14(2):** Monitoring with Alarms and Notifications

[TODO: Mark applicable enhancements]

36.4 4. Implementation Status

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

36.5 5. Assessment

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

Document History:

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

ewpage

Chapter 37

Security Planning Policy

Document-ID: NIST-0600
Control Family: Planning (PL)
Control: PL-1, PL-2
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

37.1 1. Control Description

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

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

37.2 2. Control Implementation

37.2.1 2.1 System Security Plan

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

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

37.3 3. Implementation Status

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

Document History:

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

ewpage

Chapter 38

Risk Assessment Policy

Document ID: NIST-0610
Control Family: Risk Assessment (RA)
Control: RA-1
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

38.1 1. Control Description

RA-1 Policy and Procedures

The organization develops, documents, and disseminates risk assessment policy and procedures.

38.2 2. Control Implementation

38.2.1 2.1 Risk Assessment Policy

Policy Statement: [TODO: Describe the organization's risk assessment policy]

Scope: [TODO: Scope of risk assessments]
Roles and Responsibilities: [TODO: Define roles]
Compliance: [TODO: Compliance requirements]

38.2.2 2.2 Risk Assessment Framework

Framework Components: - Risk identification - Risk analysis - Risk evaluation - Risk treatment - Risk monitoring

[TODO: Define risk assessment framework]

Risk Categories: - Strategic risks - Operational risks - Financial risks - Compliance risks - Reputational risks - Technology risks

[TODO: Specify risk categories]

38.2.3 2.3 Risk Assessment Procedures

Assessment Frequency: - Initial assessment: Before system authorization - Periodic assessments: [TODO: e.g., Annually] - Event-driven assessments: After significant changes

Assessment Methodology: [TODO: Define assessment methodology - qualitative, quantitative, or hybrid]

Risk Rating Criteria: | Likelihood | Impact | Risk Level | |————|——|————| | High | High | Critical | | High | Medium | High | | Medium | High | High | | Medium | Medium | Medium | | Low | High | Medium | | Low | Medium | Low | | Low | Low | Low |

38.2.4 2.4 Documentation Requirements

Required Documentation: - Risk assessment report - Risk register - Risk treatment plan - Residual risk acceptance

[TODO: Define documentation requirements]

38.3 3. Control Enhancements

[TODO: List applicable control enhancements]

38.4 4. Implementation Status

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

38.5 5. Assessment

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

Document History:

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

ewpage

Chapter 39

Risk Assessment and Vulnerability Management

Document ID: NIST-0620
Control Family: Risk Assessment (RA)
Controls: RA-3, RA-5, RA-7
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

39.1 1. Control Description

This document covers risk assessment and vulnerability management controls: - **RA-3:** Risk Assessment - **RA-5:** Vulnerability Monitoring and Scanning - **RA-7:** Risk Response

39.2 2. Control Implementation

39.2.1 2.1 Risk Assessment (RA-3)

Assessment Scope: - Information systems - Applications - Networks - Facilities - Personnel - Third parties

[TODO: Define assessment scope]

Assessment Process: 1. **Asset Identification** - Identify critical assets - Determine asset value - Document dependencies

2. **Threat Identification**
    - Internal threats
    - External threats
    - Natural threats
    - Environmental threats

3. **Vulnerability Identification**
   - Technical vulnerabilities
   - Procedural vulnerabilities
   - Physical vulnerabilities
4. **Impact Analysis**
   - Confidentiality impact
   - Integrity impact
   - Availability impact
5. **Likelihood Determination**
   - Threat capability
   - Vulnerability severity
   - Existing controls
6. **Risk Determination**
   - Risk = Likelihood × Impact
   - Risk prioritization

[TODO: Detail assessment process]

Risk Register: | Risk ID | Description | Likelihood | Impact | Risk Level | Owner | Status | |———|————-|————|——|————|——-|———| | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] |

39.2.2 2.2 Vulnerability Monitoring and Scanning (RA-5)

Scanning Tools: | Tool | Type | Frequency | Coverage | |——|——|————|———-| | [TODO] | Network scanner | Weekly | All network devices | | [TODO] | Web app scanner | Monthly | All web applications | | [TODO] | Database scanner | Monthly | All databases | | [TODO] | Container scanner | On build | All containers |

Scanning Schedule: - Authenticated scans: [TODO: e.g., Weekly] - Unauthenticated scans: [TODO: e.g., Monthly] - Web application scans: [TODO: e.g., Monthly] - Database scans: [TODO: e.g., Quarterly]

Vulnerability Analysis: - Severity classification (Critical, High, Medium, Low) - False positive identification - Exploitability assessment - Impact assessment

Remediation Timelines: | Severity | Remediation Timeline | Escalation | |———-|——————————|————| | Critical | 24-48 hours | CISO | | High | 7 days | Security Manager | | Medium | 30 days | System Owner | | Low | 90 days | System Owner |

Vulnerability Tracking: [TODO: Define tracking procedures and tools]

39.2.3 2.3 Risk Response (RA-7)

Response Options: 1. **Risk Avoidance** - Eliminate the risk source - Change plans to avoid risk

2. **Risk Mitigation**
   - Implement controls
   - Reduce likelihood or impact
3. **Risk Transfer**
   - Insurance
   - Outsourcing

- Contracts

4. **Risk Acceptance**
   - Formal acceptance by authorized official
   - Documentation of residual risk
   - Periodic review

[TODO: Define response procedures]

Risk Treatment Plan: | Risk ID | Response Strategy | Actions | Owner | Target Date | Status | |———|——————|———|——-|————-|———| | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] |

Residual Risk: [TODO: Define procedures for documenting and accepting residual risk]

39.3 3. Control Enhancements

- **RA-3(1):** Supply Chain Risk Assessment
- **RA-3(2):** Use of All-Source Intelligence
- **RA-3(3):** Dynamic Threat Awareness
- **RA-3(4):** Predictive Cyber Analytics
- **RA-5(1):** Update Tool Capability
- **RA-5(2):** Update Vulnerabilities to Be Scanned
- **RA-5(3):** Breadth and Depth of Coverage
- **RA-5(4):** Discoverable Information
- **RA-5(5):** Privileged Access
- **RA-5(6):** Automated Trend Analyses
- **RA-5(8):** Review Historic Audit Logs
- **RA-5(10):** Correlate Scanning Information
- **RA-5(11):** Public Disclosure Program

[TODO: Mark applicable enhancements]

39.4 4. Implementation Status

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

39.5 5. Assessment

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

Document History:

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

ewpage

Chapter 40

System and Services Acquisition Policy

Document ID: NIST-0630
Control Family: System and Services Acquisition (SA)
Controls: SA-1, SA-2, SA-3, SA-4, SA-8, SA-10, SA-15, SA-17
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

40.1 1. Control Description

This document covers system and services acquisition controls: - **SA-1:** Policy and Procedures - **SA-2:** Allocation of Resources - **SA-3:** System Development Life Cycle - **SA-4:** Acquisition Process - **SA-8:** Security and Privacy Engineering Principles - **SA-10:** Developer Configuration Management - **SA-15:** Development Process, Standards, and Tools - **SA-17:** Developer Security and Privacy Architecture and Design

40.2 2. Control Implementation

40.2.1 2.1 Acquisition Policy (SA-1)

Policy Statement: [TODO: Describe system and services acquisition policy]

Scope: [TODO: Scope of acquisitions]
Roles and Responsibilities: [TODO: Define roles]
Compliance: [TODO: Compliance requirements]

40.2.2 2.2 Allocation of Resources (SA-2)

Resource Planning: - Security requirements determination - Budget allocation for security - Personnel allocation - Technology resources

[TODO: Define resource allocation procedures]

Security Budget: | Category | Allocation | Justification | |———-|————|————-| | Security tools | [TODO] | [TODO] | | Training | [TODO] | [TODO] | | Assessments | [TODO] | [TODO] | | Incident response | [TODO] | [TODO] |

40.2.3 2.3 System Development Life Cycle (SA-3)

SDLC Phases: 1. **Initiation** - Security categorization - Preliminary risk assessment

2. **Development/Acquisition**
   - Security requirements definition
   - Security controls selection
   - Security testing
3. **Implementation**
   - Security controls implementation
   - Security assessment
   - Authorization
4. **Operations/Maintenance**
   - Continuous monitoring
   - Configuration management
   - Incident response
5. **Disposal**
   - Data sanitization
   - Asset disposal
   - Documentation

[TODO: Detail SDLC procedures]

40.2.4 2.4 Acquisition Process (SA-4)

Security Requirements: - Functional security requirements - Security assurance requirements - Security-related documentation - Protection of documentation

[TODO: Define security requirements for acquisitions]

Vendor Selection Criteria: - Security capabilities - Compliance certifications - Security track record - Incident response capabilities

[TODO: Define vendor selection criteria]

Contract Requirements: - Security clauses - Compliance requirements - Audit rights - Incident notification - Data protection

[TODO: Define contract security requirements]

40.2.5 2.5 Security Engineering Principles (SA-8)

Design Principles: - Least privilege - Defense in depth - Fail secure - Economy of mechanism - Complete mediation - Open design - Separation of privilege - Least common mechanism - Psychological acceptability

[TODO: Define application of security principles]

40.2.6 2.6 Developer Configuration Management (SA-10)

Configuration Management Requirements: - Version control - Change management - Build management - Release management

[TODO: Define developer CM requirements]

40.2.7 2.7 Development Process and Standards (SA-15)

Development Standards: - Coding standards - Security testing requirements - Code review requirements - Documentation standards

[TODO: Define development standards]

Development Tools: - Approved development tools - Security testing tools - Code analysis tools

[TODO: List approved tools]

40.2.8 2.8 Developer Security Architecture (SA-17)

Architecture Requirements: - Security architecture documentation - Threat modeling - Security design patterns - Privacy by design

[TODO: Define architecture requirements]

40.3 3. Control Enhancements

- **SA-2(1):** Specialized Components
- **SA-3(1):** Manage Preproduction Environment
- **SA-3(2):** Technology Refresh
- **SA-3(3):** Technology Refresh - Exceptions
- **SA-4(1):** Functional Properties of Security Controls
- **SA-4(2):** Design and Implementation Information for Controls
- **SA-4(5):** System, Component, and Service Configurations
- **SA-4(6):** Use of Information Assurance Products
- **SA-4(7):** NIAP-Approved Protection Profiles
- **SA-4(9):** Functions, Ports, Protocols, and Services in Use
- **SA-4(10):** Use of Approved PIV Products
- **SA-8(1):** Clear Abstractions
- **SA-8(3):** Modularity
- **SA-8(14):** Identity Management
- **SA-10(1):** Software and Firmware Integrity Verification
- **SA-15(1):** Quality Metrics
- **SA-15(3):** Criticality Analysis

- **SA-15(5):** Attack Surface Reduction
- **SA-15(7):** Automated Vulnerability Analysis
- **SA-15(8):** Reuse of Threat and Vulnerability Information
- **SA-15(11):** Archive System or Component
- **SA-17(1):** Formal Policy Model
- **SA-17(2):** Security-Relevant Components
- **SA-17(5):** Conceptually Simple Design

[TODO: Mark applicable enhancements]

40.4 4. Implementation Status

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

40.5 5. Assessment

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

Document History:

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

ewpage

Chapter 41

Developer Testing and Training

Document ID: NIST-0640
Control Family: System and Services Acquisition (SA)
Controls: SA-11, SA-16
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

41.1 1. Control Description

This document covers developer testing and training controls: - **SA-11:** Developer Testing and Evaluation - **SA-16:** Developer-Provided Training

41.2 2. Control Implementation

41.2.1 2.1 Developer Testing and Evaluation (SA-11)

Testing Requirements: - Unit testing - Integration testing - System testing - Regression testing - Security testing - Performance testing

[TODO: Define testing requirements]

Security Testing: | Test Type | Frequency | Tools | Coverage | |———–|———–|——-|———-| | Static Application Security Testing (SAST) | Every build | [TODO] | All code | | Dynamic Application Security Testing (DAST) | Weekly | [TODO] | All applications | | Interactive Application Security Testing (IAST) | Continuous | [TODO] | Runtime | | Software Composition Analysis (SCA) | Every build | [TODO] | Dependencies | | Penetration Testing | Quarterly | [TODO] | Critical systems |

Test Plan Requirements: - Test objectives - Test scope - Test procedures - Success criteria - Test environment - Test data

[TODO: Define test plan requirements]

Test Results: - Test execution records - Defect tracking - Remediation verification - Test coverage metrics

[TODO: Define test result documentation]

Acceptance Testing: - Functional requirements verification - Security requirements verification - Performance requirements verification - User acceptance testing

[TODO: Define acceptance testing procedures]

41.2.2 2.2 Developer-Provided Training (SA-16)

Training Requirements: - System administration training - User training - Security training - Maintenance training

[TODO: Define training requirements]

Training Content: | Audience | Topics | Format | Duration | |———-|———|———|———-| | Administrators | System configuration, security features, troubleshooting | [TODO] | [TODO] | | Users | System usage, security awareness, reporting | [TODO] | [TODO] | | Security Team | Security controls, monitoring, incident response | [TODO] | [TODO] | | [TODO] | [TODO] | [TODO] | [TODO] |

Training Materials: - User manuals - Administrator guides - Security guides - Training videos - Hands-on labs

[TODO: Specify required training materials]

Training Delivery: - Instructor-led training - Online training - Documentation - Hands-on workshops

[TODO: Define training delivery methods]

Training Verification: - Training completion tracking - Knowledge assessments - Certification requirements

[TODO: Define verification procedures]

41.3 3. Control Enhancements

- **SA-11(1):** Static Code Analysis
- **SA-11(2):** Threat Modeling and Vulnerability Analyses
- **SA-11(3):** Independent Verification of Assessment Plans and Evidence
- **SA-11(4):** Manual Code Reviews
- **SA-11(5):** Penetration Testing
- **SA-11(6):** Attack Surface Reviews
- **SA-11(7):** Verify Scope of Testing and Evaluation
- **SA-11(8):** Dynamic Code Analysis
- **SA-11(9):** Interactive Application Security Testing

[TODO: Mark applicable enhancements]

41.4 4. Implementation Status

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

41.5 5. Assessment

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

Document History:

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

ewpage

Chapter 42

Supply Chain Risk Management

Document ID: NIST-0650
Control Family: Supply Chain Risk Management (SR)
Controls: SR-1, SR-2, SR-3, SR-5, SR-6, SR-8, SR-10, SR-11
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

42.1 1. Control Description

This document covers supply chain risk management controls: - **SR-1:** Policy and Procedures - **SR-2:** Supply Chain Risk Management Plan - **SR-3:** Supply Chain Controls and Processes - **SR-5:** Acquisition Strategies, Tools, and Methods - **SR-6:** Supplier Assessments and Reviews - **SR-8:** Notification Agreements - **SR-10:** Inspection of Systems or Components - **SR-11:** Component Authenticity

42.2 2. Control Implementation

42.2.1 2.1 Supply Chain Risk Management Policy (SR-1)

Policy Statement: [TODO: Describe supply chain risk management policy]

Scope: [TODO: Scope of SCRM program]
Roles and Responsibilities: [TODO: Define roles]
Compliance: [TODO: Compliance requirements]

42.2.2 2.2 Supply Chain Risk Management Plan (SR-2)

Plan Components: - Supply chain risk assessment - Risk mitigation strategies - Supplier management - Incident response - Continuous monitoring

[TODO: Develop SCRM plan]

Risk Categories: - Counterfeit components - Malicious code insertion - Poor manufacturing practices - Supply chain disruption - Unauthorized modifications

[TODO: Define risk categories]

42.2.3 2.3 Supply Chain Controls and Processes (SR-3)

Supplier Selection: - Security requirements - Compliance verification - Financial stability - Geographic considerations - Track record assessment

[TODO: Define supplier selection criteria]

Contract Requirements: - Security clauses - Right to audit - Incident notification - Compliance requirements - Termination clauses

[TODO: Define contract requirements]

Supplier Monitoring: - Performance monitoring - Security monitoring - Compliance monitoring - Risk reassessment

[TODO: Define monitoring procedures]

42.2.4 2.4 Acquisition Strategies (SR-5)

Acquisition Methods: - Trusted suppliers - Multiple suppliers - Diverse supply chain - Domestic sourcing - Open-source alternatives

[TODO: Define acquisition strategies]

Risk Mitigation: - Component testing - Code review - Supply chain diversity - Escrow agreements

[TODO: Define risk mitigation strategies]

42.2.5 2.5 Supplier Assessments and Reviews (SR-6)

Assessment Frequency: - Initial assessment: Before engagement - Periodic assessments: [TODO: e.g., Annually] - Event-driven assessments: After incidents

Assessment Criteria: | Criterion | Weight | Evaluation Method | |————|———|————————-| | Security posture | [TODO] | Questionnaire, audit | | Compliance | [TODO] | Certification review | | Financial stability | [TODO] | Financial analysis | | Track record | [TODO] | Reference checks | | [TODO] | [TODO] | [TODO] |

Review Process: 1. Assessment planning 2. Data collection 3. Analysis 4. Risk rating 5. Mitigation planning 6. Decision making

[TODO: Define review process]

42.2.6 2.6 Notification Agreements (SR-8)

Notification Requirements: - Security incidents - Data breaches - Supply chain disruptions - Component vulnerabilities - Regulatory changes

[TODO: Define notification requirements]

Notification Timeline: | Event Type | Notification Timeline | Recipients | |————|————————-|————| | Security incident | [TODO: e.g., 24 hours] | [TODO] | | Data breach | [TODO: e.g., Immediate] | [TODO] | | Vulnerability | [TODO: e.g., 48 hours] | [TODO] |

42.2.7 2.7 Inspection of Systems or Components (SR-10)

Inspection Requirements: - Physical inspection - Functional testing - Security testing - Authenticity verification

[TODO: Define inspection requirements]

Inspection Procedures: [TODO: Define inspection procedures]

42.2.8 2.8 Component Authenticity (SR-11)

Authenticity Verification: - Supplier verification - Component verification - Documentation verification - Anti-counterfeit measures

[TODO: Define authenticity verification procedures]

Counterfeit Prevention: - Trusted suppliers - Chain of custody - Component testing - Tamper-evident packaging

[TODO: Define counterfeit prevention measures]

42.3 3. Control Enhancements

- **SR-2(1):** Establish SCRM Team
- **SR-3(1):** Diversity of Suppliers
- **SR-3(2):** Limitation of Harm
- **SR-5(1):** Adequate Supply
- **SR-5(2):** Assessments Prior to Selection, Acceptance, Modification, or Update
- **SR-6(1):** Testing and Analysis
- **SR-10(1):** Integrity Verification
- **SR-11(1):** Anti-Counterfeit Training
- **SR-11(2):** Configuration Control for Component Service and Repair
- **SR-11(3):** Anti-Counterfeit Scanning

[TODO: Mark applicable enhancements]

42.4 4. Implementation Status

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

42.5 5. Assessment

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

Document History:

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

ewpage

Chapter 43

System and Communications Protection

Document-ID: NIST-0700
Control Family: System and Communications Protection (SC)
Control: SC-1, SC-7, SC-8, SC-13
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

43.1 1. Control Description

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

The organization protects system and communications.

43.2 2. Control Implementation

43.2.1 2.1 Boundary Protection

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

43.2.2 2.2 Cryptographic Protection

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

43.2.3 2.3 Transmission Protection

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

43.3 3. Implementation Status

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

Document History:

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

ewpage

Chapter 44

Network Security and Boundary Protection

Document ID: NIST-0710
Control Family: System and Communications Protection (SC)
Controls: SC-5, SC-7, SC-20, SC-21, SC-22
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

44.1 1. Control Description

This document covers network security and boundary protection controls: - **SC-5:** Denial-of-Service Protection - **SC-7:** Boundary Protection - **SC-20:** Secure Name/Address Resolution Service (Authoritative Source) - **SC-21:** Secure Name/Address Resolution Service (Recursive or Caching Resolver) - **SC-22:** Architecture and Provisioning for Name/Address Resolution Service

44.2 2. Control Implementation

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

Protection Mechanisms: - Rate limiting - Traffic filtering - Load balancing - DDoS mitigation services - Redundant systems

[TODO: Define DoS protection mechanisms]

Detection and Response: - Traffic monitoring - Anomaly detection - Automated response - Incident escalation

[TODO: Define detection and response procedures]

Capacity Planning: - Bandwidth capacity - Processing capacity - Storage capacity - Redundancy

[TODO: Define capacity requirements]

44.2.2 2.2 Boundary Protection (SC-7)

Network Boundaries: | Boundary | Protection Mechanism | Monitoring | |———-|———————|————| | Internet perimeter | Firewall, IPS | 24/7 | | DMZ | Firewall, WAF | 24/7 | | Internal segments | Firewall, VLAN | 24/7 | | Wireless | NAC, 802.1X | 24/7 | | [TODO] | [TODO] | [TODO] |

Managed Interfaces: - External connections documented - Connection security requirements - Traffic flow restrictions - Monitoring requirements

[TODO: Document managed interfaces]

Network Segmentation: - Production network - Development network - Management network - Guest network

[TODO: Define network segments]

Access Control: - Inbound traffic rules - Outbound traffic rules - Default deny policy - Exception management

[TODO: Define access control rules]

44.2.3 2.3 DNS Security (SC-20, SC-21, SC-22)

Authoritative DNS (SC-20): - DNSSEC implementation - Zone signing - Key management - Validation

[TODO: Define authoritative DNS security]

Recursive DNS (SC-21): - DNSSEC validation - Response filtering - Cache poisoning protection - Query logging

[TODO: Define recursive DNS security]

DNS Architecture (SC-22): - Redundant DNS servers - Geographic distribution - Fault tolerance - Performance optimization

[TODO: Define DNS architecture]

DNS Security Measures: - Access controls - Rate limiting - Monitoring and logging - Incident response

[TODO: Define DNS security measures]

44.3 3. Control Enhancements

- **SC-5(1):** Restrict Ability to Attack Other Systems
- **SC-5(2):** Capacity, Bandwidth, and Redundancy
- **SC-5(3):** Detection and Monitoring
- **SC-7(3):** Access Points
- **SC-7(4):** External Telecommunications Services
- **SC-7(5):** Deny by Default - Allow by Exception
- **SC-7(7):** Split Tunneling for Remote Devices

- **SC-7(8):** Route Traffic to Authenticated Proxy Servers
- **SC-7(10):** Prevent Exfiltration
- **SC-7(11):** Restrict Incoming Communications Traffic
- **SC-7(12):** Host-Based Protection
- **SC-7(13):** Isolation of Security Tools, Mechanisms, and Support Components
- **SC-7(18):** Fail Secure
- **SC-7(20):** Dynamic Isolation and Segregation
- **SC-7(21):** Isolation of System Components
- **SC-20(1):** Child Subspaces
- **SC-20(2):** Data Origin and Integrity
- **SC-21(1):** Data Origin and Integrity

[TODO: Mark applicable enhancements]

44.4 4. Implementation Status

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

44.5 5. Assessment

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

Document History:

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

ewpage

Chapter 45

Cryptographic Protection

Document ID: NIST-0720
Control Family: System and Communications Protection (SC)
Controls: SC-8, SC-12, SC-13, SC-17, SC-28
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

45.1 1. Control Description

This document covers cryptographic protection controls: - **SC-8:** Transmission Confidentiality and Integrity - **SC-12:** Cryptographic Key Establishment and Management - **SC-13:** Cryptographic Protection - **SC-17:** Public Key Infrastructure Certificates - **SC-28:** Protection of Information at Rest

45.2 2. Control Implementation

45.2.1 2.1 Transmission Confidentiality and Integrity (SC-8)

Encryption Requirements: | Data Type | Encryption Method | Key Length | Protocol | |———|——————|————|———-| | Web traffic | TLS 1.2/1.3 | 256-bit | HTTPS | | Email | TLS, S/MIME | 256-bit | SMTP/TLS | | File transfer | SFTP, FTPS | 256-bit | SSH, TLS | | Database | TLS | 256-bit | DB-specific | | VPN | IPsec, SSL/TLS | 256-bit | Various |

Approved Algorithms: - Symmetric: AES-256, ChaCha20 - Asymmetric: RSA-2048+, ECDSA P-256+ - Hash: SHA-256, SHA-384, SHA-512 - Key exchange: ECDHE, DHE

[TODO: Specify approved algorithms]

45.2.2 2.2 Cryptographic Key Management (SC-12)

Key Lifecycle: 1. **Generation** - Secure random number generation - Approved algorithms - Appropriate key lengths

2. **Distribution**
   - Secure key exchange protocols
   - Out-of-band verification
   - Access controls
3. **Storage**
   - Hardware security modules (HSMs)
   - Key encryption keys (KEKs)
   - Access controls
4. **Usage**
   - Purpose-specific keys
   - Usage logging
   - Access controls
5. **Rotation**
   - Rotation schedule
   - Automated rotation
   - Key history
6. **Destruction**
   - Secure deletion
   - Verification
   - Documentation

[TODO: Define key management procedures]

Key Management System: - Centralized key management - HSM integration - Automated key rotation - Audit logging

[TODO: Describe key management system]

45.2.3 2.3 Cryptographic Protection (SC-13)

Cryptographic Modules: - FIPS 140-2/140-3 validated modules - Approved algorithms - Proper implementation - Regular updates

[TODO: List cryptographic modules in use]

Implementation Requirements: - No custom cryptography - Use of established libraries - Proper initialization - Secure defaults

[TODO: Define implementation requirements]

45.2.4 2.4 PKI Certificates (SC-17)

Certificate Management: - Certificate issuance - Certificate renewal - Certificate revocation - Certificate validation

[TODO: Define certificate management procedures]

Certificate Authorities: | CA Type | Purpose | Validation Level | |———|———|————–| | Internal CA | Internal systems | Domain validation | | Public CA | External services | Extended validation | | [TODO] | [TODO] | [TODO] |

Certificate Policies: - Certificate lifetimes - Key lengths - Allowed uses - Revocation procedures

[TODO: Define certificate policies]

45.2.5 2.5 Protection of Information at Rest (SC-28)

Encryption at Rest: | Data Type | Encryption Method | Key Management | |———|————|————-| | Database | Transparent Data Encryption (TDE) | HSM | | File systems | Full disk encryption | TPM/HSM | | Backups | AES-256 | HSM | | Archives | AES-256 | HSM | | Mobile devices | Device encryption | Device-based |

Encryption Scope: - All sensitive data - All regulated data - All backup media - All portable media

[TODO: Define encryption scope]

Key Management: - Separate encryption keys per system - Regular key rotation - Secure key storage - Key backup and recovery

[TODO: Define key management for data at rest]

45.3 3. Control Enhancements

- **SC-8(1):** Cryptographic Protection
- **SC-8(2):** Pre- and Post-Transmission Handling
- **SC-8(3):** Cryptographic Protection for Message Externals
- **SC-8(4):** Conceal or Randomize Communications
- **SC-12(1):** Availability
- **SC-12(2):** Symmetric Keys
- **SC-12(3):** Asymmetric Keys
- **SC-12(6):** Physical Control of Keys
- **SC-13(1):** FIPS-Validated Cryptography
- **SC-17(1):** Receiver Checks
- **SC-17(2):** Validation of Binding
- **SC-28(1):** Cryptographic Protection
- **SC-28(2):** Offline Storage
- **SC-28(3):** Cryptographic Keys

[TODO: Mark applicable enhancements]

45.4 4. Implementation Status

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

45.5 5. Assessment

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

Document History:

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

ewpage

Chapter 46

System and Information Integrity Policy

Document ID: NIST-0730
Control Family: System and Information Integrity (SI)
Controls: SI-1, SI-6, SI-7, SI-10, SI-11, SI-12, SI-16
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

46.1 1. Control Description

This document covers system and information integrity policy and related controls: - **SI-1:** Policy and Procedures - **SI-6:** Security and Privacy Function Verification - **SI-7:** Software, Firmware, and Information Integrity - **SI-10:** Information Input Validation - **SI-11:** Error Handling - **SI-12:** Information Management and Retention - **SI-16:** Memory Protection

46.2 2. Control Implementation

46.2.1 2.1 System and Information Integrity Policy (SI-1)

Policy Statement: [TODO: Describe the system and information integrity policy]

Scope: [TODO: Scope]
Roles and Responsibilities: [TODO: Roles]
Compliance: [TODO: Compliance requirements]

46.2.2 2.2 Security Function Verification (SI-6)

Verification Methods: - Self-tests at startup - Periodic integrity checks - Cryptographic checksums - Digital signatures

[TODO: Describe verification methods]

46.2.3 2.3 Software, Firmware, and Information Integrity (SI-7)

Integrity Protection: - Code signing - Cryptographic hashes - Integrity monitoring tools - Change detection

[TODO: Specify integrity protection measures]

Integrity Verification: [TODO: Describe verification processes]

46.2.4 2.4 Information Input Validation (SI-10)

Input Validation Controls: - Syntax checking - Range checking - Type checking - Format validation - Whitelist validation

[TODO: Detail input validation controls]

Validation Points: [TODO: List validation points]

46.2.5 2.5 Error Handling (SI-11)

Error Handling Procedures: - Secure error messages - Error logging - User notification - System recovery

[TODO: Describe error handling procedures]

Information Disclosure Prevention: [TODO: Measures to prevent information leaks]

46.2.6 2.6 Information Management and Retention (SI-12)

Retention Requirements: | Information Type | Retention Period | Storage Location | Disposal Method | |————–|————–|————–|————| | [TODO] | [TODO] | [TODO] | [TODO] |

46.2.7 2.7 Memory Protection (SI-16)

Memory Protection Mechanisms: - Address Space Layout Randomization (ASLR) - Data Execution Prevention (DEP) - Stack canaries - Memory tagging

[TODO: Describe memory protection mechanisms]

46.3 3. Control Enhancements

- **SI-6(1):** Notification of Failed Security Tests
- **SI-7(1):** Integrity Checks
- **SI-7(2):** Automated Notifications of Integrity Violations
- **SI-7(5):** Automated Response to Integrity Violations
- **SI-7(6):** Cryptographic Protection
- **SI-7(7):** Integration of Detection and Response
- **SI-10(1):** Manual Override Capability
- **SI-10(3):** Predictable Behavior

[TODO: Mark applicable enhancements]

46.4 4. Implementation Status

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

46.5 5. Assessment

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

Document History:

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

ewpage

Chapter 47

Flaw Remediation

Document ID: NIST-0740
Control Family: System and Information Integrity (SI)
Controls: SI-2, SI-5
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

47.1 1. Control Description

This document covers flaw remediation controls: - **SI-2:** Flaw Remediation - **SI-5:** Security Alerts, Advisories, and Directives

47.2 2. Control Implementation

47.2.1 2.1 Flaw Remediation (SI-2)

Flaw Identification: - Vulnerability scanning - Security advisories - Vendor notifications - Penetration testing results

[TODO: Describe identification methods]

Remediation Process: 1. Flaw identification and assessment 2. Risk evaluation 3. Remediation planning 4. Testing 5. Deployment 6. Verification

[TODO: Detail remediation process]

Remediation Timelines: | Severity | Target Remediation Time | |———-|———————| | Critical | [TODO: e.g., 24-48 hours] | | High | [TODO: e.g., 7 days] | | Medium | [TODO: e.g., 30 days] | | Low | [TODO: e.g., 90 days] |

47.2.2 2.2 Security Alerts, Advisories, and Directives (SI-5)

Information Sources: - CISA alerts - Vendor security bulletins - CERT advisories - Industry threat intelligence - Security mailing lists

[TODO: Specify information sources]

Alert Processing: 1. Receipt and review 2. Relevance assessment 3. Impact analysis 4. Action determination 5. Implementation 6. Documentation

[TODO: Describe processing workflow]

Distribution: [TODO: Define distribution lists and procedures]

47.3 3. Control Enhancements

- **SI-2(1):** Central Management
- **SI-2(2):** Automated Flaw Remediation Status
- **SI-2(3):** Time to Remediate Flaws and Benchmarks
- **SI-2(5):** Automatic Software and Firmware Updates
- **SI-2(6):** Removal of Previous Versions of Software and Firmware
- **SI-5(1):** Automated Alerts and Advisories

[TODO: Mark applicable enhancements]

47.4 4. Implementation Status

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

47.5 5. Assessment

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

Document History:

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

ewpage

Chapter 48

Malicious Code and System Monitoring

Document ID: NIST-0750
Control Family: System and Information Integrity (SI)
Controls: SI-3, SI-4, SI-8
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

48.1 1. Control Description

This document covers malicious code protection and system monitoring controls: - **SI-3:** Malicious Code Protection - **SI-4:** System Monitoring - **SI-8:** Spam Protection

48.2 2. Control Implementation

48.2.1 2.1 Malicious Code Protection (SI-3)

Protection Mechanisms: - Antivirus software - Anti-malware solutions - Endpoint detection and response (EDR) - Email filtering - Web filtering

[TODO: Describe implemented protection mechanisms]

Update Frequency: - Signature updates: [TODO: e.g., daily or automatic] - Software updates: [TODO: e.g., monthly]

Scanning Configuration: - Real-time scanning - Scheduled scans - On-demand scans - Quarantine procedures

[TODO: Specify scanning configuration]

48.2.2 2.2 System Monitoring (SI-4)

Monitoring Capabilities: - Network traffic monitoring - System event monitoring - Application monitoring - User activity monitoring - Security information and event management (SIEM)

[TODO: Describe monitoring capabilities]

Monitored Events: - Unauthorized access attempts - Privilege escalation - Malware detection - Data exfiltration attempts - Configuration changes

[TODO: Specify monitored events]

Alert Thresholds: [TODO: Define alert thresholds]

Response Procedures: [TODO: Describe response procedures]

48.2.3 2.3 Spam Protection (SI-8)

Spam Protection Mechanisms: - Email spam filters - Sender Policy Framework (SPF) - DomainKeys Identified Mail (DKIM) - Domain-based Message Authentication, Reporting, and Conformance (DMARC) - Content filtering

[TODO: Describe spam protection mechanisms]

Filtering Rules: [TODO: Specify filtering rules]

48.3 3. Control Enhancements

- **SI-3(1):** Central Management
- **SI-3(2):** Automatic Updates
- **SI-3(4):** Updates Only by Privileged Users
- **SI-3(6):** Testing and Verification
- **SI-3(7):** Nonsignature-Based Detection
- **SI-4(1):** System-Wide Intrusion Detection System
- **SI-4(2):** Automated Tools and Mechanisms for Real-Time Analysis
- **SI-4(4):** Inbound and Outbound Communications Traffic
- **SI-4(5):** System-Generated Alerts
- **SI-4(7):** Automated Response to Suspicious Events
- **SI-4(12):** Automated Organization-Generated Alerts
- **SI-4(16):** Correlate Monitoring Information
- **SI-4(23):** Host-Based Devices
- **SI-8(1):** Central Management
- **SI-8(2):** Automatic Updates

[TODO: Mark applicable enhancements]

48.4 4. Implementation Status

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

48.5 5. Assessment

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

Document History:

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

ewpage

Chapter 49

Control Traceability Matrix

Document-ID: NIST-0800
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

49.1 1. Purpose

This document provides a traceability matrix for all NIST 800-53 security controls for system {{ meta.nist.system_name }}.

49.2 2. Control Traceability Matrix

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

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

49.3 3. Control Summary

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

49.4 4. Control Families Coverage

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

Document History:

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

ewpage

Chapter 50

Control Assessment Procedures

Document ID: NIST-0810
Control Family: Assessment, Authorization, and Monitoring (CA)
Control: CA-2
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

50.1 1. Control Description

CA-2 Control Assessments

The organization develops a control assessment plan, assesses the controls, and produces a control assessment report documenting the results.

50.2 2. Control Implementation

50.2.1 2.1 Assessment Planning

Assessment Scope: - Systems to be assessed - Controls to be assessed - Assessment methods - Assessment schedule

[TODO: Define assessment scope]

Assessment Team: | Role | Name | Responsibilities | Independence | |——|——|——————|————| | Lead Assessor | [TODO] | Overall assessment | Independent | | Technical Assessor | [TODO] | Technical testing | Independent | | Subject Matter Expert | [TODO] | Domain expertise | May be internal | | [TODO] | [TODO] | [TODO] | [TODO] |

Assessment Plan: - Assessment objectives - Assessment scope - Assessment methods (Examine, Interview, Test) - Assessment procedures - Assessment schedule - Resource requirements

[TODO: Develop assessment plan]

50.2.2 2.2 Assessment Methods

Examine: - Policy review - Procedure review - Documentation review - Configuration review - Log review

Interview: - System owners - System administrators - Security personnel - Users - Management

Test: - Automated scanning - Manual testing - Penetration testing - Configuration testing - Functional testing

[TODO: Define assessment methods for each control]

50.2.3 2.3 Assessment Procedures

Assessment Steps: 1. **Preparation** - Review system documentation - Identify assessment objectives - Prepare assessment tools

2. **Execution**
    - Conduct examinations
    - Perform interviews
    - Execute tests
    - Document findings
3. **Analysis**
    - Analyze results
    - Identify deficiencies
    - Determine risk
    - Develop recommendations
4. **Reporting**
    - Prepare assessment report
    - Document findings
    - Provide recommendations
    - Brief stakeholders

[TODO: Detail assessment procedures]

50.2.4 2.4 Assessment Report

Report Contents: - Executive summary - Assessment scope - Assessment methodology - Findings and observations - Risk ratings - Recommendations - Conclusion

[TODO: Define report template]

Finding Classification: | Severity | Description | Remediation Timeline | |———-|————-|———————| | Critical | Control not implemented or ineffective | Immediate | | High | Significant deficiency | 30 days | | Medium | Moderate deficiency | 90 days | | Low | Minor deficiency | 180 days |

50.2.5 2.5 Remediation and Follow-up

Remediation Process: 1. Finding review 2. Remediation planning 3. Implementation 4. Verification 5. Closure

[TODO: Define remediation process]

Follow-up Assessment: - Verification of remediation - Residual risk assessment - Documentation update

[TODO: Define follow-up procedures]

50.3 3. Control Enhancements

- **CA-2(1):** Independent Assessors
- **CA-2(2):** Specialized Assessments
- **CA-2(3):** Leveraging Results from External Organizations
- **CA-2(4):** Reuse of Assessment Information

[TODO: Mark applicable enhancements]

50.4 4. Implementation Status

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

50.5 5. Assessment

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

Document History:

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

ewpage

Chapter 51

Plan of Action and Milestones

Document ID: NIST-0820
Control Family: Assessment, Authorization, and Monitoring (CA)
Controls: CA-5, PM-4
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

51.1 1. Control Description

This document covers Plan of Action and Milestones (POA&M) controls: - **CA-5:** Plan of Action and Milestones - **PM-4:** Plan of Action and Milestones Process

51.2 2. Control Implementation

51.2.1 2.1 POA&M Development (CA-5)

POA&M Purpose: - Document identified weaknesses - Track remediation efforts - Monitor progress - Report status

[TODO: Define POA&M purpose and scope]

POA&M Components: - Weakness description - Risk rating - Resources required - Milestones - Scheduled completion date - Status

[TODO: Define POA&M template]

POA&M Entry: | POA&M ID | Weakness | System | Risk | Owner | Target Date | Status | |——–|———-|——–|——|——-|———–|——–| | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] | [TODO] |

51.2.2 2.2 POA&M Process (PM-4)

Process Steps: 1. **Identification** - Assessment findings - Audit findings - Incident findings - Vulnerability findings

2. **Documentation**
   - Create POA&M entry
   - Assign risk rating
   - Identify resources
   - Set milestones
3. **Approval**
   - Management review
   - Resource allocation
   - Timeline approval
4. **Implementation**
   - Execute remediation
   - Track progress
   - Update status
5. **Verification**
   - Verify remediation
   - Retest controls
   - Document results
6. **Closure**
   - Final verification
   - Documentation
   - Lessons learned

[TODO: Detail POA&M process]

Roles and Responsibilities: | Role | Responsibilities | |——|————–| | System Owner | POA&M creation, resource allocation | | Security Officer | Risk assessment, verification | | Authorizing Official | Approval, risk acceptance | | [TODO] | [TODO] |

51.2.3 2.3 POA&M Tracking and Reporting

Tracking Frequency: - Weekly status updates - Monthly progress reports - Quarterly management reviews

[TODO: Define tracking frequency]

Status Categories: - Not Started - In Progress - Delayed - Completed - Cancelled

Reporting: - POA&M summary report - Overdue items report - Risk trend analysis - Resource utilization

[TODO: Define reporting requirements]

51.2.4 2.4 POA&M Review and Updates

Review Schedule: - Weekly: Individual POA&M items - Monthly: Overall POA&M status - Quarterly: POA&M process effectiveness

Update Triggers: - Status changes - Milestone completion - Resource changes - Timeline changes - Risk changes

[TODO: Define review and update procedures]

51.2.5 2.5 POA&M Metrics

Key Metrics: - Number of open POA&Ms - Average time to closure - Overdue POA&Ms - POA&Ms by risk level - POA&Ms by system

[TODO: Define metrics and targets]

Performance Targets: | Metric | Target | Current | |——–|——–|———| | Average closure time | [TODO: e.g., 90 days] | [TODO] | | Overdue rate | [TODO: e.g., <10%] | [TODO] | | Critical POA&Ms | [TODO: e.g., 0] | [TODO] |

51.3 3. Control Enhancements

- **CA-5(1):** Automation Support for Accuracy and Currency
- **PM-4(1):** Accountability

[TODO: Mark applicable enhancements]

51.4 4. Implementation Status

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

51.5 5. Assessment

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

Document History:

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

ewpage

Chapter 52

Privacy Controls

Document ID: NIST-0830
Control Family: Privacy Controls
Controls: PT-1, AP-1, AR-1, DI-1, DM-1, IP-1, SE-1, TR-1, UL-1
Organization: AdminSend GmbH
Owner: IT Operations Manager
Version: 1.0.0
Status: Draft / In Review / Approved
Last Updated: {{ meta.document.last_updated }}

52.1 1. Control Description

This document covers privacy controls: - **PT-1:** Policy and Procedures - **AP-1:** Authority to Collect - **AR-1:** Governance and Privacy Program - **DI-1:** Data Quality - **DM-1:** Minimization of Personally Identifiable Information - **IP-1:** Consent - **SE-1:** Inventory of Personally Identifiable Information - **TR-1:** Privacy Notice - **UL-1:** Internal Use

52.2 2. Control Implementation

52.2.1 2.1 Privacy Policy and Procedures (PT-1)

Policy Statement: [TODO: Describe privacy policy]

Scope: [TODO: Scope of privacy program]
Roles and Responsibilities: [TODO: Define roles]
Compliance: GDPR, CCPA, HIPAA, etc. [TODO: List applicable regulations]

52.2.2 2.2 Authority to Collect (AP-1)

Collection Authority: - Legal basis for collection - Purpose specification - Collection limitation - Consent requirements

[TODO: Define collection authority]

Authorized Collections: | Data Type | Legal Basis | Purpose | Retention | |————|————-|———|————| | [TODO] | [TODO] | [TODO] | [TODO] |

52.2.3 2.3 Governance and Privacy Program (AR-1)

Privacy Program: - Privacy governance structure - Privacy officer designation - Privacy policies and procedures - Privacy training - Privacy assessments

[TODO: Define privacy program]

Privacy Governance: - Privacy board/committee - Privacy impact assessments - Privacy risk management - Privacy compliance monitoring

[TODO: Define governance structure]

52.2.4 2.4 Data Quality (DI-1)

Data Quality Requirements: - Accuracy - Completeness - Timeliness - Relevance

[TODO: Define data quality requirements]

Data Quality Procedures: - Data validation - Data verification - Data correction - Data updates

[TODO: Define quality procedures]

52.2.5 2.5 Data Minimization (DM-1)

Minimization Principles: - Collect only necessary data - Retain only as long as needed - Limit access to authorized personnel - Anonymize when possible

[TODO: Define minimization principles]

Data Inventory: | Data Element | Purpose | Retention Period | Access Controls | |————–|———|—————–|—————| | [TODO] | [TODO] | [TODO] | [TODO] |

52.2.6 2.6 Consent (IP-1)

Consent Requirements: - Informed consent - Explicit consent - Opt-in/opt-out mechanisms - Consent withdrawal

[TODO: Define consent requirements]

Consent Management: - Consent capture - Consent storage - Consent verification - Consent revocation

[TODO: Define consent management procedures]

52.2.7 2.7 PII Inventory (SE-1)

Inventory Components: - Data elements - Data sources - Data flows - Data storage locations - Data retention periods - Access controls

[TODO: Develop PII inventory]

Inventory Maintenance: - Regular updates - Change management - Accuracy verification

[TODO: Define maintenance procedures]

52.2.8 2.8 Privacy Notice (TR-1)

Notice Requirements: - What data is collected - Why data is collected - How data is used - Who data is shared with - How long data is retained - Individual rights - Contact information

[TODO: Develop privacy notice]

Notice Delivery: - Timing of notice - Method of delivery - Language and clarity - Updates and changes

[TODO: Define notice delivery procedures]

52.2.9 2.9 Internal Use (UL-1)

Use Limitations: - Purpose limitation - Use restrictions - Sharing restrictions - Secondary use controls

[TODO: Define use limitations]

Use Monitoring: - Access logging - Use auditing - Violation detection - Enforcement

[TODO: Define monitoring procedures]

52.3 3. Control Enhancements

- **AP-1(1):** Justification for Collection
- **AR-1(1):** Automation
- **DI-1(1):** Validate PII
- **DI-1(2):** Re-Validate PII
- **DM-1(1):** Locate and Remove, Redact, or Hash PII
- **IP-1(1):** Mechanisms Supporting Itemized or Tiered Consent
- **IP-1(2):** Just-in-Time Consent
- **SE-1(1):** Automation
- **TR-1(1):** Real-Time or Layered Notice
- **UL-1(1):** Automation

[TODO: Mark applicable enhancements]

52.4 4. Implementation Status

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

52.5 5. Assessment

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

Document History:

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

ewpage

Chapter 53

Glossary and Abbreviations

Document-ID: NIST-0850
Organization: AdminSend GmbH
Version: 1.0.0
Last Updated: {{ meta.document.last_updated }}

53.1 1. Abbreviations

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

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

53.2 2. Glossary

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

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

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

Confidentiality: Preserving authorized restrictions on information access and disclosure.

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

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

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

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

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

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

Integrity: Guarding against improper information modification or destruction.

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

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

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

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

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

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

Document History:

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

ewpage