

*System security plan  
Document  
[Nama Aplikasi]*

# DAFTAR ISI

[DAFTAR ISI 1](#_Toc54116752)

[DAFTAR TABEL 2](#_Toc54116753)

[DAFTAR GAMBAR 3](#_Toc54116754)

[1. PENGENDALIAN DOKUMEN 4](#_Toc54116755)

[Referensi Penyusunan Dokumen 4](#_Toc54116756)

[Daftar Istilah dan Definisi 4](#_Toc54116757)

[Perubahan yang terjadi pada dokumen versi sebelumnya 4](#_Toc54116758)

[2. PENDAHULUAN 5](#_Toc54116759)

[2.1 Latar Belakang 5](#_Toc54116760)

[2.2 Overview Aplikasi [Nama Aplikasi] 5](#_Toc54116761)

[3. SYSTEM SECURITY PLAN 5](#_Toc54116762)

[3.1 Kebutuhan Keamanan Sistem 5](#_Toc54116763)

[3.2 Minimum Security Controls 5](#_Toc54116764)

# DAFTAR TABEL

[Tabel 1 5](#_Toc54080055)

[Tabel 2 6](#_Toc54080056)

# DAFTAR GAMBAR

[Gambar 1 4](#_Toc53064198)

# PENGENDALIAN DOKUMEN

## Referensi Penyusunan Dokumen

Referensi

|  |  |  |  |
| --- | --- | --- | --- |
| **Document** | | **Version** | **Author** |
| - | - | 1.0 |  |

Revisi / Amandemen

|  |  |  |  |
| --- | --- | --- | --- |
| **Item Revisi** | | | **Direvisi Oleh** |
| - | - | - | - |

## Daftar Istilah dan Definisi

|  |  |
| --- | --- |
| **Terms** | **Description/Explanation** |
|  |  |
|  |  |
|  |  |

## Perubahan yang terjadi pada dokumen versi sebelumnya

|  |  |
| --- | --- |
| **Change Request** | **Description/Explanation** |
|  | - |

# PENDAHULUAN

## Latar Belakang

*[Latar Belakang Aplikasi]*

## 2.2 Overview Aplikasi [Nama Aplikasi]

*[Gambaran umum Aplikasi]*

# SYSTEM SECURITY PLAN

## 3.1 Kebutuhan Keamanan Sistem

*[Kebutuhan kemanan sistem hasil dari requirement gathering]*

## 

## 3.2 Minimum Security Controls

*[Minimum security control baseline yang sesuai (low, moderate, high-impact) dapat merujuk kepada dokumen NIST SP 800-53]*

|  |  |  |
| --- | --- | --- |
| **Control No** | **Control Name**  **CONTROL ENHANCEMENT** | **Control Baseline**  **(Low, Moderate, Priority)** |
| **AC-1** | **Access Control Policy and Procedures** |  |
| **AC-2** | **Account Management** |  |
| AC-2(1) | *ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT MANAGEMENT* |  |
| AC-2(2) | *ACCOUNT MANAGEMENT | REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS* |  |
| AC-2(3) | *ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS* |  |
| AC-2(4) | *ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS* |  |
| AC-2(5) | *ACCOUNT MANAGEMENT | INACTIVITY LOGOUT* |  |
| AC-2(6) | *ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT* |  |
| AC-2(7) | *ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES* |  |
| AC-2(8) | *ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION* |  |
| AC-2(9) | *ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED / GROUP ACCOUNTS* |  |
| AC-2(10) | *ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION* |  |
| AC-2(11) | *ACCOUNT MANAGEMENT | USAGE CONDITIONS* |  |
| AC-2(12) | *ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE* |  |
| AC-2(13) | *ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS* |  |
| **AC-3** | **Access Enforcement** |  |
| AC-3(1) | *ACCESS ENFORCEMENT | RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS* |  |
| AC-3(2) | *ACCESS ENFORCEMENT | DUAL AUTHORIZATION* |  |
| AC-3(3) | *ACCESS ENFORCEMENT | MANDATORY ACCESS CONTROL* |  |
| AC-3(4) | *ACCESS ENFORCEMENT | DISCRETIONARY ACCESS CONTROL* |  |
| AC-3(5) | *ACCESS ENFORCEMENT | SECURITY-RELEVANT INFORMATION* |  |
| AC-3(6) | *ACCESS ENFORCEMENT | PROTECTION OF USER AND SYSTEM INFORMATION* |  |
| AC-3(7) | *ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL* |  |
| AC-3(8) | *ACCESS ENFORCEMENT | REVOCATION OF ACCESS AUTHORIZATIONS* |  |
| AC-3(9) | *ACCESS ENFORCEMENT | CONTROLLED RELEASE* |  |
| AC-3(10) | *ACCESS ENFORCEMENT | AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS* |  |
| **AT-1** | **Security Awareness and Training Policy and Procedures** |  |
| **AT-2** | **Security Awareness Training** |  |
| AT-2(1) | *SECURITY AWARENESS | PRACTICAL EXERCISES* |  |
| AT-2(2) | *SECURITY AWARENESS | INSIDER THREAT* |  |
| **AT-3** | **Role-Based Security Training** |  |
| AT-3(1) | *ROLE-BASED SECURITY TRAINING | ENVIRONMENTAL CONTROLS* |  |
| AT-3(2) | *ROLE-BASED SECURITY TRAINING | PHYSICAL SECURITY CONTROLS* |  |
| AT-3(3) | *ROLE-BASED SECURITY TRAINING | PRACTICAL EXERCISES* |  |
| AT-3(4) | *ROLE-BASED SECURITY TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR* |  |
| **AT-4** | **Security Training Records** |  |
| **AT-5** | **Contacts with Security Groups and Associations** |  |
| **AU-1** | **Audit and Accountability Policy and Procedures** |  |
| **AU-2** | **Audit Events** |  |
| AU-2(1) | *AUDIT EVENTS | COMPILATION OF AUDIT RECORDS FROM MULTIPLE SOURCES* |  |
| AU-2(2) | *AUDIT EVENTS | SELECTION OF AUDIT EVENTS BY COMPONENT* |  |
| AU-2(3) | *AUDIT EVENTS | REVIEWS AND UPDATES* |  |
| AU-2(4) | *AUDIT EVENTS | PRIVILEGED FUNCTIONS* |  |
| **AU-3** | **Content of Audit Records** |  |
| AU-3(1) | *CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION* |  |
| AU-3(2) | *CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT* |  |
| **CA-1** | **Security Assessment and Authorization Policies and Procedures** |  |
| **CA-2** | **Security Assessments** |  |
| CA-2(1) | *SECURITY ASSESSMENTS | INDEPENDENT ASSESSORS* |  |
| CA-2(2) | *SECURITY ASSESSMENTS | SPECIALIZED ASSESSMENTS* |  |
| CA-2(3) | *SECURITY ASSESSMENTS | EXTERNAL ORGANIZATIONS* |  |
| **CA-1** | **Configuration Management Policy and Procedures** |  |
| **CM-2** | **Baseline Configuration** |  |
| CM-2(1) | *BASELINE CONFIGURATION | REVIEWS AND UPDATES* |  |
| CM-2(2) | *BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY / CURRENCY* |  |
| CM-2(3) | *BASELINE CONFIGURATION | RETENTION OF PREVIOUS CONFIGURATIONS* |  |
| CM-2(4) | *BASELINE CONFIGURATION | UNAUTHORIZED SOFTWARE* |  |
| CM-2(5) | *BASELINE CONFIGURATION | AUTHORIZED SOFTWARE* |  |
| CM-2(6) | *BASELINE CONFIGURATION | DEVELOPMENT AND TEST ENVIRONMENTS* |  |
| CM-2(7) | *BASELINE CONFIGURATION | CONFIGURE SYSTEMS, COMPONENTS, OR DEVICES FOR HIGH-RISK AREAS* |  |
| **CP-1** | **Contingency Planning Policy and Procedures** |  |
| **CP-2** | **Contingency Plan** |  |
| CP-2(1) | *CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS* |  |
| CP-2(2) | *CONTINGENCY PLAN | CAPACITY PLANNING* |  |
| CP-2(3) | *CONTINGENCY PLAN | RESUME ESSENTIAL MISSIONS / BUSINESS FUNCTIONS* |  |
| CP-2(4) | *CONTINGENCY PLAN | RESUME ALL MISSIONS / BUSINESS FUNCTIONS* |  |
| CP-2(5) | *CONTINGENCY PLAN | CONTINUE ESSENTIAL MISSIONS / BUSINESS FUNCTIONS* |  |
| CP-2(6) | *CONTINGENCY PLAN | ALTERNATE PROCESSING / STORAGE SITE* |  |
| CP-2(7) | *CONTINGENCY PLAN | COORDINATE WITH EXTERNAL SERVICE PROVIDERS* |  |
| CP-2(8) | *CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS* |  |
| **IA-1** | **Identification and Authentication Policy and Procedures** |  |
| **IA-2** | **Identification and Authentication (Organizational Users)** |  |
| IA-2(1) | *IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS* |  |
| IA-2(2) | *IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS* |  |
| IA-2(3) | *IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO PRIVILEGED ACCOUNTS* |  |
| IA-2(4) | *IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | LOCAL ACCESS TO NON-PRIVILEGED ACCOUNTS* |  |
| IA-2(5) | *IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | GROUP AUTHENTICATION* |  |
| IA-2(6) | *IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - SEPARATE DEVICE* |  |
| IA-2(7) | *IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - SEPARATE DEVICE* |  |
| IA-2(8) | *IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO PRIVILEGED ACCOUNTS - REPLAY RESISTANT* |  |
| IA-2(9) | *IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | NETWORK ACCESS TO NON-PRIVILEGED ACCOUNTS - REPLAY RESISTANT* |  |
| IA-2(10) | *IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | SINGLE SIGN-ON* |  |
| IA-2(11) | *IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | REMOTE ACCESS - SEPARATE DEVICE* |  |
| IA-2(12) | *IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | ACCEPTANCE OF PIV CREDENTIALS* |  |
| IA-2(13) | *IDENTIFICATION AND AUTHENTICATION | OUT-OF-BAND AUTHENTICATION* |  |
| **IR-1** | **Incident Response Policy and Procedures** |  |
| **IR-2** | **Incident Response Training** |  |
| IR-2(1) | *INCIDENT RESPONSE TRAINING | SIMULATED EVENTS* |  |
| IR-2(2) | *INCIDENT RESPONSE TRAINING | AUTOMATED TRAINING ENVIRONMENTS* |  |
| **MA-1** | **System Maintenance Policy and Procedures** |  |
| **MA-2** | **Controlled Maintenance** |  |
| MA-2(1) | *CONTROLLED MAINTENANCE | RECORD CONTENT* |  |
| **MP-1** | **Media Protection Policy and Procedures** |  |
| **MP-2** | **Media Access** |  |
| MP-2(1) | *MEDIA ACCESS | AUTOMATED RESTRICTED ACCESS* |  |
| MP-2(2) | *MEDIA ACCESS | CRYPTOGRAPHIC PROTECTION* |  |
| **PE-1** | **Physical and Environmental Protection Policy and Procedures** |  |
| **PE-2** | **Physical Access Authorizations** |  |
| PE-2(1) | *PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION / ROLE* |  |
| PE-2(2) | *PHYSICAL ACCESS AUTHORIZATIONS | TWO FORMS OF IDENTIFICATION* |  |
| PE-2(3) | *PHYSICAL ACCESS AUTHORIZATIONS | RESTRICT UNESCORTED ACCESS* |  |
| **PL-1** | **Security Planning Policy and Procedures** |  |
| **PL-2** | **System Security Plan** |  |
| PL-2(1) | *SYSTEM SECURITY PLAN | CONCEPT OF OPERATIONS* |  |
| PL-2(2) | *SYSTEM SECURITY PLAN | FUNCTIONAL ARCHITECTURE* |  |
| PL-2(3) | *SYSTEM SECURITY PLAN | PLAN / COORDINATE WITH OTHER ORGANIZATIONAL ENTITIES* |  |
| **PS-1** | **Personnel Security Policy and Procedures** |  |
| **PS-2** | **Position Risk Designation** |  |
| **PS-3** | **Personnel Screening** |  |
| PS-3(1) | *PERSONNEL SCREENING | CLASSIFIED INFORMATION* |  |
| PS-3(2) | *PERSONNEL SCREENING | FORMAL INDOCTRINATION* |  |
| PS-3(3) | *PERSONNEL SCREENING | INFORMATION WITH SPECIAL PROTECTION MEASURES* |  |
| **RA-1** | **Risk Assessment Policy and Procedures** |  |
| **RA-2** | **Security Categorization** |  |
| **SA-1** | **System and Services Acquisition Policy and Procedures** |  |
| **SA-2** | **Allocation of Resources** |  |
| **SC-1** | **System and Communications Protection Policy and Procedures** |  |
| **SC-2** | **Application Partitioning** |  |
| SC-2(1) | *APPLICATION PARTITIONING | INTERFACES FOR NON-PRIVILEGED USERS* |  |
| **SI-1** | **System and Information Integrity Policy and Procedures** |  |
| **SI-2** | **Flaw Remediation** |  |
| SI-2(1) | *FLAW REMEDIATION | CENTRAL MANAGEMENT* |  |
| SI-2(2) | *FLAW REMEDIATION | AUTOMATED FLAW REMEDIATION STATUS* |  |
| SI-2(3) | *FLAW REMEDIATION | TIME TO REMEDIATE FLAWS / BENCHMARKS FOR CORRECTIVE ACTIONS* |  |
| SI-2(4) | *FLAW REMEDIATION | AUTOMATED PATCH MANAGEMENT TOOLS* |  |
| SI-2(5) | *FLAW REMEDIATION | AUTOMATIC SOFTWARE / FIRMWARE UPDATES* |  |
| SI-2(6) | *FLAW REMEDIATION | REMOVAL OF PREVIOUS VERSIONS OF SOFTWARE / FIRMWARE* |  |