System Security Plan (SSP)

Prepared in accordance with NIST SP 800-18 Rev. 1 (FISMA)

System Name: **[System Name]**

Version: **[Version]**

Date: **[Date]**

Authorizing Official (AO): **[Authorizing Official]**

Information System Security Officer (ISSO): **[ISSO]**

Information Security Officer (ISO): **[ISO]**

# 1. System Identification

1.1 System Name / Acronym:

**[System Name / Acronym]**

1.2 Unique System Identifier (Asset ID or similar):

**[Unique System Identifier]**

1.3 Responsible Organization:

**[Responsible Organization]**

1.4 Information Owner (Name/Title/Org):

**[Information Owner]**

1.4 System Owner (Name/Title/Org):

**[System Owner]**

1.5 Authorizing Official (Name/Title/Org):

**[Authorizing Official]**

1.6 Information System Security Officer (ISSO):

**[ISSO]**

1.7 Other Key Contacts (Custodian, Privacy, etc.):

**[Other Contacts]**

1.8 System Operational Status:

**[ ]** Operational / **[ ]** Under Development / **[ ]** Major Modification

1.9 Information System Type:

**[ ]** Major Application / **[ ]** General Support System / **[ ]** Minor Application

# 2. System Categorization (FIPS 199)

Confidentiality Impact: **[ ]** Low / **[ ]** Moderate / **[ ]** High

Integrity Impact: **[ ]** Low / **[ ]** Moderate / **[ ]** High

Availability Impact: **[ ]** Low / **[ ]** Moderate / **[ ]** High

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

Information Types and FIPS 199 rationale (reference to FIPS 200 / NIST SP 800-60 mappings as applicable):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Information Type | C | I | A | Notes |
|  |  |  |  |  |

# 3. System Description and Purpose

[Provide the mission/business purpose, primary functions, users, and data sensitivity.]

# 4. System Environment and Architecture

4.1 Authorization Boundary Description:

[Provide a description of the authorization boundary.]

4.2 System Components (hardware/software/services):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Component | Type | Version | Hosting/Location | Owner |
|  |  |  |  |  |

4.3 Network/Architecture Diagram(s): **[Attach/Reference]**

4.4 Data Flow(s): **[Attach/Reference]**

4.5 External Services / Cloud Dependencies (e.g., IaaS/PaaS/SaaS):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Provider | Service | Fed/Gov/TX-RAMP / etc. | Inherited Controls | Contract/Agreement Ref |
|  |  |  |  |  |

# 5. System Interconnections and Information Sharing

List each external system, the data exchanged, protection mechanisms, and agreement type (e.g., ISA/MOU/SLA).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Partner System | Interface | Data Exchanged | Agreement Type | Security Controls |
|  |  |  |  |  |

# 6. Applicable Laws, Regulations, Standards, and Policies

Identify applicable requirements (e.g., FISMA, OMB A-130, TAC 202, DIR SCSC, NIST SP 800-53, agency/system policies).

|  |  |  |
| --- | --- | --- |
| Source | Citation/ID | Applicability/Notes |
|  |  |  |

# 7. Minimum Security Controls and Tailoring

Describe the control baseline and tailoring decisions. Include scoping, compensating controls, and inheritance sources.

|  |  |  |
| --- | --- | --- |
| Decision | Rationale | Reference |
|  |  |  |

## 7.1 TAMUS Standard Inheritance (Pre-Filled – Adjust as Needed)

The following organization-wide services typically provide inherited control implementations. Validate applicability, update providers/agreements, and map to specific control IDs in Section 8.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Service / Capability** | **Provider / Owner** | **Typical Families** | **Notes / Agreements** | **Evidence Pointers** |
| Information Security Awareness Training Course 3001 | TAMUS Cybersecurity | AT |  |  |
| TrainTraq | TAMUS System Enterprise Applications | AT |  |  |
| Identity & Access Management (SSO/MFA) | TAMUS Central IT (adjust) | AC, IA, PL | Enterprise IAM policy; federation agreements | IdP config, MFA policy, onboarding/offboarding records |
| Network Security (Firewalls/Segmentation/IDS) | TAMUS Network Services (adjust) | AC, SC, SI, CA | Network security standard; managed firewall service agreement | FW rulesets, IDS alerts, network diagrams |
| Endpoint Protection (EDR/AV/Hardening) | TAMUS Endpoint Services (adjust) | CM, SI, SC | Managed EDR/AV standard; endpoint baseline | EDR console, baseline checklist |
| Vulnerability & Patch Management | TAMUS Security Operations (adjust) | RA, SI, CM | Scanning service standard; patch SLAs | Scanner reports, remediation tickets |
| Central Logging & SIEM | TAMUS Security Operations (adjust) | AU, SI, IR, CA | Logging/SIEM standard; onboarding guide | Syslog configs, SIEM dashboards |
| Backup & Disaster Recovery | TAMUS Infrastructure (adjust) | CP, MP | Backup policy; recovery objectives (RTO/RPO) | Backup job logs, restore tests |
| Secure Configuration Baselines | TAMUS Governance (adjust) | CM, SA | Baseline hardening guides; change control process | Baseline docs, change records |
| Cloud Hosting (IaaS/PaaS/SaaS) | Cloud Provider + TAMUS (adjust) | SA, SC, CP, IR, AU | Contracts, shared responsibility model, FedRAMP/AICPA reports | SSP summaries, SOC 2, FedRAMP ATO |

Guidance: In Section 8, mark applicable controls as Inherited = 'Y' and set 'Inherited From' to the specific service above.

# 8. Control Implementation Summary (from TAMUS OSCAL Catalog)

The following table enumerates ONLY the required controls included in the provided OSCAL catalog. For each control, provide system-specific implementation, inheritance, responsible roles, status, and evidence.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Control ID | Control Title | Implementation (How) | Inherited? (Y/N) | Inherited From | Parameters / ODPs | Responsible Role(s) | Status (Impl/Planned/NA) | Evidence / Artifacts | Comments |
| AC-1 | Policy and Procedures |  |  |  |  |  |  |  |  |
| AC-2 | Account Management |  |  |  |  |  |  |  |  |
| AC-3 | Access Enforcement |  |  |  |  |  |  |  |  |
| AC-5 | Separation of Duties |  |  |  |  |  |  |  |  |
| AC-6 | Least Privilege |  |  |  |  |  |  |  |  |
| AC-7 | Unsuccessful Logon Attempts |  |  |  |  |  |  |  |  |
| AC-8 | System Use Notification |  |  |  |  |  |  |  |  |
| AC-11 | Device Lock |  |  |  |  |  |  |  |  |
| AC-14 | Permitted Actions Without Identification or Authentication |  |  |  |  |  |  |  |  |
| AC-17 | Remote Access |  |  |  |  |  |  |  |  |
| AC-18 | Wireless Access |  |  |  |  |  |  |  |  |
| AC-19 | Access Control for Mobile Devices |  |  |  |  |  |  |  |  |
| AC-20 | Use of External Systems |  |  |  |  |  |  |  |  |
| AC-22 | Publicly Accessible Content |  |  |  |  |  |  |  |  |
| AT-1 | Policy and Procedures | We have a policy. | N |  |  | Human Resources | Implemented |  |  |
| AT-2 | Literacy Training and Awareness | Employees are required to complete Course 3001 upon hire and annually thereafter. | Y | Information Security Awareness Training Course 3001 |  | Human Resources | Implemented | TrainTraq Records |  |
| AT-3 | Role-based Training |  |  |  |  |  |  |  |  |
| AT-4 | Training Records |  | Y | TrainTraq |  |  |  |  |  |
| AU-1 | Policy and Procedures |  |  |  |  |  |  |  |  |
| AU-2 | Event Logging |  |  |  |  |  |  |  |  |
| AU-3 | Content of Audit Records |  |  |  |  |  |  |  |  |
| AU-4 | Audit Log Storage Capacity |  |  |  |  |  |  |  |  |
| AU-5 | Response to Audit Logging Process Failures |  |  |  |  |  |  |  |  |
| AU-6 | Audit Record Review, Analysis, and Reporting |  |  |  |  |  |  |  |  |
| AU-8 | Time Stamps |  |  |  |  |  |  |  |  |
| AU-9 | Protection of Audit Information |  |  |  |  |  |  |  |  |
| AU-11 | Audit Record Retention |  |  |  |  |  |  |  |  |
| AU-12 | Audit Record Generation |  |  |  |  |  |  |  |  |
| CA-1 | Policy and Procedures |  |  |  |  |  |  |  |  |
| CA-2 | Control Assessments |  |  |  |  |  |  |  |  |
| CA-3 | Information Exchange |  |  |  |  |  |  |  |  |
| CA-5 | Plan of Action and Milestones |  |  |  |  |  |  |  |  |
| CA-6 | Authorization |  |  |  |  |  |  |  |  |
| CA-7 | Continuous Monitoring |  |  |  |  |  |  |  |  |
| CA-8 | Penetration Testing |  |  |  |  |  |  |  |  |
| CA-9 | Internal System Connections |  |  |  |  |  |  |  |  |
| CM-1 | Policy and Procedures |  |  |  |  |  |  |  |  |
| CM-2 | Baseline Configuration |  |  |  |  |  |  |  |  |
| CM-3 | Configuration Change Control |  |  |  |  |  |  |  |  |
| CM-4 | Impact Analyses |  |  |  |  |  |  |  |  |
| CM-5 | Access Restrictions for Change |  |  |  |  |  |  |  |  |
| CM-6 | Configuration Settings |  |  |  |  |  |  |  |  |
| CM-7 | Least Functionality |  |  |  |  |  |  |  |  |
| CM-8 | System Component Inventory |  |  |  |  |  |  |  |  |
| CM-10 | Software Usage Restrictions |  |  |  |  |  |  |  |  |
| CM-11 | User-installed Software |  |  |  |  |  |  |  |  |
| CP-1 | Policy and Procedures |  |  |  |  |  |  |  |  |
| CP-2 | Contingency Plan |  |  |  |  |  |  |  |  |
| CP-3 | Contingency Training |  |  |  |  |  |  |  |  |
| CP-4 | Contingency Plan Testing |  |  |  |  |  |  |  |  |
| CP-6 | Alternate Storage Site |  |  |  |  |  |  |  |  |
| CP-8 | Telecommunications Services |  |  |  |  |  |  |  |  |
| CP-9 | System Backup |  |  |  |  |  |  |  |  |
| CP-10 | System Recovery and Reconstitution |  |  |  |  |  |  |  |  |
| CP-11 | Alternate Communications Protocols |  |  |  |  |  |  |  |  |
| IA-1 | Policy and Procedures |  |  |  |  |  |  |  |  |
| IA-2 | Identification and Authentication (Organizational Users) |  |  |  |  |  |  |  |  |
| IA-4 | Identifier Management |  |  |  |  |  |  |  |  |
| IA-5 | Authenticator Management |  |  |  |  |  |  |  |  |
| IA-6 | Authentication Feedback |  |  |  |  |  |  |  |  |
| IA-7 | Cryptographic Module Authentication |  |  |  |  |  |  |  |  |
| IA-8 | Identification and Authentication (Non-organizational Users) |  |  |  |  |  |  |  |  |
| IA-11 | Re-authentication |  |  |  |  |  |  |  |  |
| IA-12 | Identity Proofing |  |  |  |  |  |  |  |  |
| IR-1 | Policy and Procedures |  |  |  |  |  |  |  |  |
| IR-2 | Incident Response Training |  |  |  |  |  |  |  |  |
| IR-3 | Incident Response Testing |  |  |  |  |  |  |  |  |
| IR-4 | Incident Handling |  |  |  |  |  |  |  |  |
| IR-5 | Incident Monitoring |  |  |  |  |  |  |  |  |
| IR-6 | Incident Reporting |  |  |  |  |  |  |  |  |
| IR-7 | Incident Response Assistance |  |  |  |  |  |  |  |  |
| IR-8 | Incident Response Plan |  |  |  |  |  |  |  |  |
| IR-9 | Information Spillage Response |  |  |  |  |  |  |  |  |
| MA-1 | Policy and Procedures |  |  |  |  |  |  |  |  |
| MA-2 | Controlled Maintenance |  |  |  |  |  |  |  |  |
| MA-4 | Nonlocal Maintenance |  |  |  |  |  |  |  |  |
| MA-5 | Maintenance Personnel |  |  |  |  |  |  |  |  |
| MP-1 | Policy and Procedures |  |  |  |  |  |  |  |  |
| MP-2 | Media Access |  |  |  |  |  |  |  |  |
| MP-3 | Media Marking |  |  |  |  |  |  |  |  |
| MP-6 | Media Sanitization |  |  |  |  |  |  |  |  |
| MP-7 | Media Use |  |  |  |  |  |  |  |  |
| PE-1 | Policy and Procedures |  |  |  |  |  |  |  |  |
| PE-2 | Physical Access Authorizations |  |  |  |  |  |  |  |  |
| PE-3 | Physical Access Control |  |  |  |  |  |  |  |  |
| PE-6 | Monitoring Physical Access |  |  |  |  |  |  |  |  |
| PE-8 | Visitor Access Records |  |  |  |  |  |  |  |  |
| PE-12 | Emergency Lighting |  |  |  |  |  |  |  |  |
| PE-13 | Fire Protection |  |  |  |  |  |  |  |  |
| PE-14 | Environmental Controls |  |  |  |  |  |  |  |  |
| PE-15 | Water Damage Protection |  |  |  |  |  |  |  |  |
| PE-16 | Delivery and Removal |  |  |  |  |  |  |  |  |
| PE-17 | Alternate Work Site |  |  |  |  |  |  |  |  |
| PE-18 | Location of System Components |  |  |  |  |  |  |  |  |
| PL-1 | Policy and Procedures |  |  |  |  |  |  |  |  |
| PL-2 | System Security and Privacy Plans |  |  |  |  |  |  |  |  |
| PL-4 | Rules of Behavior |  |  |  |  |  |  |  |  |
| PL-10 | Baseline Selection |  |  |  |  |  |  |  |  |
| PL-11 | Baseline Tailoring |  |  |  |  |  |  |  |  |
| PM-1 | Information Security Program Plan |  |  |  |  |  |  |  |  |
| PM-2 | Information Security Program Leadership Role |  |  |  |  |  |  |  |  |
| PM-3 | Information Security and Privacy Resources |  |  |  |  |  |  |  |  |
| PM-4 | Plan of Action and Milestones Process |  |  |  |  |  |  |  |  |
| PM-5 | System Inventory |  |  |  |  |  |  |  |  |
| PM-6 | Measures of Performance |  |  |  |  |  |  |  |  |
| PM-7 | Enterprise Architecture |  |  |  |  |  |  |  |  |
| PM-9 | Risk Management Strategy |  |  |  |  |  |  |  |  |
| PM-10 | Authorization Process |  |  |  |  |  |  |  |  |
| PM-14 | Testing, Training, and Monitoring |  |  |  |  |  |  |  |  |
| PM-15 | Security and Privacy Groups and Associations |  |  |  |  |  |  |  |  |
| PM-16 | Threat Awareness Program |  |  |  |  |  |  |  |  |
| PS-1 | Policy and Procedures |  |  |  |  |  |  |  |  |
| PS-2 | Position Risk Designation |  |  |  |  |  |  |  |  |
| PS-3 | Personnel Screening |  |  |  |  |  |  |  |  |
| PS-4 | Personnel Termination |  |  |  |  |  |  |  |  |
| PS-5 | Personnel Transfer |  |  |  |  |  |  |  |  |
| PS-6 | Access Agreements |  |  |  |  |  |  |  |  |
| PS-7 | External Personnel Security |  |  |  |  |  |  |  |  |
| PS-8 | Personnel Sanctions |  |  |  |  |  |  |  |  |
| PS-9 | Position Descriptions |  |  |  |  |  |  |  |  |
| RA-1 | Policy and Procedures |  |  |  |  |  |  |  |  |
| RA-2 | Security Categorization |  |  |  |  |  |  |  |  |
| RA-3 | Risk Assessment |  |  |  |  |  |  |  |  |
| RA-5 | Vulnerability Monitoring and Scanning |  |  |  |  |  |  |  |  |
| RA-7 | Risk Response |  |  |  |  |  |  |  |  |
| SA-1 | Policy and Procedures |  |  |  |  |  |  |  |  |
| SA-2 | Allocation of Resources |  |  |  |  |  |  |  |  |
| SA-3 | System Development Life Cycle |  |  |  |  |  |  |  |  |
| SA-4 | Acquisition Process |  |  |  |  |  |  |  |  |
| SA-5 | System Documentation |  |  |  |  |  |  |  |  |
| SA-8 | Security and Privacy Engineering Principles |  |  |  |  |  |  |  |  |
| SA-9 | External System Services |  |  |  |  |  |  |  |  |
| SA-10 | Developer Configuration Management |  |  |  |  |  |  |  |  |
| SA-11 | Developer Testing and Evaluation |  |  |  |  |  |  |  |  |
| SA-22 | Unsupported System Components |  |  |  |  |  |  |  |  |
| SC-1 | Policy and Procedures |  |  |  |  |  |  |  |  |
| SC-5 | Denial-of-service Protection |  |  |  |  |  |  |  |  |
| SC-7 | Boundary Protection |  |  |  |  |  |  |  |  |
| SC-8 | Transmission Confidentiality and Integrity |  |  |  |  |  |  |  |  |
| SC-12 | Cryptographic Key Establishment and Management |  |  |  |  |  |  |  |  |
| SC-13 | Cryptographic Protection |  |  |  |  |  |  |  |  |
| SC-15 | Collaborative Computing Devices and Applications |  |  |  |  |  |  |  |  |
| 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 |  |  |  |  |  |  |  |  |
| SC-39 | Process Isolation |  |  |  |  |  |  |  |  |
| SI-1 | Policy and Procedures |  |  |  |  |  |  |  |  |
| SI-2 | Flaw Remediation |  |  |  |  |  |  |  |  |
| SI-3 | Malicious Code Protection |  |  |  |  |  |  |  |  |
| SI-4 | System Monitoring |  |  |  |  |  |  |  |  |
| SI-5 | Security Alerts, Advisories, and Directives |  |  |  |  |  |  |  |  |
| SI-10 | Information Input Validation |  |  |  |  |  |  |  |  |
| SI-12 | Information Management and Retention |  |  |  |  |  |  |  |  |
| 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-8 | Notification Agreements |  |  |  |  |  |  |  |  |
| SR-12 | Component Disposal |  |  |  |  |  |  |  |  |

[[CONTROL\_TABLE\_MARKER\_DO\_NOT\_REMOVE]]

# 9. Continuous Monitoring Strategy

[Summarize monitoring frequencies, metrics, automation tooling, and reporting (e.g., dashboards, CA-7).]

# 10. Incident Response

[Reference IR roles, playbooks, reporting/escalation paths, and testing cadence.]

# 11. Configuration Management

[Describe CM policies, baselines, change control process, and tools.]

# 12. Contingency Planning

[Summarize CP roles, BIA reference, backup/restore, and exercise/testing results.]

# 13. Privacy

[Describe privacy roles, PIAs, data minimization, consent, and individual participation.]

# 14. Risk Summary and POA&M

[Summarize known risks and link to the current Plan of Action & Milestones (POA&M).]

# 15. Roles and Responsibilities

|  |  |  |  |
| --- | --- | --- | --- |
| Role | Name/Org | Responsibilities | Contact |
|  |  |  |  |

# 16. Revision and Approval History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Changes | Prepared By | Reviewed/Approved By |
|  |  |  |  |  |

# Appendix A – Acronyms

List acronyms and abbreviations used in this SSP.

# Appendix B – References

Include references to NIST SP 800-18 Rev. 1, SP 800-53 Rev. 5, FIPS 199/200, TAC 202, DIR Security Control Standards Catalog, and organizational policies.

# Appendix C – Diagrams and Attachments

Insert or reference architecture/network/data flow diagrams and other attachments.