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** |
| 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 |

[[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.