System Security Plan (SSP) Template

State of Arizona - System Security Plan Template

AUTHORITY
To effectuate the mission and purposes of the Arizona Department of Homeland Security Cyber Command, the Agency shall establish a coordinated plan and program for information technology (IT) implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (A.R.S.)§ 18-104 and § 41-4282. Reference Statewide Policy Frameworks.

The following template may be utilized to create a State of Arizona System Security Plan (SSP).

The successful completion of this SSP will involve a coordinated effort between the agency data owner, program manager/planner, agency IT staff, and key members from the Contractor or Vendor development teams as appropriate.

State of Arizona IT and Information Security guidance and specific references listed throughout this template are a brief synopsis of requirements for convenience purposes only.
State agency staff and all contractor/vendor employees working to develop this SSP must read in full and provide required SSP elements from the following:

Standard S8120: Statewide Information Security Program
Policy P8120: Statewide Information Security Program
Policy P8110: Statewide Data Classification Policy
Policy P8230: Contingency Planning Policy

SSP development between agency and contractor takes time and effort by all parties involved. **"Do Not"** wait to begin this process. Much of the required information within this SSP should have been well thought through during the project planning phase and long before any contractor/vendor selection process takes place.

All projects involving the transfer, processing, and/or storage of state data outside of state managed and controlled environments will require **Arizona Risk and Authorization Management Program (AZRAMP) Authorization** with SSP Approval from the Arizona Department of Homeland Security, Cyber Command.

Please contact your agency IT department or agency assigned ADOA Engagement Managers for further information on specific AZRAMP & SSP requirements.

For specific information related to AZRAMP & SSP's not found elsewhere, please contact: GRC@azdohs.gov

High Level Architecture Data Flow diagrams are required for all projects involving contractor connections to state networks, transfer, processing, storage of state data to an outside environment, and internal systems updates/modifications. Please refer to the sample diagrams and guidance at the end of this document.

The Initial Required areas for PIJ submission are denoted by an asterisk and should be provided by the designated BU's, designated ISO or information security team in conjunction with a PIJ submission.

State of Arizona System Security Plan

State System Name/Title * : *Unique identifier and name of the state information system.*

State Contract or Project Investment Justification Number * : *Unique identifier issued by the State Procurement Office (SPO) or issued via the PIJ program.*

Information System Owner * : *[Assign an owner to the identified state information system. An owner must be a state employee and has the overall responsibility for procurement, development, integration, modification, or operation and maintenance of the state information system.]*

Authorizing Official*: [Document the authorizing official for the state information system. An authorizing official has the authority to formally assume responsibility for operating the state information system at an acceptable level of risk to BU operations or assets.]*

	State Information System Owner	Authorizing Official
Name		
Title		
Agency		
Address		
Email Address		
Phone Number		

System Security Plan (SSP) Template

Vendor/Contractor Information

Executive Level Contact: *[List the contact information for key executive level authority (Owner, President, VP) of the organization responsible with the services, operations and/or maintenance of the state information system.]*

Information Technology Security Contact*: [List the Contact Information for Senior IT Security (CISO, VP of IT, ISO) personnel assigned to security responsibilities with the state information system.]*

Privacy/Compliance Contact*: [List the Contact Information for Senior Privacy/Compliance Officer (CPO, PO, VP) personnel assigned to Privacy/Compliance responsibilities with the state information system.]*

NOTE: No two positions can contain the same contact information. If a Managed Service Provider is utilized for IT and/or Privacy/Compliance please include below.

	Owner/Executive	IT Security Officer	Privacy/Compliance Officer
Name			
Title			
Company			
Address			
Email Address			
Phone Number, Ext.			
Website			
Other			
24/7 Emergency Contacts			
Name			
Phone			
Email			

Arizona Risk and Authorization Management Program (AZRAMP)

AZRAMP: *[All projects involving the transfer, processing, and/or storage of state data outside state managed and controlled environments require AZRAMP Authorization with SSP Approval from the Arizona Department of Homeland Security, Cyber Command.* *Refer to Information Security Program Standard (S8120), requirements 6.3, 6.3.1, 6.3.2, 6.3.3, 6.3.4]*

State Data Transfer (select one) Does this project involve state data transferred, processed or stored to a vendor/contractor Cloud environment including vendor/contractor managed SaaS, IaaS, PaaS	
YES (continue with next section below)	**NO** (skip to Security Risk Management section)
○	○

State Data Transfer (Cont.) If "YES" was selected above, please identify current security authorizations NOTE: ISO/IEC, SOC II & III, or other forms of Self-Attestations are "NOT" recognized or accepted.				
Certification	**Authorized**	**Pending/Ready**	**In Process**	**None**
FedRAMP				
StateRAMP				
AZRamp				

Security Risk Management

Impact Assessment * : *[Assign below the Impact Assessment results of the identified state information system according to the requirements in the* Information Security Program Policy (P8120), requirements 6.3.1]

Impact Assessment Results (select one)	
Limited Adverse Impact	**Serious Adverse Impact**

System Security Plan (SSP) Template

Security Risk Assessment * : [Use the Business Risk Determination Questionnaire located HERE to complete the below Risk Scores. Attach a copy of the Questionnaire to the last page of this SSP. Refer to the Information Security Program Policy (P8120), requirements 6.3.4]

Security Risk Assessment Questionnaire	
Category	**Risk Score**
Confidentiality	
Integrity	
Availability	
Overall Risk Score	

State System Categorization * : *[Assign a single system categorization to the identified state information system according to the requirements in the* Information Security Program Policy (P8120), requirements 6.3.3]

System Categorization Level (select one)	
Standard	**Protected**

Data Classification * : *[Assign below Data Classification involved that will be created, stored, processed or transmitted to/from the identified state information system according to the requirements in the* Data Classification Policy (P8110), requirements 6.2 - 6.3]

Data Classification Level (select one)	
Public	**Confidential**

Data Elements/Types * : *[Identify all Data Elements/Types that will be created, stored, processed or transmitted to/from the identified State information system according to the requirements in the* Data Classification Policy (P8110), requirements 6.2.1 a. - n.]

Data Elements/Types Select all that apply with **"X"** (refer to P8110 for full description)					
a. SSP&V		f. EP		k. LCS & II	
b. PHI/ePHI		g. RA & SAR		l. OSoCD	
c. FAD(I)		h. PII & SSN		m. ONsoCD	
d. CJI		i. FTI		n. ORPbL	
e. CI/FFR		j. CUI		*Please describe ORPbL:*	

State Information System Operational Status*: [Indicate the current operational status of the state information system. If required, indicate specific parts or subsystems of the state information system if more than one status is selected.]*

	System Name	Subsystem Name (If needed)
◯ Operational		
◯ Under Development		
◯ Major Modification		

Information System Type*:*

Use this area to: *[Indicate the type of system: Major Application – An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application; or General Support System – An interconnected set of information resources under the same direct management control that shares common functionality (including hardware, software, information, data, minor applications, communications, and people).]*

General System Description / Purpose*:*

Use this area to: *[Describe the function or purpose of the system and the information processes.]*

System Environment * *:*

Use this area to: *[Provide a general technical description of the state information system. Include hardware, software, and communications equipment.]*

System Interconnections / Information Sharing:

***[List interconnected systems and system identifiers**, indicate if there is an agreement on file (e.g., Information Sharing Agreement, Memorandum of Understanding, Service Level Agreement, HIPAA BAA, or other agreement), date of agreement, and name of authorizing official.]*

System Name	Business Unit	Type	Agreement	Date	Official

Related Laws / Regulations / Policies:
Use this area to: *[List any laws or regulations that establish specific security or privacy requirements for the state information system or data residing on the system. State PSPs may be used for guidance but only include relevant and applicable laws and regulations.]*

Minimum Security Control Exceptions*:*
Use below boxes to indicate: *[Minimum Security Controls are based on the categorization of the system and the statewide security and privacy policy set.* List any exceptions with the statewide security and privacy policies below or planned controls (e.g., controls not yet in place but budgeted and planned, together with rationale, compensating controls for the exception, and expected date of implementation for planned controls.]

Policy #	Policy Name	Exceptions	Compensating Controls	Rationale for Exception
P8110	Data Classification	None		
P8120	Information Security Program	None		

P8130	System Security Acquisition	None		
P8210	Security Awareness Training	None		
P8220	System Security Maintenance	None		
P8230	Contingency Planning	None		
P8240	Incident Response Planning	None		
P8250	Media Protection Policy	None		
P8260	Physical Protections	None		
P8270	Personnel Security Controls	None		
P8280	Acceptable Use	None		
P8310	Account Management	None		
P8320	Access Control	None		
P8330	System Security Audit	None		
P8340	Identification and Authentication	None		
P8350	System and Communication Protection	None		
P8410	System Privacy	None		

State Information System Security Plan Dates: *[List completion date of plan, approval date of plan, along with* approver.*]*

	Security Plan Completion	AZDOHS Security Plan Approval
Name		
Title		
Date		

SAMPLE REFERENCES DATA FLOW DIAGRAMS

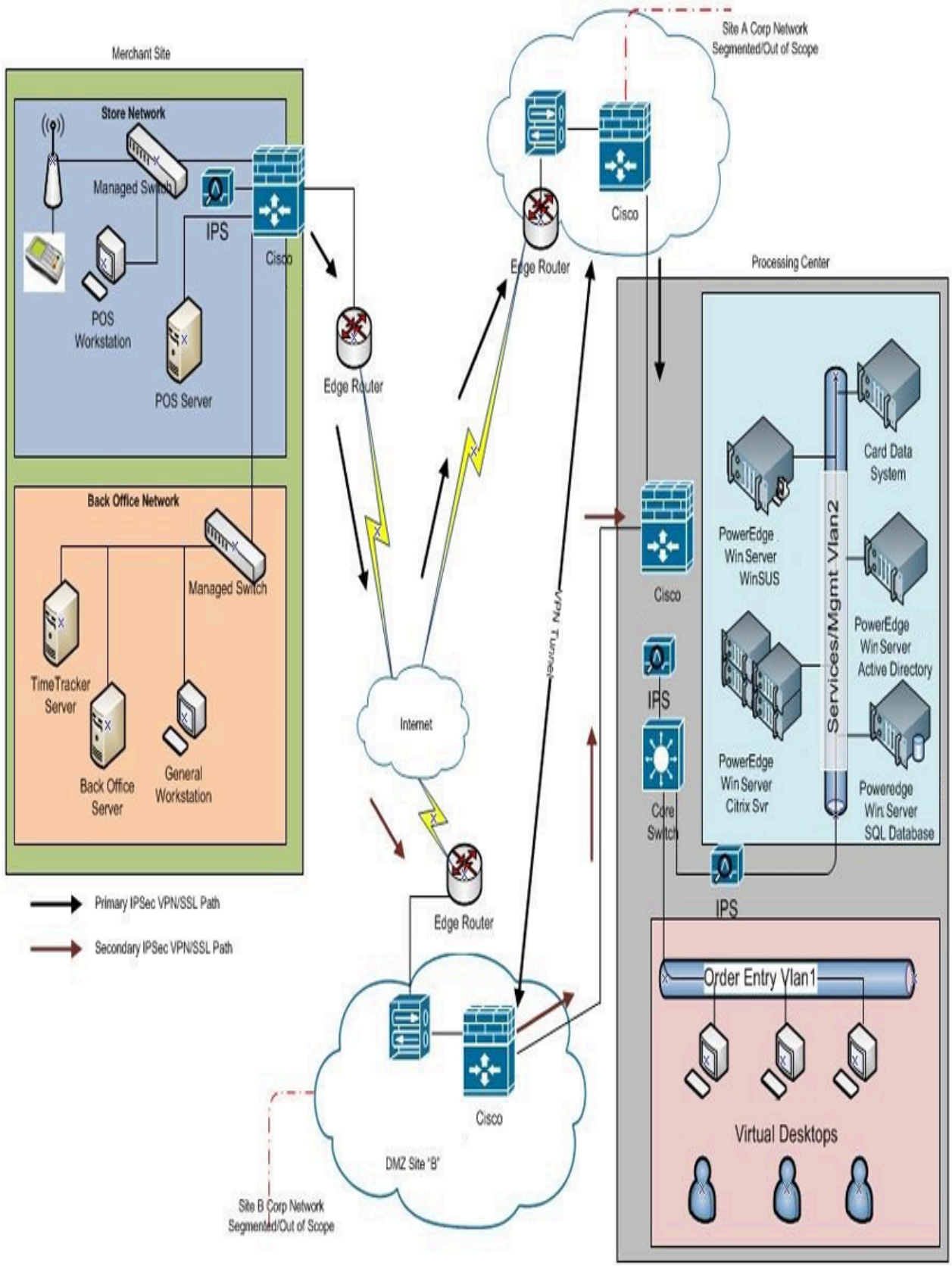
The following information is for reference purposes to assist in the development of IT Dataflow Architectural Diagrams.

Designing Network Diagrams begin with Layer 3, which show the IP subnets and all Layer 3 network devices like routers, firewalls, load balancers and encryption in transit/at rest. The Layer 3 diagram must show all of the important network segments and subnets and how they're interconnected.

Network diagramming rules and tips:

- Layout is important and should represent the flow of traffic in a broad sense. Another layout consideration is to always draw your network segments either horizontally or vertically.
- The Layer 3 diagram should show any high availability mechanisms and redundant network components or redundant paths. It's customary to show router redundancy protocols as an elongated ellipse that covers the router links included in the high availability group.
- The other important thing about Layer 3 diagrams is that they should only include Layer 3 objects. You can show a switch on a Layer 3 diagram only if it's a Layer 3 switch, and then only because it functions as a router.
- Another useful thing to put into a Layer 3 diagram is organizational boxes. If there are security zones or interesting groupings of users by function or servers by application, put them together on the picture, put a box around them, and label the box clearly. It's then easy to see the exact network path those users take to reach their servers.
- In more complicated network designs, use a base Layer 3 diagram showing the VLANs, routers, and firewalls. Then create several other diagrams to lay over the base diagram.

System Security Plan (SSP) Template



Updated: 1/26/26

Attach Copy of Business Risk Questionnaire Here

Risk Determination Questionnaire located HERE