Tailoring PSP Templates Guide

Introduction

This guide was developed to assist those assisting Budget Units (BU) in the tailoring of PSP Templates into BU policies. The guide provides general guidance for all BUs and where appropriate specific guidance for "small agencies" vs. "large agencies". It is envisioned that this guide be continually updated and shared within the group that is providing assistance. The majority of updates and expansions to this guide are expected in the FAQ section.

Suggested Discussion with BU

Individual BUs may have a myriad of questions or concerns regarding the PSP tailoring project. However, they may not know where to begin in discussing the project. The following discussion outline, Table 1, has been useful in the discussions with other BUs and is documented below as a suggested discussion agenda.

Topic	Instructions	Discussion
Systems Discussion	Talk to the BU about the number and type of systems they have.	**Single System**: Smaller BUs will benefit from calling all of their system components (e.g., servers, laptops, web apps, etc.) a single system. This greatly simplifies the process.
		User of Others Systems: BUs that are given a login to another agency's or another company's system may typically consider that system to be owned by the other agency or company. Examples include e-banking, application service providers (e.g., salesforce.com), and systems run by other agencies in fulfillment of the other agency's mission.
Sensitive Data Discussion	Talk to the BU about any sensitive data they may have.	If the BUs system contains any confidential data then all requirements (standard system requirements and protected system requirements – indicated with a (P) apply. Many BUs will simply know that they have sensitive data and that can end the discussion but for those BUs that are not sure ask specifically about the following types of data that may be on their systems. - **Medical Records**. Many licensing boards in the medical profession have these records. - **Card Holder Data (CHD).** If the BU has a merchant ID, then they need to comply with PCI DSS. If they don't know if they have a merchant ID they should check with their finance person. Note: Many agencies have their credit card processing run through a state system in which the state retains the merchant id (and has a sub ID for each agency). If this is the BUs only credit card processing then they do not need to comply with

Tailoring PSP Templates Guide

Topic	Instructions	Discussion
		PCI DSS and they may not have CHD in their system. - **Other**. Ask the BU what other information their system stores, transmits or processes that may be considered confidential.
The PSP Tailoring Project	If the BU has any questions regarding the project, discuss them here.	**Due dates**. The Draft policies are due from each BU by July 1. If the BU has any exceptions to the PSP Template then they will indicate the exception in the associated policy in section 4. With each exception the BU shall indicate the requirement number and the requested change. If the requested change is a strengthening of the requirement nothing else is required. If the requested change is not then the BU shall include a description of compensating controls or a risk-based rationale of why the change makes sense.
		Out-Sourced & External Services. Many BUs why they need to create policies if they outsource all the administration of the systems to someone else (e.g., DOA). Let them know that the BU is responsible for the protection of their data. If they choose to outsource these functions they need to ensure that the entity they outsource it to is required to protect the data. The policies do not need to be modified depending on who administers the systems. You may point them to the following: P8130 System Acquisition Policy. - [6.3] when outsourcing, contracts must include security requirements - [6.6] the BU must implement a service level agreement and provide oversight of this agreement.

Tailoring PSP Templates Guide

Topic	Instructions	Discussion
Writing the policies	To write the BUs policies the following steps are required	1) Globally replace " BU " in each document with the name of the agency. 2) Define/specify parameters and/or values for each requirement with the phrase "BU-defined" or "BU-specified". There are 34 such instances. This guide provides a reference and a discussion for each of these instances in Table 2. 3) Confirm adoption of each requirement OR request a policy exception. This is done in section 4 of each policy and must have either a) a list of compensating controls or b) a risk rationale for each requested policy exception. 4) Email your draft policies to your DOA liaison by July 1, 2015.

Table 1. BU PSP Project Meeting Discussion Template. *When meeting with each BU the topics of the discussion are likely to cover a discussion of systems, data confidentiality, the PSP tailoring project, and the approach to writing policies.*

Addressing "BU-defined" and "BU-specified" Requirements

Within the PSP templates there are 34 occurrences of a placeholder in the requirement for the BU to define or specify an element of the requirement. These placeholders are there because the requirement does not lend itself to a strict definition or assignment that may fit all agencies. The flexibility of the placeholders allows each BU to tailor the policy to meet their specific need.

This is likely to be an area of PSP tailoring that either gets overlook (i.e., the BU simply leaves the requirements as-is resulting in an incomplete requirement) or is the source of confusion for some BUs. It would be useful to engage the BU in a discussion to point out these placeholders and let the BU know that they must be defined and specified. If the BU needs assistance in determining the value or statements for the placeholders the Table 2 provides some guidance. The following table provides an index to the requirements within the PSP templates where a Budget Unit (BU) will need to define or specify an element of the requirement to tailor it to the BU's needs.

Policy	Policy Title	Rqmnt #	Title	Requirement Text	BU-defined discussion
8120	Information Security Program	6.3.4.d	Security Risk Assessment	Disseminate risk assessment results to the BU CIO, BU ISO, state information system owner, and other BU-defined personnel or roles	Define the roles within the BU that should receive this report. Larger agencies may include an auditing function, a compliance officer, a librarian, or other roles that require a copy of this report. Smaller agencies may collapse the number of roles receiving this report to include the CIO and Executive Director only.

Tailoring PSP Templates Guide

Policy	Policy Title	Rqmnt #	Title	Requirement Text	BU-defined discussion
		6.3.5.e	Vulnerability Scanning	Share information obtained from the vulnerability scanning process and security control assessments with BU-defined personnel or roles to help eliminate similar vulnerabilities in other state information systems (i.e. systemic weaknesses or deficiencies.)	Define the roles within the BU that should receive this report. Larger agencies may include multiple roles within the IT departments and Security departments, or other roles that require a copy of this information. Smaller agencies may collapse the number of roles receiving this information to include the CIO and Executive Director only.
		6.3.5.i (P)	Vulnerability Scanning: provide privileged access	The state information system implements privileged access authorization to BU-defined components containing highly Confidential Data (e.g., databases);	Define components within the BU information system that contain highly confidential data. This will include databases for most BUs with confidential data but other components such as cloud storage, check processing systems, or vital records systems may be listed as well. These systems should be listed if privileged access vulnerability scanning is judged to be an essential control for these components risk-based decision.
		6.5.5.d	Continuous Monitoring	Ongoing security status monitoring of BU-defined metrics in accordance with the BU continuous monitoring strategy.	Define metrics to be collected and monitored to implement your BUs security program. BUs should look to ADOA security program as an example of useful security metrics.
8130	System security acquisition	6.2.a	Technology Life cycle	Manage the state information system using a BU-defined technology life cycle that incorporates information security considerations	Define your BUs technology life cycle. Include a listing and definition of its stages in your supporting documentation.
		6.4.b	State Information System Documentation	Ensure documentation is available to BU-defined personnel or roles	Define the roles within the BU that should receive this information. Larger agencies may include multiple roles within the IT departments and Security departments, or other roles that require a copy of this information. Smaller agencies may collapse the number of

Tailoring PSP Templates Guide

Policy	Policy Title	Rqmnt #	Title	Requirement Text	BU-defined discussion
					roles receiving this information to include the CIO and Executive Director only.
8220	System Security Maintenance	6.3.4.b	Information System Monitoring	Identify unauthorized use of the state information system through BU-defined intrusion-monitoring tools	List the intrusion monitoring tools your BU utilizes.
8250	Media Protection	6.7	Media Use	The BU shall restrict the use of [BU-specified type of digital media] on [BU-specified state information systems and/or system components].	List any media restricted by your BU. If this list changes according to certain components (e.g., no USB thumb drives in laptops) then specify which type of digital media is restricted for each component. Many BUs may not list any restrictions; in which case this requirement may simply state, "The BU does not restrict the use of any types of digital media on BU state information systems."
8280	Acceptable Use	6.6	User-Based Technology Agreements	The user-based technology access agreements shall be developed by the BU and contains BU-defined security controls. Standard 8220, System Security Maintenance provides guidance to BUs for minimum recommended user-based technology controls.	Define specific security controls for any user-based technology used within your BU (e.g., iPads, Smart phones). Many BUs may not allow any user-based technology. Others may not have any restrictions on it. At a minimum the BU should review the standard S8220 for minimum recommended controls.
8310	Account Management	6.3.4 (P)	Separation of Duties	The BU shall separate BU-defined duties; documents separation of duties of individuals; and defines state information system access authorizations to support separation of duties.	Separation of duties is a security control to be employed when a single person should not be involved from beginning to end on a single task or when looking to establish oversight and governance. BUs should establish their own SoD requirements. Some of the areas to look into these requirements include sensitive transactions such as accounts payable/accounts receivable,

Tailoring PSP Templates Guide

Policy	Policy Title	Rqmnt #	Title	Requirement Text	BU-defined discussion
					new code moving to production, security controls implementation and design and audit. Budget units that outsource account management and/or administration should consider enforcing a separation between privileged account holders and those who review audit logs of these commands.
		6.5.1 (P)	Automated Audit Actions	The BU shall ensure the state information system automatically audits account creation, modification, enabling, disabling, and removal actions and notifies, as required BU-defined personnel or roles.	Define the roles within the BU that should receive this report. Larger agencies may include an auditing function, a compliance officer, a librarian, or other roles that require a copy of this report. Smaller agencies may collapse the number of roles receiving this report to include the CIO and Executive Director only.
		6.7.2 (P)	Automatic Removal of Temporary Accounts	The state information system automatically removes or disables temporary and emergency accounts after a BU-defined time.	Define number of days that may pass before a temporary or emergency account should be disabled. Emergency accounts should be short-lived (e.g., 1-7 days) and temporary accounts may be longer term (e.g., 7-90 days).
		6.7.3 (P)	Disable Inactive Accounts	The BU shall ensure the state information system automatically disables inactive accounts after BU-defined time period. For state information systems containing cardholder data (CHD) the time period must be no less than 90 days.	Define number of days that may pass before an inactive account should be disabled. PCI requires that this be no more than 90 days.
8320	Access Control	6.3 (P)	Information Flow Enforcement	The BU shall ensure the state information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on BU-defined	Define the information flows allowed by your BUs firewalls. The design principle of the firewall ("Default Deny All") means that only BU required flows (e.g., external request to port 80) shall be allowed by the firewall.

Policy	Policy Title	Rqmnt #	Title	Requirement Text	BU-defined discussion
				information flow control policies, including Policy 8350, Systems and Communications Protections. These policies prohibit direct public access between the Internet and any system component in the Protected state information system.	
		6.9	Unsuccessful Logon Attempts	The BU shall ensure the state information system enforces a BU specified limit of consecutive invalid logon attempts by a user; and automatically locks the account/node for a BU specified period of time or locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded, consistent with the Access Control Standard 8320.	Define the period of time that an account shall be locked when too many password guesses have been attempted. Any amount of time over 15 minutes will address most threats to password guessing but BUs may want to set this period to several hours or 1 day.
		6.10	System Use Notification	Displays to users a BU-defined notification banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, state laws, Executive Orders, directives, policies, regulations, standards, and guidance and shall state the following	Define the BU notification banner to be used in the web facing applications and systems and the (potentially different) use notification for internal systems. Templates for such a notification may be available. Also the system use notification may have been established before and already in use. BUs should carefully review the banner to with information security and technology leads as well as the privacy and legal officers to ensure it is appropriate and accurate.
		6.11 (P)	Session Lock	The BU shall ensure the state information system prevents further	Define the period of inactivity that requires a session to be locked. Consider 5-15 minutes.

Policy	Policy Title	Rqmnt #	Title	Requirement Text	BU-defined discussion
				access to the system by initiating a BU specified limit of time inactivity or upon receiving a request from a user; and retains the session lock for a BU specified limit of time or until the user reestablishes access using established identification and authentication procedures. If the user does not reestablish access within a BU specified limit of time the session is dropped.	Define the period of time the session shall be locked. It is suggested that there is no period of time for the session lock and instead the session is locked until the user reestablishes access. Define the period of inactivity that requires a session to be dropped. Consider 30-60 minutes.
		6.13.4 (P)	Privileged Access Commands	The BU shall authorize the execution of privileged commands and access to security-relevant information using remote access only for BU-defined needs, and documents the rationale for such access in the security plan for the state information system.	In general privileged commands (e.g., changing firewall rules, establishing a user account) should be done onsite and not exposed to remote access. However, the BU may have a business need to have certain privileged commands executed over a remote session for business reasons despite the risk. In these cases the BU should document these privileged commands, the circumstances in which it would be allowed and a rationale for such access. This is to be documented in the system security plan.
		6.17 (P)	Information Sharing	The BU shall facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for BU-defined circumstances; and shall employ mechanisms or processes to assist users in making information sharing/collaboration	If the BU determines a business need for information sharing with a partner then the circumstances in which it shares information and any restrictions on that access (e.g., time of day, type of file, transmission methods, encryption requirements) shall be documented in this requirement.

Tailoring PSP Templates Guide

Policy	Policy Title	Rqmnt #	Title	Requirement Text	BU-defined discussion
				decisions.	
8330	System Security Audit	6.3	Audit Storage Capacity	The BU shall allocate audit record storage capacity in accordance with BU-defined audit record storage requirements.	Define the amount of storage space to be allocated for audit. This may be specified in many ways but it is best specified by number of days of audit records.
		6.4	Response to Audit Processing Failures	The BU shall ensure the state information system alerts BU-defined personnel or roles in the event of an audit processing failure; and shuts down the state information system, overwrites the oldest audit records, or stops generating audit records.	Define the roles within the BU that should receive this report. Larger agencies may include an multiple roles within IT that require this information. Smaller agencies may simply indicate a single IT role.
		6.5	Audit Review, Analysis, and Reporting	The BU shall review and analyze state information system audit records periodically for indications of inappropriate or unusual activity; and reports findings to BU-defined personnel or roles. State information systems with cardholder data (CHD) shall perform this review daily.	Define the roles within the BU that should receive this report. Larger agencies may include an auditing function, a compliance officer, a librarian, or other roles that require a copy of this report. Smaller agencies may collapse the number of roles receiving this report to include the CIO and Executive Director only.
		6.7	Time Stamps	The BU shall ensure the state information system uses internal system clocks to generate time stamps for audit records; and generates time in the time stamps that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) and provides a granularity of time to a BU-defined unit of time.	Define the granularity of time to be provided in time stamps for audit records. In general a granularity of 1 second would be adequate to support most investigations. If the BU has a need for a higher level of granularity then it should be noted here.
		6.7.1 (P)	Synchronization with Authoritative	The BU shall ensure the state information system synchronizes	Define frequency by which system clocks are synchronized. In general once

Tailoring PSP Templates Guide

Policy	Policy Title	Rqmnt #	Title	Requirement Text	BU-defined discussion
			Time Source	internal state information system clocks a BU-defined frequency with a BU-defined time source when the time difference is greater than a BU-defined time period.	an hour would suffice. Define time source in which to synchronize with. (NIST provides an internet time service but others may suffice as well). Define time period by which system clocks would be determined to be out of synch. In general a 1 second misalignment should be corrected.
		6.8.1 (P)	Access by Subset of Privileged Users	The BU shall authorize access and modification to management of audit functionality to only a BU-defined subset of privileged users.	Define role of privileged users who have the authority to modify system audit (e.g., monitoring, logging) functions, parameters, and files. It is a design principle to ensure that this include a subset of all privileged users to ensure oversight of this privileged function.
		6.9	Audit Record Retention	The BU shall retain audit records for a BU-defined time period with a BU-defined time period available for immediate analysis to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. For state information systems with cardholder data these defined times are at least one year with a minimum of three months immediately available for analysis.	Define amount of time audit records shall be retained. Include time frame for immediate analysis (i.e., stored online) and time frame for available. Unless there is a burden to storing these records, it is recommended that you follow the 3 months / 1 year guidance required for systems with cardholder data, even if you do not have such data.
		6.10.a		The BU shall ensure the state information system provides audit record generation capability for the auditable events, defined in Section 6.1 (Audit Records), at	List any system components, besides servers, firewalls, and workstations that may produce useful audit records. At a minimum include laptops.

Tailoring PSP Templates Guide

Policy	Policy Title	Rqmnt #	Title	Requirement Text	BU-defined discussion
				servers, firewalls, workstations, and other BU-defined system components.	
		6.10.c		Allows BU-defined personnel or roles to select which auditable events are to be audited by specific components of the state information system	Define role that has the system privilege to select which events are audited.
		6.3	Identifier Management	The BU shall manage the state information system identifiers by receiving authorization from BU-defined personnel or roles to assign individual, role, or device identifier.	Define role that authorizes the assignment of a system identifier (e.g., user id) to an individual. This may be the supervisor or human resources.
		6.4.g	Authenticator Management	The BU shall manage the state information system authenticators (e.g., passwords, tokens, certificate, and key cards) by Changing/refreshing authenticators [BU-defined time period by authenticator type (e.g., passwords, tokens, biometrics, PKI certificates, and key cards)];	Define the time period in which authenticators shall be refreshed. It is suggested that passwords be changed every 90 days and tokens (both hard and soft tokens) be refreshed every 1-2 years based on manufacturer recommendations (e.g., battery life, key management, software upgrades).
		6.4.3 (P)	In Person or Trusted Third-Party Registration	The BU shall require that the registration process to receive authenticators be conducted in person or by a trusted third-party before the registration authority with authorization by BU-defined personnel or roles.	Define role that authorizes the assignment of a system identifier (e.g., user id) to an individual. This may be the supervisor or human resources. [same as above 6.3]
		6.4.4	Hardware Token-based Authentication	The BU shall ensure the state information system, for hardware token-based authentication, employs mechanisms that satisfy BU-defined token	Define the Public Key Infrastructure (PKI) with which a token must comply (e.g., AZ State PKI, BU PKI).

Policy	Policy Title	Rqmnt #	Title	Requirement Text	BU-defined discussion
				quality requirements (e.g., compliant with a particular PKI).	
8350	System and Communication Protection	6.3.4 (P)	Transmission Confidentiality and Integrity	Cryptographic or Alternate Physical Protection - The BU shall ensure the state information system prevents unauthorized disclosure of information and, if required, detects changes to information during transmission unless otherwise protected by BU-defined alternative physical safeguards.	Either protect transmissions technically (i.e., encryption) or through alternative physical means. Examples of physical protections include pressurized conduit or protected distribution systems. If you choose technical means only delete the text beginning with "unless".
8410	System Privacy	6.16	Data Retention and Disposal	The BU shall retain each collection of PII for BU-defined time period to fulfill the purposes identified in the notice or as required by law, refer to Policy DRAFT, Document Retention	Define time period for retention of PII. This needs to be consistent with laws and the State librarian guidance. The Arizona State Library has an online application that covers retention schedules on a agency by agency basis: http://apps.azlibrary.gov/records/schedules.aspx

Table 2. BU-Defined and BU-specified Placeholders in the PSP Templates. *Each BU is instructed to replace these placeholders with a BU-defined or BU-specified value or statement.*

Frequently Asked Questions

Annual Risk Assessment [P8120, 6.3.4.b].

Q1: We are a small agency and risk assessments cost a lot of money. Can we do these every other year?

A1: You may request a policy exception on this requirement. Include either compensating controls (e.g., we run vulnerability scans every month) or provide a risk rationale (e.g., our system is a standard system in a static environment). While you are at it, you should consider your policy requirements for

- **vulnerability scanning** (6.3.5 required quarterly and when new vulnerabilities are identified for all systems standard and protected),
- **wireless AP testing** (6.5.1.d required quarterly for all systems standard and protected), and
- **penetration testing** (6.5.6 required annually for protected systems)

Tailoring PSP Templates Guide

Line Item for Security Budgets [P8130, 6.1.c].

Q2: Do we need to have a distinct line item for security in our budget? Budgets are set by the legislature and they come back as a lump sum.

A2: The requirement states that the line item for security must be in the "organizational programming and budgeting documentation". This is our own BUs documents not from the legislature that is required.

Q3: I'm a small agency, what am I going to spend on security?

A3: Common elements of a security budget include the cost of the following: Anti-malware subscriptions, anticipated expenditures on security components (e.g., firewalls, IDS, etc.), cost of risk assessment, penetration test, vulnerability scans, wireless scanning, anticipated incident handling, security awareness training, security technical training and conferences.

Marking Media [8250 Media Protection, 6.2].

Q4: The requirement states that we have to mark digital and non-digital media. Our BU sends out a lot of paper and it would be onerous for us to label it all. Do we really have to do that?

A4: If you truly believe it is in the best interest of the citizen and your agency to send out paper copies (or digital media) of sensitive information without labeling it you could request and exception but this seems a rather high risk. Consider some methods that may make it easier to comply such as stock paper with a labeled header and footer for high volume hard copy productions; binding materials together and labeling the front cover, obtaining digital media drives with labels printed on them.

Physical Protections [8260 Physical Protection]

Q5 [6.3.d]: Visitor Badges. The requirement states that we must give the visitor a badge or sticker for access to our facility. We are a small agency all working in a single room a badge seems overkill.

A5: This may be a good requirement for a risk-based exception. If you consider the risk of a visitor being onsite without a clear indication that they are a visitor then request an exception here. Your compensating controls are all areas of the office are viewable by multiple people, all employees are well-known to each other, and visitors are all escorted and supervised.

Q6 [6.5] Visitor Log. Do we really need a visitor log? We don't get many visitors. This seems to be a hassle.

Tailoring PSP Templates Guide

A6: The visitor log is a rather easy control to implement. It consists of a log book with columns for the name, agency, date and times. It is suggested that the visitor log also include a signature block for the visitor to indicate that they agree to the "on premise" acceptable use policy. Include a laminated copy of this policy as part of the book.

Q7 [6.9] Fire Suppression. The requirement is for fire suppression and detection devices for the system. Does this include our office space?

A7: The requirement is intended to cover anywhere a system component resides, including the office space. The requirement is only for any type of fire suppression and detection so sprinkler systems and smoke detectors count. If you are housed in a facility without any such protection (first ensure your building is compliant with code) request an exception on those facilities that have no such systems and list compensating controls such as handheld fire extinguishers.

Q8 [6.10] Temperature and Humidity Monitoring. Am I required to monitor the temperature of my office environment because it houses workstations?

A8: No. The requirement is for data centers, computer rooms, and server rooms.

Q9 [All] Requirement References. We do not need to comply with HIPAA or PCI so I removed those requirements. Is that OK?

A9: Not exactly. You may request an exception to any other requirements based on perceived risk or compensating controls. The references at the end of each requirement (shown in square brackets) refer to the source of the requirement. This is not intended as an applicability indicator. The indication at the beginning of the requirement (e.g., (P), (P-PHI)) is an denotes applicability, see section 3 of the policy templates.