

Sample Audit Checklist for CJIS Security Policy (CJISSECPOL) Area 17

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
5.17	Planning (PL)¹					
1.	Based on inquiry and record examination, has the Tribe or TGRA developed, documented, and disseminated to organizational personnel with planning responsibilities an agency-level planning policy that: <ul style="list-style-type: none"> • Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance? • Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines? 	___	___	___	PL-1, a.1.(c)	
		___	___	___	PL-1, a.1.(d)	
2.	Does the Tribe or TGRA have procedures to facilitate the implementation of the planning policy and the associated planning controls?	___	___	___	PL-1, a.2	
3.	Has the Tribe or TGRA designated organizational personnel with information security and privacy responsibilities to manage the development, documentation, and dissemination of the planning policy and procedures?	___	___	___	PL-1, b	
4.	Based on inquiry and record examination, has the Tribe or TGRA reviewed and updated the current planning: <ul style="list-style-type: none"> • Policy annually and following any security incidents involving unauthorized access to Criminal Justice Information (CJI) / Criminal History Record Information (CHRI) or systems used to process, store, or transmit CJI / CHRI? • Procedures annually and following any security incidents involving unauthorized access to CJI / CHRI or systems used to process, store, or transmit CJI / CHRI? 	___	___	___	PL-1, c.1	
		___	___	___	PL-1, c.2	

¹ These requirements are sanctionable for audit beginning October 1, 2024.

Sample Audit Checklist for CJIS Security Policy (CJISSECPOL) Area 17

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
5.	Based on inquiry and record examination, has the Tribe or TGRA developed security and privacy plans for the system that:					
	• Are consistent with the organization’s enterprise architecture?	_____	_____	_____	PL-2, a.1	
	• Explicitly define the constituent system components?	_____	_____	_____	PL-2, a.2	
	• Describe the operational context of the system in terms of mission and business processes?	_____	_____	_____	PL-2, a.3	
	• Identify the individuals that fulfill system roles and responsibilities?	_____	_____	_____	PL-2, a.4	
	• Identify the information types processed, stored, and transmitted by the system?	_____	_____	_____	PL-2, a.5	
	• Provide the security categorization of the system, including supporting rationale?	_____	_____	_____	PL-2, a.6	
	• Describe any specific threats to the system that are of concern to the organization?	_____	_____	_____	PL-2, a.7	
	• Provide the results of a privacy risk assessment for systems processing Personally Identifiable Information (PII)?	_____	_____	_____	PL-2, a.8	
	• Describe the operational environment for the system and any dependencies on or connections to other systems or system components?	_____	_____	_____	PL-2, a.9	
	• Provide an overview of the security and privacy requirements for the system?	_____	_____	_____	PL-2, a.10	
	• Identify any relevant control baselines or overlays, if applicable?	_____	_____	_____	PL-2, a.11	
	• Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions?	_____	_____	_____	PL-2, a.12	
	• Include risk determinations for security and privacy architecture and design decisions?	_____	_____	_____	PL-2, a.13	
	• Include security- and privacy-related activities affecting the system that require planning and coordination with organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities?	_____	_____	_____	PL-2, a.14	

Sample Audit Checklist for CJIS Security Policy (CJISSECPOL) Area 17

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
	<ul style="list-style-type: none"> Are reviewed and approved by the authorizing official or designated representative prior to plan implementation? 	___	___	___	PL-2, a.15	
6.	Based on inquiry and record examination, does the Tribe or TGRA distribute copies of the plans and communicate subsequent changes to the plans to organizational personnel with system security and privacy planning and plan implementation responsibilities; system developers; organizational personnel with information security and privacy responsibilities?	___	___	___	PL-2, b	
7.	Based on inquiry and record examination, does the Tribe or TGRA review the system security and privacy plans at least annually or when required due to system changes or modifications?	___	___	___	PL-2, c	
8.	Based on inquiry and record examination, does the Tribe or TGRA update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments?	___	___	___	PL-2, d	
9.	Based on inquiry and record examination, does the Tribe or TGRA protect the plans from unauthorized disclosure and modification?	___	___	___	PL-2, e	
10.	Based on inquiry and record examination, does the Tribe or TGRA establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy?	___	___	___	PL-4, a	
11.	Based on inquiry and record examination, does the Tribe or TGRA receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system?	___	___	___	PL-4, b	
12.	Based on inquiry and record examination, does the Tribe or TGRA review and update the rules of behavior at least annually?	___	___	___	PL-4, c	

Sample Audit Checklist for CJIS Security Policy (CJISSECPOL) Area 17

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
13.	Based on inquiry and record examination, does the Tribe or TGRA require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge annually, or when the rules are revised or updated?	___	___	___	PL-4, d	
14.	Based on inquiry and record examination, does the Tribe or TGRA include in the rules of behavior, restrictions on: <ul style="list-style-type: none"> • Use of social media, social networking sites, and external sites/applications? • Posting organizational information on public websites? • Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications? 	___	___	___	PL-4, (1) a	
		___	___	___	PL-4, (1) b	
		___	___	___	PL-4, (1) c	
15.	Based on inquiry and record examination, does the Tribe or TGRA develop security and privacy architectures for the system that: <ul style="list-style-type: none"> • Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information? • Describe the requirements and approach to be taken for processing PII to minimize privacy risk to individuals? • Describe how the architectures are integrated into and support the enterprise architecture? • Describe any assumptions about, and dependencies on, external systems and services? 	___	___	___	PL-8, a.1	
		___	___	___	PL-8, a.2	
		___	___	___	PL-8, a.3	
		___	___	___	PL-8, a.4	
16.	Based on inquiry and record examination, does the Tribe or TGRA review and update the architectures at least annually or when changes to the system or its environment occur to reflect changes in the enterprise architecture?	___	___	___	PL-8, b	
17.	Based on inquiry and record examination, does the Tribe or TGRA reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions?	___	___	___	PL-8, c	

Sample Audit Checklist for CJIS Security Policy (CJISSECPOL) Area 17

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
18.	Based on inquiry and record examination, does the Tribe or TGRA select a control baseline ² for the system?	___	___	___	PL-10	
19.	Based on inquiry and record examination, does the Tribe or TGRA tailor the selected control baseline by applying specified tailoring actions ³ ?	___	___	___	PL-11	

² Control baselines are predefined sets of controls specifically assembled to address the protection needs of a group, organization, or community of interest. Controls are chosen for baselines to either satisfy mandates imposed by laws, executive orders, directives, regulations, policies, standards, and guidelines or address threats common to all users of the baseline under the assumptions specific to the baseline. Baselines represent a starting point for the protection of individuals' privacy, information, and information systems with subsequent tailoring actions to manage risk in accordance with mission, business, or other constraints.

³ Tailoring a control baseline is accomplished by identifying and designating common controls, applying scoping considerations, selecting compensating controls, assigning values to control parameters, supplementing the control baseline with additional controls as needed, and providing information for control implementation.