Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	Access Control[1] (AC)[2]					
1.	Has the Tribe or TGRA developed, documented, and disseminated to organizational personnel with access control responsibilities an agency-level access control policy that:					
	- Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance?	____	____	____	AC-1, a.1.(a)	
	- Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines?	____	____	____	AC-1, a.1.(b)	
2.	Has the Tribe or TGRA developed, documented, and disseminated to organizational personnel with access control responsibilities procedures to facilitate the implementation of the access control policy and the associated access controls?	____	____	____	AC-1, a.2	
3.	Based on inquiry and record examination, has the Tribe or TGRA designated an individual with security responsibilities to manage the development, documentation, and dissemination of the access control policy and procedures?	____	____	____	AC-1, b	
4.	Based on inquiry and record examination, has the Tribe or TGRA reviewed and updated current access control:					
	- 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?	____	____	____	AC-1, c.1	
	- Procedures annually and following any security incidents involving unauthorized access to CJI / CHRI or systems used to process, store, or transmit CJI / CHRI?	____	____	____	AC-1, c.2	

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

[2] Refer to CJISSECPOL Section 5.20.6 for additional access control requirements related to mobile devices used to access Criminal Justice Information (CJI) / Criminal History Record Information (CHRI).

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
5.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Define and document the types of accounts allowed and specifically prohibited for use within the system?	____	____	____	AC-2, a	
	• Assign account managers?	____	____	____	AC-2, b	
	• Require conditions for group and role membership?	____	____	____	AC-2, c	
	• Specify:					
	o Authorized users of the system?	____	____	____	AC-2, d.1	
	o Group and role membership?	____	____	____	AC-2, d.2	
	o Access authorizations (i.e., privileges) and attributes listed for each account as follows:					
	▪ Email Address Text?	____	____	____	AC-2, d.3	
	▪ Employer Name?	____	____	____	AC-2, d.3	
	▪ Federation Id?	____	____	____	AC-2, d.3	
	▪ Given Name?	____	____	____	AC-2, d.3	
	▪ Identity Provider Id?	____	____	____	AC-2, d.3	
	▪ Sur Name?	____	____	____	AC-2, d.3	
	▪ Telephone Number?	____	____	____	AC-2, d.3	
	▪ Identity Provider Id?	____	____	____	AC-2, d.3	
	▪ Unique Subject Id?	____	____	____	AC-2, d.3	
	▪ Counter Terrorism Data Self Search Home Privilege Indicator?	____	____	____	AC-2, d.3	
	▪ Criminal History Data Self Search Home Privilege Indicator?	____	____	____	AC-2, d.3	
	▪ Criminal Intelligence Data Self Search Home Privilege Indicator?	____	____	____	AC-2, d.3	
	▪ Criminal Investigative Data Self Search Home Privilege Indicator?	____	____	____	AC-2, d.3	
	▪ Display Name?	____	____	____	AC-2, d.3	
	▪ Government Data Self Search Home Privilege Indicator?	____	____	____	AC-2, d.3	
	▪ Local Id?	____	____	____	AC-2, d.3	
	▪ NCIC Certification Indicator?	____	____	____	AC-2, d.3	
	▪ N-DEx Privilege Indicator?	____	____	____	AC-2, d.3	
	▪ PCII Certification Indicator?	____	____	____	AC-2, d.3	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	▪ 28 CFR Certification Indicator?	____	____	____	AC-2, d.3	
	▪ Employer ORI?	____	____	____	AC-2, d.3	
	▪ Employer Organization General Category Code?	____	____	____	AC-2, d.3	
	▪ Employer State Code?	____	____	____	AC-2, d.3	
	▪ Public Safety Officer Indicator?	____	____	____	AC-2, d.3	
	▪ Sworn Law Enforcement Officer Indicator?	____	____	____	AC-2, d.3	
	▪ Authenticator Assurance Level?	____	____	____	AC-2, d.3	
	▪ Federation Assurance Level?	____	____	____	AC-2, d.3	
	▪ Identity Assurance Level?	____	____	____	AC-2, d.3	
	▪ Intelligence Analyst Indicator?	____	____	____	AC-2, d.3	
	• Require approvals by organizational personnel with account management responsibilities for requests to create accounts?	____	____	____	AC-2, e	
	• Create, enable, modify, disable, and remove accounts in accordance with agency policy?	____	____	____	AC-2, f	
	• Monitor the use of accounts?	____	____	____	AC-2, g	
	• Notify account managers and system/network administrators within:					
	o One day when accounts are no longer required?	____	____	____	AC-2, h.1	
	o One day when users are terminated or transferred?	____	____	____	AC-2, h.2	
	o One day when system usage or need-to-know changes for an individual?	____	____	____	AC-2, h.3	
	• Authorize access to the system based on:					
	o A valid access authorization?	____	____	____	AC-2, i.1	
	o Intended system usage?	____	____	____	AC-2, i.2	
	o Attributes as listed in AC-2(d)(3)?	____	____	____	AC-2, i.3	
	• Review accounts for compliance with account management requirements at least annually?	____	____	____	AC-2, j	
	• Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group?	____	____	____	AC-2, k	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	• Align account management processes with personnel termination and transfer processes?	____	____	____	AC-2, l	
6.	Based on inquiry and record examination, does the Tribe or TGRA support the management of system accounts using automated mechanisms including email, phone, and text notifications to:					
	• Create, enable, modify, disable, and remove accounts?	____	____	____	AC-2, (1)	
	• Monitor system outage usage?	____	____	____	AC-2, (1)	
	• Report atypical system account usage?	____	____	____	AC-2, (1)	
	Notify account managers:					
	• When an account is created, enabled, modified, disabled or removed?	____	____	____	AC-2, (1)	
	• When users are terminated or transferred?	____	____	____	AC-2, (1)	
7.	Based on inquiry and record examination, does the Tribe or TGRA automatically remove temporary and emergency accounts within 72 hours?	____	____	____	AC-2, (2)	
8.	Based on inquiry and record examination, does the Tribe or TGRA disable accounts within one (1) week when the accounts:					
	• Have expired?	____	____	____	AC-2, (3)(a)	
	• Are no longer associated with a user or individual?	____	____	____	AC-2, (3)(b)	
	• Are in violation of organizational policy?	____	____	____	AC-2, (3)(c)	
	• Have been inactive for 90 calendar days?	____	____	____	AC-2, (3)(d)	
9.	Based on inquiry and record examination, does the Tribe or TGRA automatically audit account creation, modification, enabling, disabling, and removal actions?	____	____	____	AC-2, (4)	
10.	Based on inquiry and record examination, does the Tribe or TGRA require that users log out when a work period has been completed?	____	____	____	AC-2, (5)	
11.	Based on inquiry and record examination, does the Tribe or TGRA disable accounts of individuals within 30 minutes of discovery of direct threats to the confidentiality, integrity, or availability of CJI / CHRI?.	____	____	____	AC-2, (13)	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
12.	Based on inquiry and record examination, does the Tribe or TGRA enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies?	____	____	____	AC-3	
13.	Based on inquiry and record examination, does the Tribe or TGRA provide automated or manual processes to enable individuals to have access to elements of their personally identifiable information?	____	____	____	AC-3, (14)	
14.	Based on inquiry and record examination, does the Tribe or TGRA enforce approved authorizations for controlling the flow of information within the system and between connected systems by preventing CJI / CHRI from being transmitted unencrypted across the public network, blocking outside traffic that claims to be from within the agency, and not passing any web requests to the public network that are not from the agency-controlled or internal boundary protection devices (e.g., proxies, gateways, firewalls, or routers)?	____	____	____	AC-4	
15.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Identify and document separation of duties based on specific duties, operations, or information systems, as necessary, to mitigate risk to CJI / CHRI?	____	____	____	AC-5, a	
	• Define system access authorizations to support separation of duties?	____	____	____	AC-5, b	
16.	Based on inquiry and record examination, does the Tribe or TGRA employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks?	____	____	____	AC-6	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
17.	Based on inquiry and record examination, does the Tribe or TGRA authorize access for personnel including security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information security personnel, maintainers, system programmers, etc.) to:					
	• Established system accounts, configured access authorizations (i.e., permissions, privileges), set events to be audited, set intrusion detection parameters, and other security functions?	____	____	____	AC-6, (1)(a)	
	• Security-relevant information in hardware, software, and firmware?	____	____	____	AC-6, (1)(b)	
18.	Based on inquiry and record examination, does the Tribe or TGRA require that users of system accounts (or roles) with access to privileged security functions or security-relevant information (e.g., audit logs), use non-privileged accounts or roles, when accessing non-security functions?	____	____	____	AC-6, (2)	
19.	Based on inquiry and record examination, does the Tribe or TGRA restrict privileged accounts on the system to privileged users?	____	____	____	AC-6, (5)	
20.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Review annually the privileges assigned to non-privileged and privileged users to validate the need for such privileges?	____	____	____	AC-6, (7)a	
	• Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs?	____	____	____	AC-6, (7)b	
21.	Based on inquiry and record examination, does the Tribe or TGRA log the execution of privileged functions?	____	____	____	AC-6, (9)	
22.	Based on inquiry and record examination, does the Tribe or TGRA prevent non-privileged users from executing privileged functions?	____	____	____	AC-6, (10)	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
23.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Enforce a limit of five (5) consecutive invalid logon attempts by a user during a 15-minute time period?	____	____	____	AC-7, a	
	• Automatically lock the account or node until released by an administrator when the maximum number of unsuccessful attempts is exceeded?	____	____	____	AC-7, b	
24.	Based on inquiry and record examination, does the Tribe or TGRA display a system use notification message to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:					
	• Users are accessing a restricted information system?	____	____	____	AC-8, a.1	
	• System usage may be monitored, recorded, and subject to audit?	____	____	____	AC-8, a.2	
	• Unauthorized use of the system is prohibited and subject to criminal and civil penalties?	____	____	____	AC-8, a.3	
	• Use of the system indicates consent to monitoring and recording?	____	____	____	AC-8, a.4	
25.	Based on inquiry and record examination, does the Tribe or TGRA retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system?	____	____	____	AC-8, b	
26.	Based on inquiry and record examination, does the Tribe or TGRA for publicly accessible systems:					
	• Display system use information consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines, before granting further access to the publicly accessible system?	____	____	____	AC-8, c.1	
	• Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities?	____	____	____	AC-8, c.2	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
	• Include a description of the authorized uses of the system?	____	____	____	AC-8, c.3	
27.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Prevent further access to the system by initiating a device lock after a maximum of 30 minutes of inactivity and requiring the user to initiate a device lock before leaving the system unattended?	____	____	____	AC-11, a	
	• Retain the device lock until the user reestablishes access using established identification and authentication procedures?	____	____	____	AC-11, b	
28.	Based on inquiry and record examination, does the Tribe or TGRA conceal, via the device lock, information previously visible on the display with a publicly viewable image?	____	____	____	AC-11 (1)	
29.	Based on inquiry and record examination, does the Tribe or TGRA automatically terminate a user session after a user has been logged out?	____	____	____	AC-12	
30.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Identify any specific user actions that can be performed on the system without identification or authentication consistent with organizational mission and business functions?	____	____	____	AC-14, a	
	• Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication?	____	____	____	AC-14, b	
31.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed?	____	____	____	AC-17, a	
	• Authorize each type of remote access to the system prior to allowing such connections?	____	____	____	AC-17, b	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
32.	Based on inquiry and record examination, does the Tribe or TGRA employ automated mechanisms to monitor and control remote access methods?	____	____	____	AC-17, (1)	
33.	Based on inquiry and record examination, does the Tribe or TGRA implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions?	____	____	____	AC-17, (2)	
34.	Based on inquiry and record examination, does the Tribe or TGRA route remote accesses through authorized and managed network access control points?	____	____	____	AC-17, (3)	
35.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for compelling operational needs?	____	____	____	AC-17, (4)a	
	• Document the rationale for remote access in the security plan for the system?	____	____	____	AC-17, (4)b	
36.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access?	____	____	____	AC-18, a	
	• Authorize each type of wireless access to the system prior to allowing such connections?	____	____	____	AC-18, b	
37.	Based on inquiry and record examination, does the Tribe or TGRA protect wireless access to the system using authentication of authorized users and agency-controlled devices, and encryption?	____	____	____	AC-18, (1)	
38.	Based on inquiry and record examination, does the Tribe or TGRA disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment?	____	____	____	AC-18, (3)	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
39.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas?	____	____	____	AC-19, a	
	• Authorize the connection of mobile devices to organizational systems?	____	____	____	AC-19, b	
40.	Based on inquiry and record examination, does the Tribe or TGRA employ full-device encryption to protect the confidentiality and integrity of information on full- and limited-feature operating system mobile devices authorized to process, store, or transmit CJI / CHRI?	____	____	____	AC-19, (5)	
41.	Based on inquiry and record examination, does the Tribe or TGRA establish agency-level policies governing the use of external systems consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:					
	• Access the system from external systems?	____	____	____	AC-20, a.1	
	• Process, store, or transmit organization-controlled information using external systems?	____	____	____	AC-20, a.2	
42.	Based on inquiry and record examination, does the Tribe or TGRA prohibit the use of personally-owned information systems including mobile devices (i.e., bring your own device [BYOD]) and publicly accessible systems for accessing, processing, storing, or transmitting CJI / CHRI?	____	____	____	AC-20, b	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
43.	Based on inquiry and record examination, does the Tribe or TGRA permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:					
	• Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans?	____	____	____	AC-20, (1)a	
	• Retention of approved system connection or processing agreements with the organizational entity hosting the external system?	____	____	____	AC-20, (1)b	
44.	Based on inquiry and record examination, does the Tribe or TGRA restrict the use of organization-controlled portable storage devices by authorized individuals on external systems?	____	____	____	AC-20, (2)	
45.	Based on inquiry and record examination, does the Tribe or TGRA					
	• Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions as defined in an executed information exchange agreement?	____	____	____	AC-21, a	
	• Employ attribute-based access control (see AC-2(d)(3)) or manual processes as defined in information exchange agreements to assist users in making information sharing and collaboration decisions?	____	____	____	AC-21, b	

#	*QUESTION*	*YES*	*NO*	*N/A*	*STANDARD*	*COMMENT*
46.	Based on inquiry and record examination, does the Tribe or TGRA:					
	• Designate individuals authorized to make information publicly accessible?	____	____	____	AC-22, a	
	• Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information?	____	____	____	AC-22, b	
	• Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included?	____	____	____	AC-22, c	
	• Review the content on the publicly accessible system for nonpublic information quarterly and remove such information, if discovered?	____	____	____	AC-22, d	