

Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
Awareness and Training (AT)¹						
1.	Has the Tribe or TGRA developed an organizational-level awareness and training policy to ensure all personnel with physical or logical access ² to CJI ³ /CHRI ⁴ are aware of their specific individual responsibilities and expected behavior when they access it or systems that contain or process it?	_____	_____	_____	AT	
	Does the training policy convey the impact those individual positions have on the overall security of information systems?	_____	_____	_____	AT	
	For the questions above, simply restating controls does not constitute an organizational policy or procedure.					
2.	Does the Tribe or TGRA disseminate its organization-level awareness and training policy to all personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CHRI?	_____	_____	_____	AT-1, a.1	
	Does the Tribe or TGRA document its dissemination of the policy?	_____	_____	_____	AT-1, a.1	

¹ These requirements are sanctionable for audit beginning October 1, 2023.

² The physical or logical (electronic) ability, right or privilege to view, modify or make use of CJI.

³ Criminal Justice Information (CJI) is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

⁴ Criminal History Record Information (CHRI) is a subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
3.	Does the Tribe or TGRA's organization-level awareness and training policy address its purpose ⁵ , scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance?	_____	_____	_____	AT-1, a.1(a)	
	Is the policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines?	_____	_____	_____	AT-1, a.1(b)	
	Has the Tribe or TGRA developed procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls?	_____	_____	_____	AT-1, a.2	
4.	Based on inquiry and record examination, has the Tribe or TGRA designated organizational personnel with information security awareness and training responsibilities to manage the development, documentation, and dissemination of the awareness and training policy and procedures?	_____	_____	_____	AT-1, b	
5.	Based on inquiry and record examination, does the Tribe or TGRA review and update the current awareness and training policy annually and following changes in the information system operating environment, when security incidents occur or when changes to the CJIS Security Policy are made?	_____	_____	_____	AT-1, c.1	
6.	Based on inquiry and record examination, does the Tribe or TGRA review and update its procedures annually and following changes in information system operating environment, when security incidents occur or when changes in the CJIS Security Policy are made?	_____	_____	_____	AT-1, c.2	
7.	Based on inquiry and record examination, does the Tribe or TGRA provide security and privacy literacy training to system users (including managers, senior executives, and contractors) as part of initial training for new users prior to the users accessing CJI and annually thereafter?	_____	_____	_____	AT-2, a.1	

⁵ See Question 1.

Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
8.	Based on inquiry and record examination, does the Tribe or TGRA provide security and privacy literacy training to system users (including managers, senior executives, and contractors) when required by system changes or within 30 days of any security event for individuals involved in the event?	_____	_____	_____	AT-2, a.2	
9.	Based on record examination, does the Tribe or TGRA employ one or more of the following techniques to increase the security and privacy awareness of system users?					
	1. Displaying posters	_____	_____	_____	AT-2, b.1	
	2. Offering supplies inscribed with security and privacy reminders	_____	_____	_____	AT-2, b.2	
	3. Displaying logon screen messages	_____	_____	_____	AT-2, b.3	
	4. Generating email advisories or notices from organizational officials	_____	_____	_____	AT-2, b.4	
	5. Conducting awareness events	_____	_____	_____	AT-2, b.5	
10.	Does the Tribe or TGRA update literacy training and awareness content annually and following changes in the information system operating environment, when security incidents occur or when changes are made in the CJIS Security Policy?	_____	_____	_____	AT-2, c	
11	Does the Tribe or TGRA incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques?	_____	_____	_____	AT-2, d	
12.	Does the Tribe or TGRA provide literacy training on recognizing and reporting potential indicators of insider threats?	_____	_____	_____	AT-2, (2)	
13.	Does the Tribe or TGRA provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining?	_____	_____	_____	AT-2, (3)	

Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
14.	Based on record examination, does the Tribe or TGRA provide role-based security and privacy training to personnel with the following roles and responsibilities?					
	All individuals with unescorted access to a physically secure location.	_____	_____	_____	AT-3, a	
	General User: A user, but not a process, who is authorized to use an information system.	_____	_____	_____	AT-3, a	
	Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that general users are not authorized to perform.	_____	_____	_____	AT-3, a	
	Organizational Personnel with Security Responsibilities: Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJIS Security Policy.	_____	_____	_____	AT-3, a	
15.	Based on inquiry and record examination, does the Tribe or TRGA provide role-based security and privacy training to personnel before authorizing access to the system, information, or performing assigned duties, and annually thereafter?	_____	_____	_____	AT-3, a.1	
16.	Based on inquiry and record examination, does the Tribe or TRGA provide role-based security and privacy training to personnel when required by system changes?	_____	_____	_____	AT-3, a.2	
17.	Does the Tribe or TGRA update role-based training content annually and following audits; changes in the information system operating environment; security incidents; or when changes are made to the CJIS Security Policy?	_____	_____	_____	AT-3, b	
18.	Does the Tribe or TGRA incorporate lessons learned into role-based training from internal or external security incidents or breaches?	_____	_____	_____	AT-3, c	

Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)

#	<i>QUESTION</i>	<i>YES</i>	<i>NO</i>	<i>N/A</i>	<i>STANDARD</i>	<i>COMMENT</i>
19.	Based on record examination, does the Tribe or TGRA incorporate the minimum following topics into appropriate role-based training content for all individuals with unescorted access to a physically secure location?					
	a. Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information Penalties	_____	_____	_____	AT-3, d.1.a	
	b. Reporting Security Events	_____	_____	_____	AT-3, d.1.b	
	c. Incident Response Training	_____	_____	_____	AT-3, d.1.c	
	d. System Use Notification	_____	_____	_____	AT-3, d.1.d	
	e. Physical Access Authorizations	_____	_____	_____	AT-3, d.1.e	
	f. Physical Access Control	_____	_____	_____	AT-3, d.1.f	
	g. Monitoring Physical Access	_____	_____	_____	AT-3, d.1.g	
	h. Visitor Control	_____	_____	_____	AT-3, d.1.h	
	i. Personnel Sanctions	_____	_____	_____	AT-3, d.1.i	

Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
20.	Based on record examination, does the Tribe or TGRA include the following topics into appropriate role-based training content for a General User ⁶ , in addition to AT-3 d.1?					
	a. Criminal Justice Information	_____	_____	_____	AT-3, d.2.a	
	b. Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information	_____	_____	_____	AT-3, d.2.b	
	c. Personally Identifiable Information	_____	_____	_____	AT-3, d.2.c	
	d. Information Handling	_____	_____	_____	AT-3, d.2.d	
	e. Media Storage	_____	_____	_____	AT-3, d.2.e	
	f. Media Access	_____	_____	_____	AT-3, d.2.f	
	g. Audit Monitoring, Analysis, and Reporting	_____	_____	_____	AT-3, d.2.g	
	h. Access Enforcement	_____	_____	_____	AT-3, d.2.h	
	i. Least Privilege	_____	_____	_____	AT-3, d.2.i	
	j. System Access Control	_____	_____	_____	AT-3, d.2.j	
	k. Access Control Criteria	_____	_____	_____	AT-3, d.2.k	
	l. System Use Notification	_____	_____	_____	AT-3, d.2.l	
	m. Session Lock	_____	_____	_____	AT-3, d.2.m	
	n. Personally Owned Information Systems	_____	_____	_____	AT-3, d.2.n	
	o. Password	_____	_____	_____	AT-3, d.2.o	
	p. Access Control for Display Medium	_____	_____	_____	AT-3, d.2.p	
	q. Encryption	_____	_____	_____	AT-3, d.2.q	
	r. Malicious Code Protection	_____	_____	_____	AT-3, d.2.r	
	s. Spam and Spyware Protection	_____	_____	_____	AT-3, d.2.s	
	t. Cellular Devices	_____	_____	_____	AT-3, d.2.t	
	u. Mobile Device Management	_____	_____	_____	AT-3, d.2.u	
	v. Wireless Device Risk Mitigations	_____	_____	_____	AT-3, d.2.v	
	w. Wireless Device Malicious Code Protection	_____	_____	_____	AT-3, d.2.w	
	x. Literacy Training and Awareness/Social Engineering and Mining	_____	_____	_____	AT-3, d.2.x	
	y. Identification and Authentication (Organizational Users)	_____	_____	_____	AT-3, d.2.y	
	z. Media Protection	_____	_____	_____	AT-3, d.2.z	

⁶ A user, but not a process, who is authorized to use an information system.

Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
21.	Based on record examination, does the Tribe or TGRA include the following topics into appropriate role-based training content for a Privileged User ⁷ , in addition to AT-3 d.1 and 2?					
	a. Access Control	_____	_____	_____	AT-3, d.3.a	
	b. System and Communications Protection and Information Integrity	_____	_____	_____	AT-3, d.3.b	
	c. Patch Management	_____	_____	_____	AT-3, d.3.c	
	d. Data backup and storage—centralized or decentralized approach	_____	_____	_____	AT-3, d.3.d	
	e. Most recent changes to the CJIS Security Policy	_____	_____	_____	AT-3, d.3.e	
22.	Based on record examination, does the Tribe or TGRA include the following topics into appropriate role-based training content for Organizational Personnel with Security Responsibilities ⁸ , in addition to AT-3 d.1, 2 and 3?					
	a. Local Agency Security Officer Role	_____	_____	_____	AT-3, d.4.a	
	b. Authorized Recipient Security Officer Role	_____	_____	_____	AT-3, d.4.b	
	c. Additional state/local/tribal/territorial or federal agency roles and responsibilities	_____	_____	_____	AT-3, d.4.c	
	d. Summary of audit findings from previous NIGC audits of local agencies	_____	_____	_____	AT-3, d.4.d	
	e. Findings from the last FBI CJIS Division audit	_____	_____	_____	AT-3, d.4.e	
23.	Does the Tribe or TGRA provide all personnel with initial and annual training in the employment and operation of personally identifiable information processing and transparency controls when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJI?	_____	_____	_____	AT-3, (5)	

⁷ A user that is authorized (and, therefore, trusted) to perform security relevant functions that general users are not authorized to perform.

⁸ Personnel with the responsibility to ensure the confidentiality, integrity, and availability of CJI and the implementation of technology in a manner compliant with the CJISSECPOL.

Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
24.	Does the Tribe or TGRA document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training?	_____	_____	_____	AT-4, a	
25.	Does the Tribe or TGRA retain individual training records for a minimum of three years?	_____	_____	_____	AT-4, b	