

**Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)**

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

<sup>1</sup> These requirements are sanctionable for audit beginning October 1, 2024.

**Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)**

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
5.	Based on inquiry and record examination, has the Tribe or TGRA developed a contingency plan for the system that:					
	<ul style="list-style-type: none"> <li>Identifies essential mission and business functions and associated contingency requirements?</li> </ul>	___	___	___	CP-2, a.1	
	<ul style="list-style-type: none"> <li>Provides recovery objectives, restoration priorities, and metrics?</li> </ul>	___	___	___	CP-2, a.2	
	<ul style="list-style-type: none"> <li>Addresses contingency roles, responsibilities, assigned individuals with contact information?</li> </ul>	___	___	___	CP-2, a.3	
	<ul style="list-style-type: none"> <li>Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure?</li> </ul>	___	___	___	CP-2, a.4	
	<ul style="list-style-type: none"> <li>Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented?</li> </ul>	___	___	___	CP-2, a.5	
	<ul style="list-style-type: none"> <li>Addresses the sharing of contingency information?</li> </ul>	___	___	___	CP-2, a.6	
	<ul style="list-style-type: none"> <li>Is reviewed and approved by agency head or their designee?</li> </ul>	___	___	___	CP-2, a.7	
6.	Based on inquiry and record examination, does the Tribe or TGRA distribute copies of the contingency plan to organizational personnel with contingency planning or incident response duties?	___	___	___	CP-2, b	
7.	Based on inquiry and record examination, does the Tribe or TGRA coordinate contingency planning activities with incident handling activities?	___	___	___	CP-2, c	
8.	Based on inquiry and record examination, does the Tribe or TGRA review the contingency plan for the system annually?	___	___	___	CP-2, d	
9.	Based on inquiry and record examination, does the Tribe or TGRA update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing?	___	___	___	CP-2, e	

**Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)**

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
10.	Based on inquiry and record examination, does the Tribe or TGRA communicate contingency plan changes to organizational personnel with contingency planning or incident response duties?	___	___	___	CP-2, f	
11.	Based on inquiry and record examination, does the Tribe or TGRA incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training?	___	___	___	CP-2, g	
12.	Based on inquiry and record examination, does the Tribe or TGRA protect the contingency plan from unauthorized disclosure and modification?	___	___	___	CP-2, h	
13.	Based on inquiry and record examination, does the Tribe or TGRA coordinate contingency plan development with organizational elements responsible for related plans <sup>2</sup> ?	___	___	___	CP-2, (1)	
14.	Based on inquiry and record examination, does the Tribe or TGRA plan for the resumption of essential mission and business functions within twenty-four (24) hours of contingency plan activation?	___	___	___	CP-2, (3)	
15.	Based on inquiry and record examination, does the Tribe or TGRA identify critical system assets supporting essential mission and business functions?	___	___	___	CP-2, (8)	
16.	Based on inquiry and record examination, does the Tribe or TGRA provide contingency training to system users consistent with assigned roles and responsibilities: <ul style="list-style-type: none"> <li>• Within thirty (30) days of assuming a contingency role or responsibility?</li> <li>• When required by system changes?</li> <li>• Annually thereafter?</li> </ul>	___	___	___	CP-3, a.1	
		___	___	___	CP-3, a.2	
		___	___	___	CP-3, a.3	

<sup>2</sup> Plans that are related to contingency plans include Business Continuity Plans, Disaster Recovery Plans, Critical Infrastructure Plans, Continuity of Operations Plans, Crisis Communications Plans, Insider Threat Implementation Plans, Data Breach Response Plans, Cyber Incident Response Plans, Breach Response Plans, and Occupant Emergency Plans.

**Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)**

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
17.	Based on inquiry and record examination, does the Tribe or TGRA review and update contingency training content annually and following any security incidents involving unauthorized access to CJI / CHRI or systems used to process, store, or transmit CJI / CHRI, or training simulations or exercises?	___	___	___	CP-3, b	
18.	Based on inquiry and record examination, does the Tribe or TGRA: <ul style="list-style-type: none"> <li data-bbox="228 594 792 842">• Test the contingency plan for the system annually using the following tests to determine the effectiveness of the plan and the readiness to execute the plan: checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), or comprehensive exercises?</li> <li data-bbox="228 852 792 884">• Review the contingency plan test results?</li> <li data-bbox="228 894 792 919">• Initiate corrective actions, if needed?</li> </ul>	___	___	___	CP-4, a	
		___	___	___	CP-4, b	
		___	___	___	CP-4, c	
19.	Based on inquiry and record examination, does the Tribe or TGRA coordinate contingency plan testing with organizational elements responsible for related plans <sup>3</sup> ?	___	___	___	CP-4, (1)	
20.	Based on inquiry and record examination, has the Tribe or TGRA established an alternate storage site, including necessary agreements <sup>4</sup> to permit the storage and retrieval of system backup information?	___	___	___	CP-6, a	
21.	Based on inquiry and record examination, does the Tribe or TGRA ensure that the alternate storage site provides controls equivalent to that of the primary site?	___	___	___	CP-6, b	
22.	Based on inquiry and record examination, has the Tribe or TGRA identified an alternate storage site that is sufficiently separated from the primary storage site to reduce susceptibility to the same threats?	___	___	___	CP-6, (1)	

<sup>3</sup> Id.

<sup>4</sup> Items covered by alternate storage site agreements include environmental conditions at the alternate sites, access rules for systems and facilities, physical and environmental protection requirements, and coordination of delivery and retrieval of backup media.

*Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)*

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
23.	Based on inquiry and record examination, does the Tribe or TGRA identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions <sup>5</sup> ?	___	___	___	CP-6, (3)	
24.	Based on inquiry and record examination, has the Tribe or TGRA established an alternate processing site, including necessary agreements to permit the transfer and resumption of operations for essential mission and business functions within the time period defined in the system contingency plan(s) when the primary processing capabilities are unavailable?	___	___	___	CP-7, a	
25.	Based on inquiry and record examination, does the Tribe or TGRA make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption?	___	___	___	CP-7, b	
26.	Based on inquiry and record examination, does the Tribe or TGRA provide controls at the alternate processing site that are equivalent to those at the primary site?	___	___	___	CP-7, c	
27.	Based on inquiry and record examination, has the Tribe or TGRA identified an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats?	___	___	___	CP-7, (1)	
28.	Based on inquiry and record examination, does the Tribe or TGRA identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions?	___	___	___	CP-7, (2)	

<sup>5</sup> Explicit mitigation actions include duplicating backup information at other alternate storage sites if access problems occur at originally designated alternate sites or planning for physical access to retrieve backup information if electronic accessibility to the alternate site is disrupted.

*Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)*

#	QUESTION	YES	NO	N/A	STANDARD	COMMENT
29.	Based on inquiry and record examination, has the Tribe or TGRA developed alternate processing site agreements that contain priority-of-service provisions <sup>6</sup> in accordance with availability requirements (including recovery time objectives)?	_____	_____	_____	CP-7, (3)	
30.	Based on inquiry and record examination, has the Tribe or TGRA established alternate telecommunications services, including necessary agreements to permit the resumption of system operations for essential mission and business functions within the time period as defined in the system contingency plan(s) when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites?	_____	_____	_____	CP-8	
31.	Based on inquiry and record examination, has the Tribe or TGRA: <ul style="list-style-type: none"> <li>• Developed primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives)?</li> <li>• Requested Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier?</li> </ul>	_____	_____	_____	CP-8, (1) a	
		_____	_____	_____	CP-8, (1) b	
32.	Based on inquiry and record examination, has the Tribe or TGRA Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services?	_____	_____	_____	CP-8, (2)	

<sup>6</sup> Priority of service agreements refer to negotiated agreements with service providers that ensure that organizations receive priority treatment consistent with their availability requirements and the availability of information resources for logical alternate processing and/or at the physical alternate processing site.

**Sample Audit Checklist for CJIS Security Policy (CJISSECPOL)**

<b>#</b>	<b>QUESTION</b>	<b>YES</b>	<b>NO</b>	<b>N/A</b>	<b>STANDARD</b>	<b>COMMENT</b>
30.	Based on inquiry and record examination, does the Tribe or TGRA conduct backups of user-level information <sup>7</sup> contained in operational systems for essential business functions as required by the contingency plans?	___	___	___	CP-9, a	
31.	Based on inquiry and record examination, does the Tribe or TGRA conduct backups of system-level information <sup>8</sup> contained in the system as required by the contingency plans?	___	___	___	CP-9, b	
32.	Based on inquiry and record examination, does the Tribe or TGRA conduct backups of system documentation, including security- and privacy-related documentation as required by the contingency plans?	___	___	___	CP-9, c	
33.	Based on inquiry and record examination, does the Tribe or TGRA protect the confidentiality, integrity, and availability of backup information?	___	___	___	CP-9, d	
34.	Based on inquiry and record examination, does the Tribe or TGRA test backup information as required by the contingency plans to verify media reliability and information integrity?	___	___	___	CP-9, (1)	
35.	Based on inquiry and record examination, does the Tribe or TGRA implement cryptographic mechanisms to prevent unauthorized disclosure and modification of CJI / CHRI?	___	___	___	CP-9, (8)	
36.	Based on inquiry and record examination, does the Tribe or TGRA provide for the recovery and reconstitution of the system to a known state within the timeframe as required by the contingency plans after a disruption, compromise, or failure?	___	___	___	CP-10	
37.	Based on inquiry and record examination, does the Tribe or TGRA implement transaction recovery for systems that are transaction-based <sup>9</sup> ?	___	___	___	CP-10, (2)	

<sup>7</sup> User-level information includes information other than system-level information.

<sup>8</sup> System-level information includes system state information, operating system software, middleware, application software, and licenses.

<sup>9</sup> Transaction-based systems include database management systems and transaction processing systems. Mechanisms supporting transaction recovery include transaction rollback and transaction journaling.