YourIT!
Your Logo Goes Here

CJIS Security Policy

Policies and Procedures

Prepared for: Client Company

Prepared by: YourIT Company

Table of Contents

29	AC-2(3) - Account disabling for expired inactive or unauthorized users
30	AC-2(4) - Automated auditing of account management actions
31	AC-2(5) - User-initiated logout after work period completion
32	AC-2(13) - Timely disabling of high-risk user accounts
33	AC-3 - Enforce authorized logical access controls
34	AC-3(14) - Individual access to personal information
35	AC-4 - Information flow control and boundary protection
36	AC-5 - Separation of duties and access authorization
37	AC-6 - Least privilege access enforcement
38	AC-6(1) - Authorization of privileged user access to security functions
39	AC-6(2) - Use non-privileged accounts for non-security functions
40	AC-6(5) - Privileged Account Access Restriction
41	AC-6(7) - Annual user privilege review and adjustment
42	AC-6(9) - Privileged function execution logging
43	AC-6(10) - Restrict privileged function execution to authorized users
44	AC-7 - Limit and lockout after invalid logon attempts
45	AC-8 - System use notification and acknowledgment
46	AC-11 - Automatic and user-initiated device locking
47	AC-11(1) - Device lock display concealment
48	AC-12 - Automatic user session termination after logout
49	AC-14 - Identification and authentication exceptions documentation
50	AC-17 - Remote access authorization and usage restrictions
51	AC-17(1) - Automated monitoring and control of remote access
52	AC-17(2) - Cryptographic protection of remote access sessions
53	AC-17(3) - Remote access through authorized network points
54	AC-17(4) - Authorized privileged remote access with documentation
55	AC-18 - Wireless access configuration and authorization
56	AC-18(1) - Wireless access authentication and encryption
57	AC-18(3) - Disable unused embedded wireless networking
58	AC-19 - Mobile device configuration and connection authorization
59	AC-19(5) - Full-device encryption for mobile devices
60	AC-20 - External system use and BYOD policy

61	AC-20(1) - External system access control verification
62	AC-20(2) - Portable storage device use restrictions on external systems
63	AC-21 - Information sharing authorization verification and control
64	AC-22 - Public information posting authorization and review
65	AT-1 - Security awareness and training policy management
66	AT-2 - Security and privacy literacy training and awareness
67	AT-2(2) - Insider threat indicator literacy training
68	AT-2(3) - Social engineering and social mining training
69	AT-3 - Role-Based Security and Privacy Training
70	AT-3(5) - PII processing and transparency training
71	AT-4 - Security and privacy training documentation retention
72	AU-1 - Audit and accountability policy and procedures management
73	AU-2 - Event types specification and annual review for audit logging
74	AU-3 - Audit record content requirements
75	AU-3(1) - Detailed audit record content requirements
76	AU-3(3) - Limit PII in audit records to minimum necessary
77	AU-4 - Audit log storage capacity allocation
78	AU-5 - Audit logging failure alert and recovery
79	AU-6 - Audit record review analysis and reporting
80	AU-6(1) - Automated audit record review and reporting
81	AU-6(3) - Cross-repository audit record correlation
82	AU-7 - Audit record reduction and reporting capability
83	AU-7(1) - Audit record search and sorting capability
84	AU-8 - Audit record timestamp generation and precision
85	AU-9 - Audit information protection and alerting
86	AU-9(4) - Restricted audit log management access
87	AU-11 - Audit record retention and management
88	AU-12 - Configurable audit record generation and logging
89	CA-1 - Assessment Authorization and Monitoring Policy Management
90	CA-2 - Control assessment planning and execution
91	CA-2(1) - Independent control assessments by impartial assessors
92	CA-3 - Information exchange agreements and management

93	CA-5 - Plan of action and milestones management
94	CA-6 - System authorization and common control acceptance
95	CA-7 - System-level continuous security and privacy monitoring
96	CA-7(1) - Independent control assessment and monitoring
97	CA-7(4) - Integrated risk monitoring in continuous strategy
98	CA-9 - Internal system connection authorization and review
99	CM-1 - Configuration management policy and procedure maintenance
100	CM-2 - System baseline configuration and topology maintenance
101	CM-2(2) - Automated baseline configuration management
102	CM-2(3) - Baseline configuration version retention for rollback
103	CM-2(7) - Secure configuration and inspection of devices for high-risk travel
104	CM-3 - Configuration Change Control and Oversight
105	CM-3(2) - System change testing and documentation
106	CM-3(4) - Information security and privacy board membership
107	CM-4 - System change security and privacy impact analysis
108	CM-4(2) - Post-change security and privacy control verification
109	CM-5 - Access restrictions for system changes
110	CM-6 - Secure configuration settings management
111	CM-7 - System least functionality enforcement
112	CM-7(1) - System functions and services review and removal
113	CM-7(2) - Software execution control and restrictions
114	CM-7(5) - Authorized software program control and review
115	CM-8 - System component inventory and accountability
116	CM-8(1) - System component inventory updates
117	CM-8(3) - Automated detection and isolation of unauthorized components
118	CM-9 - Configuration management plan development and approval
119	CM-10 - Software license compliance and peer-to-peer control
120	CM-11 - User software installation policy enforcement and monitoring
121	CM-12 - CJI location and access documentation
122	CM-12(1) - Automated identification of CJI in systems
123	CP-1 - Contingency planning policy and procedure management

124	CP-2 - System contingency planning and management
125	CP-2(1) - Contingency plan coordination with related plans
126	CP-2(3) - Contingency plan for 24-hour function resumption
127	CP-2(8) - Identification of critical system assets
128	CP-3 - Contingency role-based training and updates
129	CP-4 - Annual contingency plan testing and review
130	CP-4(1) - Contingency plan testing coordination
131	CP-6 - Alternate storage site establishment and controls
132	CP-6(1) - Alternate storage site separation
133	CP-6(3) - Alternate storage site accessibility and mitigation planning
134	CP-7 - Alternate processing site establishment and controls
135	CP-7(1) - Alternate processing site separation
136	CP-7(2) - Alternate site accessibility risk assessment and mitigation
137	CP-7(3) - Alternate processing site priority-of-service agreements
138	CP-8 - Alternate telecommunications service agreements
139	CP-8(1) - Telecommunications Service Priority Agreements and Enrollment
140	CP-8(2) - Alternate telecommunications service redundancy
141	CP-9 - Backup and protection of system and user data
142	CP-9(1) - Backup media reliability and integrity testing
143	CP-9(8) - Cryptographic protection of backup data at rest
144	CP-10 - System recovery and reconstitution after disruption
145	CP-10(2) - Transaction recovery implementation
146	IA-0 - Use of FBI Authorized Originating Agency Identifier (ORI)
147	IA-1 - Identification and authentication policy and procedures management
148	IA-2 - Unique identification and authentication of organizational users
149	IA-2(1) - Multi-factor Authentication for Privileged Accounts
150	IA-2(2) - Multi-factor authentication for non-privileged accounts
151	IA-2(8) - Replay-Resistant Authentication Implementation
152	IA-2(12) - Accept and verify PIV-compliant credentials
153	IA-3 - Device identification and authentication before connection
154	IA-4 - System Identifier Assignment and Reuse Prevention

155	IA-4(4) - Individual Identifier Management by Status
156	IA-5 - Authenticator management and multi-factor authentication requirements
157	IA-5(1)(a) - Memorized Secret Management and Protection
158	IA-5(1)(b) - Look-up Secret Generation, Usage, and Protection
159	IA-5(1)(c) - Out-of-band authenticator secure channel and verification
160	IA-5(1)(d) - One-Time Password (OTP) Authenticator Security Requirements
161	IA-5(1)(e) - Cryptographic Authenticator Key Protection and Usage
162	IA-5(2) - Public key authentication and certificate validation
163	IA-5(6) - Authenticator protection by information security category
164	IA-6 - Obscure authentication feedback to prevent exposure
165	IA-7 - Cryptographic module operator authentication mechanisms
166	IA-8 - Non-organizational user identification and authentication
167	IA-8(1) - PIV Credential Acceptance and Verification
168	IA-8(2) - NIST-Compliant External Authenticator Acceptance and Documentation
169	IA-8(4) - Identity management using SAML or OpenID Connect
170	IA-11 - User re-authentication on role or credential changes
171	IA-12 - User identity proofing and verification
172	IA-12(2) - Identity evidence
173	IA-12(3) - Identity evidence validation and verification
174	IA-12(5) - Out-of-band address verification for identity proofing
175	IR-1 - Incident response policy and procedure management
176	IR-2 - Incident response training and content updates
177	IR-2(3) - Incident response breach identification training
178	IR-3 - Annual incident response capability testing
179	IR-3(2) - Incident response testing coordination with related plans
180	IR-4 - Comprehensive incident handling and response management
181	IR-4(1) - Automated incident handling support tools
182	IR-5 - Incident tracking and documentation
183	IR-6 - Incident reporting and notification procedures
184	IR-6(1) - Automated incident reporting mechanisms

185	IR-6(3) - Supply chain incident information sharing
186	IR-7 - Incident response support resource provision
187	IR-7(1) - Automated incident response information availability
188	IR-8 - Incident response plan development and management
189	IR-8(1) - Incident response plan for PII breach notification
190	MA-1 - Maintenance policy and procedure management
191	MA-2 - System maintenance control and documentation
192	MA-3 - System maintenance tools approval and review
193	MA-3(1) - Maintenance tool inspection for unauthorized modifications
194	MA-3(2) - Malicious code scanning of diagnostic media
195	MA-3(3) - Maintenance equipment removal authorization and sanitization
196	MA-4 - Nonlocal maintenance and diagnostic controls
197	MA-5 - Maintenance personnel authorization and supervision
198	MA-6 - Maintenance support and spare parts for critical components
199	MP-1 - Media protection policy and procedure management
200	MP-2 - Media access restriction to authorized users
201	MP-3 - System media security marking and exemptions
202	MP-4 - Media storage protection and encryption
203	MP-5 - System media transport protection and accountability
204	MP-6 - Media sanitization and secure disposal
205	MP-7 - Media use restrictions on criminal justice systems
206	PE-1 - Physical and environmental protection policy and procedures management
207	PE-2 - Facility access authorization and management
208	PE-3 - Physical access authorization and control management
209	PE-4 - Physical access control for system cabling
210	PE-5 - Physical access control for output devices
211	PE-6 - Physical access monitoring and log review
212	PE-6(1) - Physical intrusion alarms and surveillance monitoring
213	PE-8 - Visitor access record retention and review
214	PE-8(3) - Visitor access record PII minimization
215	PE-9 - Power equipment and cabling protection

216	PE-10 - Emergency power shutoff controls for data centers
217	PE-11 - Uninterruptible power supply for data centers
218	PE-12 - Emergency lighting for data center power outages
219	PE-13 - Fire detection and suppression with independent power
220	PE-13(1) - Automatic fire detection and notification system
221	PE-14 - Data center environmental control maintenance
222	PE-15 - Water damage protection with shutoff valves
223	PE-16 - System component entry and exit authorization
224	PE-17 - Alternate work site security and controls
225	PL-1 - Agency-level planning policy and procedures management
226	PL-2 - System Security and Privacy Plan Development and Maintenance
227	PL-4 - Rules of behavior establishment and acknowledgment
228	PL-4(1) - Social media and external site usage restrictions
229	PL-8 - System security and privacy architecture development and maintenance
230	PL-9 - Centralized Management of Security Controls
231	PL-10 - Control baseline selection for system security
232	PL-11 - Control baseline tailoring and customization
233	PS-1 - Personnel security policy and procedure management
234	PS-2 - Position risk designation and screening criteria
235	PS-3 - Personnel screening and rescreening for CJI access
236	PS-4 - Employee termination access revocation and exit procedures
237	PS-5 - Access authorization updates for personnel transfers
238	PS-6 - Access agreement development and enforcement
239	PS-7 - External provider personnel security management
240	PS-8 - Employee sanctions process and notification
241	PS-9 - Security and privacy roles in job descriptions
242	RA-1 - Risk assessment policy and procedure management
243	RA-2 - System and Information Security Categorization
244	RA-3 - System risk assessment and reporting
245	RA-5 - Vulnerability monitoring and remediation management
246	RA-5(2) - Vulnerability scan update within 24 hours

247	RA-5(5) - Privileged Access Authorization for Vulnerability Scanning
248	RA-5(11) - Public vulnerability reporting channel establishment
249	RA-7 - Risk response based on organizational tolerance
250	RA-9 - Criticality analysis of system components and functions
251	SA-1 - System and services acquisition policy and procedures management
252	SA-2 - Information security resource planning and allocation
253	SA-3 - System development lifecycle with security and privacy integration
254	SA-4 - Security and privacy requirements in acquisition contracts
255	SA-4(1) - Functional properties description for controls
256	SA-4(2) - Design and implementation documentation for controls
257	SA-4(9) - Identification of system functions ports protocols and services
258	SA-4(10) - Use FIPS 201-Approved PIV Products
259	SA-5 - System and User Security Documentation Management
260	SA-8 - Systems security and privacy engineering principles application
261	SA-8(33) - Personally Identifiable Information Minimization
262	SA-9 - External Service Provider Security and Compliance Management
263	SA-9(2) - External service functions and port disclosure
264	SA-10 - Developer configuration management and change control
265	SA-11 - Ongoing security testing and flaw remediation
266	SA-15 - Secure development process documentation and review
267	SA-15(1) - Developer criticality analysis at key lifecycle stages
268	SA-22 - Unsupported system component support and replacement
269	SC-1 - System and communications protection policy management
270	SC-2 - Separation of User and System Management Functions
271	SC-4 - Prevent unauthorized information transfer via shared resources
272	SC-5 - Denial-of-service protection and mitigation
273	SC-7 - Managed Interface Monitoring and Boundary Protection
274	SC-7(3) - Limit external network connections
275	SC-7(4) - Managed interface and control plane traffic protection
276	SC-7(5) - Network traffic deny-by-default policy
277	SC-7(7) - Prevent split tunneling for remote access

278	SC-7(8) - Authenticated proxy routing for internal traffic
279	SC-7(24) - Personally Identifiable Information Processing Controls
280	SC-8 - Confidentiality and integrity of transmitted CJI
281	SC-8(1) - Cryptographic protection of CJI in transit
282	SC-10 - Session network connection termination after inactivity
283	SC-12 - Cryptographic key management and control
284	SC-13 - Encryption of CJI in transit outside secure locations
285	SC-15 - Remote activation prohibition and use indication
286	SC-17 - Public key certificate issuance and trust management
287	SC-18 - Mobile code authorization and control
288	SC-20 - Authoritative name resolution with integrity verification
289	SC-21 - Name and address resolution data authentication and integrity verification
290	SC-22 - Fault-tolerant name and address resolution with role separation
291	SC-23 - Session communication authenticity protection
292	SC-28 - Cryptographic protection of CJI at rest outside secure locations
293	SC-28(1) - Encryption of CJI at rest outside secure locations
294	SC-39 - Separate execution domains for system processes
295	SI-1 - System and information integrity policy management
296	SI-2 - System flaw identification and timely remediation
297	SI-2(2) - Quarterly vulnerability scanning and patching
298	SI-3 - Malicious code protection and response mechanisms
299	SI-4 - Comprehensive system monitoring and intrusion detection
300	SI-4(2) - Automated near real-time event analysis
301	SI-4(4) - Inbound and outbound traffic monitoring for anomalies
302	SI-4(5) - System compromise alert notifications
303	SI-5 - Security alerts and directives management
304	SI-7 - Software and firmware integrity verification and response
305	SI-7(1) - Weekly integrity checks at security events
306	SI-7(7) - Detection of unauthorized configuration and privilege changes
307	SI-8 - Spam protection at system boundaries
308	SI-8(2) - Automated daily spam protection updates

309	SI-10 - Input validation for CJI processing systems
310	SI-11 - Secure error message generation and disclosure
311	SI-12 - Information management and retention compliance
312	SI-12(1) - Minimize Personally Identifiable Information Use
313	SI-12(2) - Minimize Use of PII in Research and Training
314	SI-12(3) - Information disposal after retention period
315	SI-16 - Memory protection with DEP and ASLR
316	SR-1 - Supply chain risk management policy and procedures
317	SR-2 - Supply chain risk management planning and protection
318	SR-2(1) - Supply chain risk management team establishment
319	SR-5 - Supply chain risk mitigation through preferred suppliers
320	SR-8 - Supply chain compromise notification agreements
321	SR-10 - System and component tamper inspection
322	SR-12 - Controlled disposal of CJI and media

Purpose

Establish uniform, enforceable security requirements to safeguard CJI throughout its lifecycle, ensuring consistent controls, oversight, and accountability in alignment with FBI CJIS policy and applicable laws.

Scope

Applies to all CJAs, NCJAs, contractors, and service providers that access, process, transmit, or store CJI covering personnel with unescorted logical or physical access and all systems, networks, and facilities (on-premises or cloud) where unencrypted CJI may reside or traverse.

Sanctions/Compliance

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy. Legal actions also may be taken for violations of applicable regulations and laws.

5.20 - Mobile device usage and wireless access control

CJIS Security Policy	Other Requirements
5.20 Mobile device usage and wireless access control	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

This policy area describes considerations and requirements for mobile devices including smartphones and tablets. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section augment those in other areas of the Policy to address the gaps introduced by using mobile devices. The agency shall: (i) establish usage restrictions and implementation guidance for mobile devices; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections without requiring network or peripheral cabling. Appendix G provides reference material and additional information on mobile devices.

Guidance
Agencies must define usage restrictions and implementation guidance for mobile devices and authorize, monitor, and control wireless access to systems handling CJI, in addition to baseline controls in other policy areas. Governance should clearly state which device types and wireless technologies are permitted, roles and responsibilities, criteria for authorization, and conditions for monitoring and revocation. Auditors should expect an approved policy, an inventory/authorization register for mobile/wireless access, and monitoring evidence (e.g., periodic reviews or alerts) demonstrating enforcement and oversight.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CJIS-CJISSECPOL 5.20 - Establish usage restrictions and wireless access control: Establish usage restrictions and control wireless access to systems containing Criminal Justice Information (CJI) or Criminal History Record Information (CHRI) by authorizing, monitoring, and managing mobile devices such as smartphones, tablets, and laptops. Wireless access points must be secured through measures including validation testing to detect unauthorized devices, physical security, controlled wireless coverage, strong authentication, encryption, and regular monitoring to prevent unauthorized access or data exposure. This control ensures that wireless technologies, which enable communication without physical cables, are properly restricted and managed to protect sensitive criminal justice data.

  Procedure

- Establish and enforce usage restrictions and authorization policies for all wireless access to systems containing CJI/CHRI.
- Maintain an inventory of all wireless access points (APs), perform regular validation testing to detect rogue APs, and physically secure APs against unauthorized access or manipulation.
- Enable logging on wireless devices and review logs monthly to monitor and control authorized wireless access, retaining evidence of compliance.

References
No References.

5.20.1 - Wireless technology minimum security requirements

CJIS Security Policy	Other Requirements
5.20.1 Wireless technology minimum security requirements	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Examples of wireless communication technologies include, but are not limited to: 802.11, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls.

Guidance
Wireless technologies (e.g., 802.11, cellular, Bluetooth, satellite, microwave, LMR) must meet at least the same security baseline applied to wired networks. Agencies should define risk-based wireless baselines per technology/implementation that add controls commensurate with the threat surface and mission use (e.g., stronger encryption/authentication, segmentation, signal/coverage management, logging). Auditors should look for approved policy and baselines mapping wired-to-wireless equivalence, documented risk assessments by technology, and evidence of monitoring that verifies continued adherence.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CJIS-CJISSECPOL 5.20.1 - Wireless technology minimum security requirements: Establish and enforce wireless security baselines that are at least equivalent to wired baselines for each approved technology, add risk based controls as needed per technology, and monitor for ongoing adherence.

  Procedure
  - Inventory all wireless technologies and map them to business use and risk
  - Define and publish per-technology baselines that meet or exceed wired controls (encryption/auth/segmentation/logging)
  - Validate implementation via configuration review and sample testing and retain evidence

References
No References.

5.20.1.1 - Secure management and configuration of 802.11 wireless access points

CJIS Security Policy	Other Requirements
5.20.1.1 Secure management and configuration of 802.11 wireless access points	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

802.11 Wireless Protocols
Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used. Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency's network that processes unencrypted CJI:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
5. Enable user authentication and encryption mechanisms for the management interface of the AP.
6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Identification and Authentication (IA).
7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.
8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.
10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
11. Ensure that the ad hoc mode has been disabled.
12. Disable all nonessential management protocols on the APs.
13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g., SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.
14. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum, logs shall be reviewed monthly.

15. Insulate, virtually (e.g., virtual local area network (VLAN) and ACLs) or physically (e.g., firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

Guidance
Wireless networks that touch systems processing unencrypted CJI must be managed and configured with FIPS 140-2 validated protections; legacy pre-802.11i protocols (e.g., WEP, WPA) are not permitted. The organization should demonstrate end-to-end governance and hardening of access points comprehensive inventory, controlled placement and coverage, secure administrative access using FIPS-compliant protocols, removal of defaults, and routine monitoring to prevent rogue or misconfigured devices. Auditors should expect evidence such as policies and configuration standards, inventories and baseline configs, range/rogue-AP testing results, segmentation diagrams limiting wireless-to-wired access to operational need, and periodic log/review records.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls
- CJIS-CJISSECPOL 5.20.1.1(1) - Validate absence of rogue access points: Validate through testing that no unauthorized wireless access points (rogue APs) exist within the organization's 802.11 wireless local area network (WLAN). This control ensures the organization fully understands and secures its wireless network posture by confirming only authorized APs provide wireless access, thereby protecting sensitive criminal justice information (CJI) from unauthorized interception or access. Rogue APs are unauthorized devices that can connect to the network without approval, posing security risks.

  Procedure
  - Conduct regular wireless network scans to detect and identify any unauthorized or rogue access points within the WLAN environment.
  - Maintain and review an up-to-date inventory of all authorized access points and compare scan results to this inventory to confirm no rogue devices exist.
  - Document and retain validation testing results as evidence of compliance and to support ongoing WLAN security posture assessments.

- CJIS-CJISSECPOL 5.20.1.1(2) - Maintain inventory of APs and 802.11 devices: Maintain an inventory of all wireless access points (APs) and 802.11 devices managed by the organization that have access to unencrypted Criminal Justice Information (CJI) or Criminal History Record Information (CHRI). Access points are devices that allow wireless devices to connect to a wired network, and 802.11 refers to the set of standards for wireless local area networking (Wi-Fi). This inventory helps the organization monitor and control wireless access to sensitive information by tracking all such devices in use.

  Procedure
  - Create and maintain a detailed inventory of all access points and 802.11 wireless devices including location, configuration, and security settings.
  - Regularly review and update the inventory to ensure accuracy and detect unauthorized devices.
  - Retain documented evidence of inventory updates and reviews to demonstrate compliance during audits.

- CJIS-CJISSECPOL 5.20.1.1(3) - Ensure physical security of APs: Ensure physical security of wireless access points (APs) to prevent unauthorized individuals from gaining physical access or

manipulating the devices. Access points are hardware devices that allow wireless devices to connect to a wired network, and protecting them physically helps maintain the integrity and security of the wireless network that handles sensitive Criminal Justice Information (CJI). This control focuses on safeguarding APs from tampering or unauthorized use that could compromise the confidentiality or availability of the network.

Procedure
- Secure all access points in locked rooms or enclosures accessible only to authorized personnel.
- Apply tamper-evident seals on access points and monitor physical access through surveillance or access logs.
- Maintain and review documented evidence of physical security measures and access records for all access points regularly.

- CJIS-CJISSECPOL 5.20.1.1(4) - Perform AP boundary testing: Perform AP boundary testing to determine the exact extent of wireless coverage provided by each access point (AP) in the organization's wireless network. This testing ensures that the wireless signal is confined strictly to the areas necessary for operational purposes, reducing the risk of unauthorized access beyond intended boundaries. Access points are devices that allow wireless devices to connect to a wired network, and controlling their coverage helps protect sensitive information such as Criminal Justice Information (CJI) and Criminal History Record Information (CHRI).

  Procedure
  - Conduct regular wireless access point boundary tests to measure and verify that signal coverage is limited to operational areas only.
  - Adjust access point settings such as transmit power and antenna orientation to restrict wireless coverage strictly within required physical boundaries.
  - Document and retain test results as evidence of compliance with wireless coverage limitations and review them periodically for ongoing validation.

- CJIS-CJISSECPOL 5.20.1.1(5) - Secure AP management interface: Enforce user authentication and encryption mechanisms for the management interface of all wireless access points (APs) that handle unencrypted Criminal Justice Information (CJI). This control requires that only authorized users can access the AP management functions through secure, FIPS-compliant protocols, ensuring that sensitive network configurations and data are protected from unauthorized access or interception.

  Procedure
  - Enable strong user authentication and encryption using FIPS-compliant protocols for all wireless access point management interfaces.
  - Disable all non-FIPS compliant management access methods and enforce robust administrative password policies per CJIS Identification and Authentication requirements.
  - Maintain and review logs of management access to wireless access points monthly to verify compliance and detect unauthorized access attempts.

- CJIS-CJISSECPOL 5.20.1.1(6) - Use strong admin passwords with lifecycle control: Enforce the use of strong administrative passwords on wireless access points (APs) that manage access to Criminal Justice Information (CJI). Ensure these passwords are changed regularly according to the organization's Identification and Authentication (IA) policy to prevent unauthorized access. Strong administrative passwords help protect the management interface of APs, which control wireless network security and access to sensitive information.

  Procedure

  - Enforce strong password complexity and length requirements for all administrative accounts on wireless access points. 2;Change administrative passwords regularly and immediately upon personnel changes in accordance with IA policy. 3;Maintain and review documented evidence of password changes and compliance with IA policy during audits.

- CJIS-CJISSECPOL 5.20.1.1(7) - Restrict and secure AP reset usage: Restrict access to the reset function on wireless access points (APs) to authorized personnel only, ensuring that resets are performed only when necessary. After any reset, restore the APs to the organization's hardened security settings rather than factory defaults to maintain protection of sensitive information. This control helps prevent unauthorized changes that could weaken the security of wireless networks handling Criminal Justice Information (CJI).

  Procedure
  - Restrict access point reset functionality to authorized personnel only and document each reset event.
  - Immediately restore hardened security settings on access points after any reset, avoiding factory default configurations.
  - Maintain and review logs of all access point resets regularly to verify compliance and detect unauthorized activity.

- CJIS-CJISSECPOL 5.20.1.1(8) - Harden SSID configuration: Enforce the hardening of wireless access point (AP) configurations by changing default Service Set Identifiers (SSIDs), disabling SSID broadcast so the network name is not publicly advertised, and ensuring SSID names do not contain any organization-identifying information such as division or location names. The SSID is the unique name that identifies a wireless network, and these measures reduce the risk of unauthorized access or identification of the organization's network infrastructure.

  Procedure
  - Change the default SSID on all wireless access points to a non-identifiable name that does not reveal agency information.
  - Disable SSID broadcast on all wireless access points to prevent the network name from being publicly visible.
  - Maintain and review configuration records demonstrating that SSIDs do not contain agency-identifying information and that SSID broadcast is disabled.

- CJIS-CJISSECPOL 5.20.1.1(9) - Enable all wireless product security features: Enable all security features on wireless access points (APs) managed by the organization, including cryptographic authentication, firewalls, and other privacy protections. This control ensures that wireless devices used to access Criminal Justice Information (CJI) or Criminal History Record Information (CHRI) have all available security mechanisms activated to protect sensitive data from unauthorized access or interception. Cryptographic authentication refers to verifying device identities using encryption, while firewalls control network traffic to prevent unauthorized connections.

  Procedure
  - Enable all available security features on wireless access points, including cryptographic authentication, firewall, and privacy protections.
  - Configure strong administrative passwords and secure management interfaces using FIPS-compliant protocols, and disable nonessential services on all wireless products.
  - Maintain and review configuration and security logs regularly to verify that all wireless security features remain enabled and effective.

- CJIS-CJISSECPOL 5.20.1.1(10) - Use ?128-bit encryption and unique keys: Enforce the use of encryption keys that are at least 128 bits in length to protect wireless communications involving Criminal Justice Information (CJI). Replace any default shared encryption keys with unique keys

to prevent unauthorized access, ensuring that each wireless access point uses distinct cryptographic keys. This control helps maintain the confidentiality and integrity of sensitive data transmitted over wireless networks.

Procedure
- Enforce the use of encryption keys with a minimum length of 128 bits for all wireless communications involving CJI/CHRI.
- Replace all default or shared encryption keys with unique keys for each wireless access point or device to prevent unauthorized access.
- Maintain and review documentation of encryption key generation and replacement activities to demonstrate compliance with CJIS encryption requirements.

- CJIS-CJISSECPOL 5.20.1.1(11) - Disable ad hoc mode: Disable ad hoc mode on all wireless access points to prevent devices from connecting directly to each other without using a central access point. Ad hoc mode allows devices to form spontaneous peer-to-peer networks, which can bypass organizational controls and increase the risk of unauthorized access to sensitive Criminal Justice Information (CJI). Disabling this mode helps ensure that all wireless communications are managed and secured through authorized infrastructure.

  Procedure
  - Disable ad hoc mode on all wireless access points to ensure devices connect only through authorized infrastructure. 2;Configure wireless access points to operate exclusively in infrastructure mode and verify settings through periodic audits. 3;Document and retain configuration records demonstrating ad hoc mode is disabled on all access points for compliance verification.

- CJIS-CJISSECPOL 5.20.1.1(12) - Disable nonessential management protocols: Disable all nonessential management protocols on wireless access points (APs) to reduce security risks. Management protocols are the communication methods used to configure and control APs, and disabling those not required for operations helps prevent unauthorized access or manipulation. This control ensures that only necessary management functions remain active, protecting the integrity of systems that handle Criminal Justice Information (CJI).

  Procedure
  - Disable all nonessential management protocols on wireless access points to minimize security vulnerabilities. 2;Configure access points to allow only FIPS-compliant secure protocols for management access and authentication. 3;Document and review access point configurations regularly to verify that only required management protocols are enabled.

- CJIS-CJISSECPOL 5.20.1.1(13) - Use FIPS-compliant secure management protocols: Enforce the use of Federal Information Processing Standards (FIPS) compliant secure management protocols for all management access and authentication to wireless access points. This control requires that management interfaces use approved cryptographic protocols such as HTTPS, SFTP, or SNMP over TLS to protect sensitive information and prevent unauthorized access. FIPS compliance ensures that the cryptographic methods meet federal security standards for safeguarding Criminal Justice Information (CJI).

  Procedure
  - Configure all management interfaces to use only FIPS-compliant secure protocols such as HTTPS, SFTP, or SNMP over TLS for authentication and access.
  - Disable all non-FIPS-compliant management protocols on wireless access points and related devices to prevent insecure access.

    - Maintain and review logs of management access sessions regularly to verify compliance with FIPS protocol usage and secure authentication practices.

- CJIS-CJISSECPOL 5.20.1.1(14) - Enable and review AP logs: Enable logging on all wireless access points (APs) managed by the organization to record security-relevant events. Review these logs regularly, at least monthly according to local policy, to detect and respond to unauthorized access or other security incidents. This control helps ensure the organization monitors wireless network activity to protect sensitive Criminal Justice Information (CJI) and Criminal History Record Information (CHRI).

  Procedure
    - Enable logging on all wireless access points to capture security events and activities. 2;Review access point logs at least monthly according to local policy to identify potential security incidents. 3;Maintain records of log reviews as evidence of compliance and for audit purposes.

- CJIS-CJISSECPOL 5.20.1.1(15) - Isolate wireless from wired infrastructure: Isolate the wireless network from the wired operational infrastructure by using virtual or physical separation methods such as virtual local area networks (VLANs) or firewalls. Limit access between wireless and wired networks strictly to what is necessary for operational purposes to reduce the risk of unauthorized access to sensitive Criminal Justice Information (CJI). This control ensures that wireless access points do not provide unrestricted connectivity to the wired network, thereby protecting the organization's information systems.

  Procedure
    - Segment wireless networks from wired infrastructure using VLANs or firewalls to restrict access strictly to operational needs. 2;Limit and monitor interconnections between wireless and wired networks to prevent unauthorized lateral movement. 3;Maintain and review documentation evidencing network segmentation and access controls to demonstrate compliance.

- CJIS-CJISSECPOL 5.20.1.1(16) - Sanitize APs before disposal: Sanitize access points (APs) before disposal by clearing all configuration settings to prevent the disclosure of sensitive information such as network configurations, encryption keys, and passwords. This control ensures that when wireless access points are decommissioned, no residual data remains that could be exploited to gain unauthorized access to the organization's systems or data.

  Procedure
    - Establish and enforce procedures to clear all configuration settings, including passwords and encryption keys, from APs before disposal. 2;Authorize trained personnel to perform the sanitization process and ensure factory reset or secure wiping methods are applied. 3;Document each AP's sanitization with date, personnel involved, and method used as evidence of compliance.

References
No References.

5.20.1.2 - Cellular handheld device security controls

CJIS Security Policy	Other Requirements
5.20.1.2 Cellular handheld device security controls	N/A

Policy
The organization will implement internal controls to satisfy the following requirement:

Control:
Cellular telephones, smartphones (i.e., Blackberry, iPhones, etc.), tablets, personal digital assistants (PDA), and aircards are examples of cellular handheld devices or devices that are capable of employing cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks. Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

1. Loss, theft, or disposal.
2. Unauthorized access.
3. Malware.
4. Spam.
5. Electronic eavesdropping.
6. Electronic tracking (threat to security of data and safety of the criminal justice professional).
7. Cloning (not as prevalent with later generation cellular technologies).
8. Server-resident data.

Guidance
Organizations must establish and enforce governance for cellular handheld devices that access or can access CJI, including smartphones, tablets, aircards, and devices with auxiliary radios (e.g., Bluetooth/IR). Controls should be risk-based and demonstrably address the major threat categories for these devices loss/theft and disposal, unauthorized access, malware/spam, eavesdropping, tracking, cloning, and exposure of server-resident data throughout the device lifecycle. Auditors should expect clear policy and baseline requirements, authorization/asset records for covered devices, and evidence of ongoing monitoring and review to keep protections effective as technologies and threats evolve.

Responsibilities
The Security Officer is responsible for ensuring the implementation of this policy.

Related Internal Controls

- CJIS-CJISSECPOL 5.20.1.2 - Inspect managed devices for international use: Inspect managed mobile devices before and after they are deployed internationally to verify that all security controls required by the organization’s policies are properly implemented and functioning. This inspection ensures that devices accessing Criminal Justice Information (CJI) or Criminal History Record Information (CHRI) maintain protections such as encryption and authentication, except for voice

transmissions on cellular devices which are exempt. The control addresses risks from potential modifications by foreign cellular providers and mandates documented verification to maintain the integrity and security of sensitive information during overseas use.

Procedure

- Inspect all managed devices before and after international deployment to verify that security controls, including voice encryption and authentication exemptions, are correctly applied per policy. 2;Document inspection results and maintain records to demonstrate compliance with organizational policies and CJIS requirements.

References

No References.

Truncated Sample Document