**CJIS Compliance Guide for PSAPs**

Achieving and maintaining compliance with the Criminal Justice Information Services (CJIS) Security Policy is critical for your organization's security and operational integrity.

This guide will help you clearly understand essential compliance areas, provide practical, actionable steps, and serve as an ongoing reference for your compliance journey.

**1. Understanding CJIS Security Policy**

CJIS Security Policy protects Criminal Justice Information (CJI), ensuring confidentiality, integrity, and availability. Compliance is mandatory for PSAPs handling sensitive data.

**Key Compliance Areas:**

- Security Protocols
- Employee Training
- Network Security
- Access Controls
- Incident Response
- Regular Auditing

---

**2. Security Protocols**

Clear procedures ensure data is managed securely.

**Actionable Steps:**

- Implement mandatory encryption for all CJI data (at rest, transit, and use).
- Maintain exclusive agency control of encryption keys.
- Establish and enforce secure data retention and disposal processes.

**Example:**

Encryption ensures sensitive call data and criminal records accessed by dispatchers are protected from unauthorized viewing.

---

### 3. Employee Training

Staff must understand their responsibilities clearly.

**Actionable Steps:**

- Provide CJIS-specific security training annually.
- Use role-based training tailored specifically for dispatchers.
- Conduct regular scenario-based cybersecurity exercises.

**Diagram:**

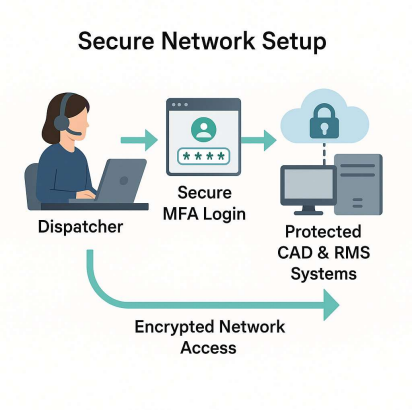

---

### 4. Network Security

Robust network protection is critical to safeguard sensitive data.

**Actionable Steps:**

- Deploy continuous network monitoring solutions.
- Implement vulnerability scans and patch regularly.
- Establish secure, encrypted remote access methods.




---

**5. Access Controls**

Strict access ensures only authorized personnel interact with sensitive information.

**Actionable Steps:**

- Require multi-factor authentication (MFA) for all system access.
- Assign permissions using "least privilege" principles.
- Clearly separate duties to prevent conflicts and unauthorized access.

**Example:**

Dispatchers have access limited to necessary systems, reducing potential security risks from misuse.

---

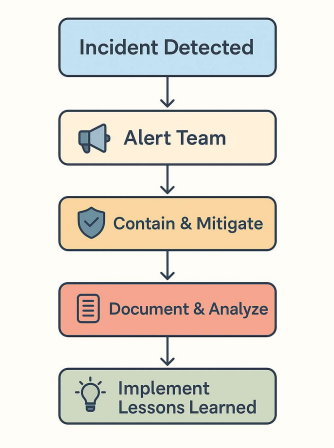
**6. Incident Response**

Prompt and effective response minimizes damage from cyber incidents.

**Actionable Steps:**

- Develop a detailed, PSAP-specific incident response plan.
- Regularly test the plan through realistic exercises.
- Train staff to recognize, report, and respond swiftly to incidents.

Incident Response Flow:




---

**7. Regular Auditing**

Ongoing audits ensure continual compliance.

**Actionable Steps:**

- Schedule regular internal audits of security protocols.
- Utilize third-party auditors annually to verify compliance.
- Address audit findings promptly with corrective action.

**Example:**

An annual audit identifies and helps correct gaps in dispatcher access protocols, ensuring continued compliance.

---

**Conclusion & Ongoing Reference**

Compliance with the CJIS Security Policy is ongoing. Use this guide as a foundational reference and continuously refine your processes, maintaining clear documentation and actively engaging your staff in compliance initiatives. Through vigilance and dedication, your PSAP will consistently uphold the highest standards of data security, safeguarding your community's trust.

---

**Brian Nelson**

Brian Nelson is a cybersecurity strategist with over 15 years of experience in critical infrastructure protection, specializing in telecommunications and public safety networks. As a senior consultant and advisor, Brian works closely with government agencies and industry partners to design and deploy advanced security solutions that mitigate emerging cyber threats, including those posed by quantum computing. His expertise encompasses network security architecture, incident response, and compliance with federal cybersecurity standards for emergency services.

---

**Kenyon Langford**

Kenyon Langford is the Principal of 911 Nurd, a specialized IT consulting firm focused on public safety technology solutions. With extensive expertise in 911 response systems, law enforcement communications, and emergency management infrastructure, Kenyon advises agencies on cybersecurity, network modernization, and strategic technology implementation. He has led multiple initiatives to help public safety organizations transition to next-generation communication networks and implement robust security frameworks, including post-quantum cryptography and Zero Trust architectures.