AGENCY REQUIRED POLICY CHECKLIST

NON-STORAGE OF CJI

☐ **Relationship to Local Security Policy and Other Policies - CSP Section 1.3**

"The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy, and, where applicable, the local security policy."

- Does the agency have a policy that states the agency must comply with the CSP?
- Does the agency have documented procedures to facilitate the implementation of the CSP?

☐ **Personally Identifiable Information (PII) - CSP Section 4.3**

"Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from criminal justice information (CJI)."

- Does the agency have a Personally Identifiable Information policy?
- Does the policy describe appropriate security controls for handling PII extracted from CJI?
    - Physical protection
    - Logical protection
    - Dissemination

☐ **Information Exchange - CSP Section 5.1.1**

"In these instances, the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate the requestor of CJI as an authorized recipient before disseminating CJI."

- Does the agency have a policy stating how agency members will validate the requestor of CJI is an authorized recipient before disseminating CJI?

☐ **Information Handling - CSP Section 5.1.1.1**

"Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration, or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange."

- What are the agency's procedures for handling, processing, storing, and communication of CJI?
- Do the procedures provide criteria for how personnel are to protect information from unauthorized disclosure, alteration, or misuse?

☐ Incident Response - CSP Section 5.3

"Agencies shall (i) establish an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities."

- Does the agency have a policy that describes how the agency prepares/has prepared for a security incident?
- Does the policy describe actions the user should take in the event of a security incident?
- Does the policy describe how agency personnel track, document and report the incident to the appropriate agency officials and the FDLE Information Security Officer?
- The policy should include physical incident response.

☐ Personally Owned Information Systems - CSP Sections 5.5.6.1

"A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices."

- Does your policy prohibit the use of personally owned information system from accessing, processing, storing, and/or transmitting CJI?

☐ Media Protection - CSP Section 5.8

"Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media."

- Does your policy describe procedures to ensure access to electronic and physical media is restricted to authorized individuals?
- Does your policy include procedures to ensure secure:
    - Handling media?
    - Transporting media?
    - Storing media?

☐ Electronic Media Sanitization and Disposal - CSP Section 5.8.3

"The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel." ***<u>This policy is only needed if the agency utilizes electronic device for storage such as an external hard drive.</u>***

- Does your policy describe the steps your agency takes to sanitize or destroy electronic media?
- Does your policy state the sanitization or destruction will be witnessed or carried out by authorized personnel?

☐ Disposal of Physical Media - CSP Section 5.8.4

"Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel."

- Does your policy describe the procedures to securely dispose of physical media?
- Does your policy state the disposal or destruction of physical media will be witnessed or carried out by authorized personnel?

☐ Physical Protection - CSP Section 5.9

"Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures."

- Does your policy describe how CJI is protected through access control measures?
    - Include access control measures for information system hardware, software, and media (electronic and physical)?

☐ Personnel Sanctions - CSP Section 5.12.4

"The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures."

- Does your policy describe the sanction process for personnel that fail to comply with established agency policies and procedures?