Diocese of Pensacola-Tallahassee Policy and Procedures for CJIS Compliance

Table of Contents:

Relationship Policy

The overriding goal of this policy is to comply with the CJIS Security Policy requirements. Due to the evolving nature of the CJIS Security Policy, it is necessary to separately communicate the requirements of the CJIS Security Policy as they are developed and enhanced. These additional requirements are intended to be an enhancement to the existing Standard Operating Procedures of the Diocese of Pensacola-Tallahassee. The Diocese of Pensacola-Tallahassee shall adhere, at a minimum, to the CJIS Security Policy. While the Diocese of Pensacola-Tallahassee may augment or increase the standards, it cannot detract from the minimum requirements set forth by the FBI CJIS Security Policy.

PERSONALLY IDENTIFIABLE INFORMATION (PII)

PII Personally Identifiable Information (PII) –is any information pertaining to an individual that can be used to distinguish or trace a person's identity. PII is defined as any one or more of types of information including, but not limited to:

1. Social security number
2. Username and password
3. Passport number
4. Credit card number
5. Clearances
6. Banking information
7. Biometrics
8. Data and place of birth
9. Mothers maiden name
10. Criminal, medical and financial records
11. Educational transcripts
12. Photos and video including any of the above

All physical files that contain PII will reside within a locked file cabinet or room when not being actively viewed or modified. PII is not to be downloaded to mobile devices (such as laptops, personal digital assistants, mobile phones, tablets or removable media) or to systems outside the protection of the agency. PII will also not be sent through any form of insecure electronic communication as significant security risks emerge when PII is transferred from a secure location to a less secure location or is disposed of improperly. When disposing of PII the physical file should be shredded by a crisscross shredder. All disposal of PII will be done by authorized personnel of the Diocese of Pensacola-Tallahassee. CJI may not be transmitted through Diocesan email or scanned into any media device.

All PII will be collected only when there is a legal authority and it is necessary to conduct diocesan duties.

Access to PII is only handled when the information is needed to conduct diocesan official duties and should only be utilized for official purposes. Authorized diocesan personnel will destroy the documents when no longer needed.

INFORMATION EXCHANGE

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. It is used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.

2. Identity History Data—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.

4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).

5. Case/Incident History—information about the history of criminal incidents.

Before disseminating criminal justice information (CJI) the Diocese of Pensacola-Tallahassee will contact FDLE Criminal History Services at (850) 410-8161 for written authorization to release the information to the requesting agency**.** The Diocese of Pensacola-Tallahassee will verify the receiver of the information by having a list of current authorized individuals/agencies allowed access to certain information and validate that the receiver is on the list. The Diocese of Pensacola-Tallahassee will put forth formal agreements with other agencies, when information is exchanged on a regular basis, prior to exchanging criminal justice information as well as use of secondary dissemination.

All CJI released to other agencies shall be documented in the dissemination log including: date, subject's name, SID or FBI number, requestor, requestor agency, reason disseminated, and purpose code.

CJI will only be transmitted to authorized individuals/agencies by hand delivery, certified mail, or secure fax machine to secure fax machine.

INFORMATION HANDLING

Information obtained from the CJI systems, must only be used for criminal justice purposes. Personnel must follow all CJIS Security Policy, state and federal rules and regulations regarding CJI information. All personnel with access to CJI shall receive the proper training within 30 days of hire. All information outlined in the information exchange and disposal of physical media shall be followed as well.

Physical information, such as reports that contain criminal justice information is stored in the records room that is only accessible to authorized personnel. The documents are stored in a locked filing cabinet, in locked room with limited access by trained and authorized personnel.

INCIDENT RESPONSE FOR PHYSICAL FORMS OF CJI

If an incident occurs involving any CJI, the LASO shall be contacted immediately. If it is deemed by the LASO to be a security breach of confidential information, a Security Incident Response Form will be filled out and submitted to FDLE ISO at fdlecjisiso@flcjn.net.

All users are responsible for reporting known or suspected information security incidents. All incidents must be reported immediately to the agency LASO in the Human Resource Department of the Diocese of Pensacola-Tallahassee.

When a CJIS security incident is reported to the agency's LASO, the LASO will document evidence of such breach and attempt to recover missing CJIS to the extent possible. The LASO will determine where and how the breach occurred and identify the source of compromise and the time frame involved. LASO will collect necessary information to complete a Security Incident Reporting Form, and contact FDLE ISO. LASO will also consult with the Bishop and Chancellor of the Diocese of Pensacola-Tallahassee to determine necessary measures to prevent such incident and protect CJIS information.

PERSONALLY OWNED INFORMATION SYSTEMS

Personally owned devices include cell phones, tablets or any other device that is owned and maintained by the user, not the Diocese of Pensacola-Tallahassee.

Personally owned devices are not allowed to access the Diocese of Pensacola-Tallahassee's network. Therefore, a device that is not owned by the Diocese of Pensacola-Tallahassee**,** shall not process, store, access or transmit CJI.

MEDIA PROTECTION

Media in any form will not be used to transmit, store or maintain CJI by the Diocese of Pensacola-Tallahassee. It is the policy of the Diocese of Pensacola-Tallahassee to only transmit, store and maintain hard copies of CJI.

DISPOSAL OF PHYSICAL MEDIA

N/A

CJI will not be stored in any form of media.

PHYSICAL PROTECTION

Only authorized personnel have access to areas where criminal justice information is located. All areas are equipped with locked doors, locked file cabinets and only authorized personnel with appropriate training shall have unescorted access to the physically secure locations.

Any transportation of CJI will be done so securely as stated in the information exchange section of this policy. Only authorized personnel with required training can transport CJI.

PERSONNEL SANCTIONS

Any user who violates any portion of this policy will be subject to the standard disciplinary processes in place with the Diocese of Pensacola-Tallahassee. Sanctions against staff that violate information systems and or security policies may include formal disciplinary action up to and including termination based on offense severity.