Wakulla County School Board

Criminal Justice Information Services

CJIS Handbook

WAKULLA COUNTY SCHOOL BOARD

Policy and Procedures Compliance Handbook for CJIS

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 Wakulla County School Board (WCSB). WCSB shall adhere, at a minimum, to the CJIS Security Policy. While WCSB 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 anyone 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 workstations or 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. All disposal of PII will be done by authorized Agency personnel.

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

Access to PII is only conducted when the information is needed to conduct Agency official duties and should only be utilized for official purposes. Agency members will not create duplicate copies of documents that contain PII and will destroy the documents when no longer needed. Agency does not extract PII from CJI.

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) WCSB will contact FDLE Criminal History Services at (850) 410-8161 for written authorization to release the information to the requesting agency**.**

WCSB currently does not share CJI with any other agency.

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. CJI or PII will not be transmitted via email. 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 Human Resource Personnel Vault located at the Wakulla School Board District Office. The vault is locked at all times and only authorized personnel are allowed to enter. When documents are removed, the information is kept by an authorized individual and then returned.

.

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.

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 Agency Head and appropriate Agency personnel 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 agency.

WCSB allows personally owned devices. The following terms and conditions apply for all personally owned devices that are used to access, process, store or transmit CJI:

1. All access via Wi-Fi must be 802.11, WPA2 and meet the requirements for FIPS 140-2 encryption. WCSB implements all of the appropriate security controls for WCSB managed wireless access points with access to the network that processes unencrypted CJI.

2. The **ManageEngine Mobile Device Management** is employed on all personally owned devices that access or transmit CJI. Devices that have any unauthorized changes made to them shall not be used to process, store, or transmit CJI. The following controls are applied via **name of device**:

    a. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.
    b. **MDM solution name** will be configured and implemented to perform at least:
        i. Remote locking of device
        ii. Remote wiping of device
        iii. Setting and locking device configuration
        iv. Detection of "rooted" and "jailbroken" devices
        v. Enforcement of folder or disk level encryption
        vi. Application of mandatory policy settings on the device
        vii. Detection of unauthorized configurations
        viii. Detection of unauthorized software or applications
        ix. Ability to determine the location of agency controlled devices
        x. Prevention of unpatched devices from accessing CJI or CJI systems
        xi. Automatic device wiping after a specified number of failed access attempts

3. For wireless devices that access CJI the following will be applied:

a. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing.
b. Configuration for local device authentication.
c. Use advanced authentication or CSO approved compensating controls.
d. Encrypt hard drives on the device.
e. Erase cached information, to include authenticators in applications, when session is terminated.
f. Employ personal firewalls or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
g. Employ malicious code protection or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.

4. Employ the following on all mobile devices (i.e. laptops)
    a. Patches and updates
    b. Malicious code protection
    c. Personal Firewall that performs the following activities:
        i. Manage program access to the internet.
        ii. Block unsolicited requests to connect to the user device.
        iii. Filter incoming traffic by IP address or protocol.
        iv. Filter incoming traffic by destination ports.
        v. Maintain an IP traffic log.
    d. Implement local device authentication used to unlock the device for use.
    e. Employ two factor advanced authentication

MEDIA PROTECTION

Media in all forms shall be protected at all times.

Physical media is restricted to authorized individuals. Only those users of WCSB who have appropriate security awareness training will be allowed to handle criminal justice information in any form.

Handling physical media- WCSB will ensure that only authorized individuals will be granted access to media containing criminal justice information. The media will be stored within the physically secure building and kept behind locked doors and locked cabinets. Hard copies will be shredded by authorized personnel by using a cross cut shredder.

Any media that is transported outside the physically secure location will be kept in list how it will be transported (i.e. sealed envelope, lock brief case, etc.).

DISPOSAL OF PHYSICAL MEDIA

The disposal of criminal justice information must be done in an effective manner in order to protect the secure information. The purpose of this policy is to lay out the proper disposal and destruction of physical media within the Wakulla County School District.

When no longer needed, all physical media will be disposed of by shredding.

All forms of destruction of physical media will be witnessed or carried out by authorized agency personnel.

PHYSICAL PROTECTION

The purpose of this policy is to provide guidance for all agency personnel physical protection of criminal justice information.

Only authorized personnel have access to the room where criminal justice information is located. The room is equipped with locked doors and a locked file cabinet and only Agency members with appropriate training shall have unescorted access to the physically secure location of Wakulla County School District.

All physical media containing CJI will be locked in filing cabinet in a locked office. Only authorized personnel will have a key to the cabinet.

Any transportation of CJI will be done so securely. Only authorized personnel can transport CJI. It will physically be with the personnel.

PERSONNEL SANCTIONS

Any user who violates any portion of this policy will be subject to the standard disciplinary processes in place with Wakulla County School District. 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.