SUWANNEE COUNTY SCHOOL BOARD
SPECIAL MEETING
October 11, 2022

AGENDA

Call to Order – Immediately following the Workshop

The Superintendent recommends approval to adopt the agenda.

1. The Superintendent recommends approval of the RIVEROAK Technical College Procedures for Criminal Justice Information Services (CJIS), as required by the Florida Department of Law Enforcement (FDLE) and Federal Bureau of Investigation (FBI). **(pgs. 2-13)**

2. Discussion and possible action on appointment of a Board member to the District Calendar Committee.

3. Discussion and possible action on the purchase of the Branford Woman's Club property owned by the Town of Branford, Parcel Identification #16-06S-14E-03954-000000.

Adjourn

RIVEROAK Technical College

Procedures for CJIS Compliance

Table of Contents:

Relationship Policy 2

Personally Identifiable Information (PII) 2

Information Exchange 2

Information Handling 2

Incident Response 2

Personally Owned Information Systems 3

Media Protection 4

Disposal of Physical Media 4

Physical Protection 5

Personnel Sanctions 6

Authorized Personnel 6

Relationship Policy

The overriding goal of this procedure 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 **RIVEROAK Technical College. RIVEROAK Technical College** shall adhere, at a minimum, to the CJIS Security Policy. While **RIVEROAK Technical College** 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 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. **RIVEROAK Technical College** 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) **RIVEROAK Technical College** will contact FDLE Criminal History Services at (850) 410-8161 for written authorization to release the information to the requesting agency. **RIVEROAK Technical College** 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 in the Student Records Room that is only accessible to identified personnel (List of those with access is at entry-way to Student Records Room). The documents are stored in a locked filing cabinet in locked Records Room and are only removed when needed for operational purposes. When removed, the information is kept by an authorized individual and then returned. The removal is documented in a log.

Files are not transported to another Suwannee County School District facility for storage.

INCIDENT RESPONSE FOR PHYSICAL FORMS OF CJI

If an incident occurs involving any CJI, the LASO (College Administrator) 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 RIVEROAK Technical College'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 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.

RIVEROAK Technical College allows personally owned devices to access email and student information management system (FOCUS). No personally owned device will access, process, store, or transmit CJI.

MEDIA PROTECTION

Media in all forms (electronic and physical) shall be protected at all times. Media is restricted to authorized individuals. Only those users of the Agency who have appropriate security awareness training will be allowed to handle criminal justice information in any form.

Physical media (i.e. physical documents) shall only be stored for **postsecondary program year**. The Agency 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 location** and kept behind locked doors. When no longer needed, the electronic media will be disposed of by authorized agency personnel. Hard copies will be shredded by authorized personnel using a cross cut shredder.

Any media that is transported outside the physically secure location at no time be released to an unauthorized person or left without proper documentation. Any physical media that is transported outside the physically secure location will be kept in a sealed envelope with evidence tape to ensure that the chain of custody is kept. All electronic media transported will be encrypted using an application that is FIPS 140-2 certified and employ at least 128 bit encryption. When the media is released to another user, the user will document the transaction in a secondary dissemination log for validation purposes. RIVEROAK Technical College does not transport CJI, with the exception of the LASO printing one copy of the background screening and delivering to File Clerk in RIVEROAK Technical College Student Services Department.

Media Sanitization

a. Sanitize or destroy digital and non-digital media prior to disposal, release out of agency control, or release for reuse using overwrite technology at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media will be destroyed (cut up, shredded, etc.). Physical media will be securely disposed of when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration; and b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

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 **RIVEROAK Technical College**.

Currently, **RIVEROAK Technical College** does not dispose of any CJI.

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

PHYSICAL PROTECTION

The purpose of these guidelines is to provide guidance for all agency personnel, support personnel and private contractors and vendors for the physical, logical and electronic protection of criminal justice information.

Only authorized personnel have access to the Student Records Room where CJI is stored. The building is equipped with badge swipe access for Agency personnel.

Visitors must sign in at the front desk and produce identification. Visitors will wear a visitors badge after going through RAPTOR process and are not allow access without escort within building.

All computer screens are turned away from public view, but CJI information is not stored on computers. It is only accessed at Suwannee County School District's site.

All physical media containing CJI will be locked in the Student Records Room. Only authorized personnel will have a key to the Student Records Room. If confidential information is removed from Student Records Room by authorized personnel, a log will be maintained noting date, time of removal and date, time of return with authorized personnel's signature.

THE LASO (Administrator) is the only authorized individual who may print CJI. CJI is printed at the School District's Personnel office by the LASO and once printed, hand delivered by the LASO to the Filing Clerk to be placed in locked file cabinet in secure Student Records Room for filing. If Filing Clerk is unavailable, the LASO will place a sealed envelope with CJI in designated filing cabinet located in Student Records Room for filing.

All Agency computers are equipped with boundary protection tools and spam and spy ware to avoid any intrusion attacks.

PERSONNEL SANCTIONS

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

AUTHORIZED PERSONNEL

The following personnel are authorized to access the Student Records Room:

- LASO, College Administrator
- Student Services Coordinator
- Clerk
- Financial Aid Specialist
- Testing Administrator
- Registrar/Data Operator

RIVEROAK Technical College

~~Policy and~~ Procedures for CJIS Compliance

Table of Contents:

Relationship Policy 2

Personally Identifiable Information (PII) 2

Information Exchange 2

Information Handling 2

Incident Response 2

Personally Owned Information Systems 3

Media Protection 4

Disposal of Physical Media 4

Physical Protection 5

Personnel Sanctions 6

Authorized Personnel 6

Relationship Policy

The overriding goal of this procedure ~~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 **RIVEROAK Technical College. RIVEROAK Technical College** shall adhere, at a minimum, to the CJIS Security Policy. While **RIVEROAK Technical College** 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 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. **RIVEROAK Technical College** 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) **RIVEROAK Technical College** will contact FDLE Criminal History Services at (850) 410-8161 for written authorization to release the information to the requesting agency. **RIVEROAK Technical College** 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 in the Student Records Room that is only accessible to identified personnel (List of those with access is at entry-way to Student Records Room). The documents are stored in a locked filing cabinet in locked Records Room and are only removed when needed for operational purposes. When removed, the information is kept by an authorized individual and then returned. The removal is documented in a log.

Files are not transported to another Suwannee County School District facility for storage.

INCIDENT RESPONSE FOR PHYSICAL FORMS OF CJI

If an incident occurs involving any CJI, the LASO (College Administrator) 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 RIVEROAK Technical College'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 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.

RIVEROAK Technical College allows personally owned devices to access email and student information management system (FOCUS). No personally owned device will access, process, store, or transmit CJI.

MEDIA PROTECTION

Media in all forms (electronic and physical) shall be protected at all times. Media is restricted to authorized individuals. Only those users of the Agency who have appropriate security awareness training will be allowed to handle criminal justice information in any form.

Physical media (i.e. physical documents) shall only be stored for **postsecondary program year**. The Agency 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 location** and kept behind locked doors. When no longer needed, the electronic media will be disposed of by authorized agency personnel. Hard copies will be shredded by authorized personnel using a cross cut shredder.

Any media that is transported outside the physically secure location at no time be released to an unauthorized person or left without proper documentation. Any physical media that is transported outside the physically secure location will be kept in a sealed envelope with evidence tape to ensure that the chain of custody is kept. All electronic media transported will be encrypted using an application that is FIPS 140-2 certified and employ at least 128 bit encryption. When the media is released to another user, the user will document the transaction in a secondary dissemination log for validation purposes. RIVEROAK Technical College does not transport CJI, with the exception of the LASO printing one copy of the background screening and delivering to File Clerk in RIVEROAK Technical College Student Services Department.

Media Sanitization

a. Sanitize or destroy digital and non-digital media prior to disposal, release out of agency control, or release for reuse using overwrite technology at least three times or degauss digital media prior to disposal or releose for reuse by unauthorized individuals. Inoperable digital media will be destroyed (cut up, shredded, etc.). Physical media will be securely disposed of when no longer needed for investigative or security purposes, whichever is later. Physical media will be destroyed by crosscut shredding or incineration; and b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

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 **RIVEROAK Technical College.**

Currently, **RIVEROAK Technical College** does not dispose of any CJI.

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

PHYSICAL PROTECTION

The purpose of these guidelines~~this policy~~ is to provide guidance for all agency personnel, support personnel and private contractors and vendors for the physical, logical and electronic protection of criminal justice information.

Only authorized personnel have access to the Student Records Room where CJI is stored. The building is equipped with badge swipe access for Agency personnel.

Visitors must sign in at the front desk and produce identification. Visitors will wear a visitors badge after going through RAPTOR process and are not allow access without escort within building.

All computer screens are turned away from public view, but CJI information is not stored on computers. It is only accessed at Suwannee County School District's site.

All physical media containing CJI will be locked in the Student Records Room. Only authorized personnel will have a key to the Student Records Room. If confidential information is removed from Student Records Room by authorized personnel, a log will be maintained noting date, time of removal and date, time of return with authorized personnel's signature.

THE LASO (Administrator) is the only authorized individual who may print CJI. CJI is printed at the School District's Personnel office by the LASO and once printed, hand delivered by the LASO to the Filing Clerk to be placed in locked file cabinet in secure Student Records Room for filing. If Filing Clerk is unavailable, the LASO will place a sealed envelope with CJI in designated filing cabinet located in Student Records Room for filing.

All Agency computers are equipped with boundary protection tools and spam and spy ware to avoid any intrusion attacks.

PERSONNEL SANCTIONS

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

AUTHORIZED PERSONNEL

The following personnel are authorized to access the Student Records Room:

- LASO, College Administrator
- Student Services Coordinator
- Clerk
- Financial Aid Specialist
- Testing Administrator
- Registrar/Data Operator