Title: Criminal Justice Information Handling and Storage (Employee Handling of Employee Records)	Number: A6Hx2-3.55A
Policy Number: 6Hx2-3.55	Page: 1 of 6

Personally Identifiable Information (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. Mother's maiden name
10. Criminal, medical and financial records
11. Educational transcripts
12. Photos and video including any of the above

All electronic files that contain PII will reside within the College's physically secure locations. 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 College. 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 or electronic file should be shredded or securely deleted. All disposal of PII will be done by authorized College employees.

All PII will be collected only when there is a legal authority and it is necessary to conduct college duties. Access to PII is only conducted when the information is needed to conduct College official duties and should only be utilized for official purposes.

College employees will not create duplicate copies of documents that contain PII and will destroy the documents when no longer needed. When PII is extracted from a document, College employees may only target the PII that is required for the task. PII that is extracted shall not be retained beyond the records retention rules for the data and the system it was accessed from. PII shall not be stored or transmitted via personally owned devices. PII may not be taken home by any College employee.

Information Handling

The College utilizes a standalone secured workstation which is dedicated to FDLE CJIS. The doors have key card locks that are only accessible to college employees. The workstation is encrypted with FIPS 140-2 certified encryption in order to secure the criminal justice data stored on them. Physical information, such as reports that

contain criminal justice information is stored in the secured file room that is only accessible to specific Human Resources employees. The documents are stored in a locked filing cabinet 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. Any information that must leave the facility for transport will be done so only by authorized employees and only for operational purposes.

Information Exchange

Criminal Justice Information is the term used to refer to all of the FBI CJI 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 CJI 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.

The College does allow for criminal justice information to be shared with current authorized college employees. This exchange is allowed only via hard copy.

The College will verify the receiver of the information by having a list of current authorized individuals that are allowed access to certain information. The College will validate that the receiver is on the list and document the information given as well as the identity of the requestor in a secondary dissemination log.

Incident Response

All users are responsible for reporting known or suspected information or information technology security incidents. All incidents must be reported immediately to the College Local Agency Security Officer (LASO). The LASO will inform a member of IT and document the incident. If a suspected incident occurs on the FDLE CJIS workstation, the user shall not turn off the device. The user will leave the device on and report the incident. The College will employ Microsoft System Center Endpoint Protection on the desktop and will ensure that the antivirus software is up-to-date. Incident response will be managed based on the level of severity of the incident. The level is a measure of its impact or threat on the operation or integrity of the College and its' information. High Level (potential to impact the desktop or criminal justice information) Medium Level (potential to impact a

Title: Criminal Justice Information Handling and Storage (Employee Handling of Employee Records)	Number: A6Hx2-3.55A
Policy Number: 6Hx2-3.55	Page: 3 of 6

non-critical system) Low Level (has little or no risk of infecting a criminal justice system). If the level is moved to High, the LASO will notify FDLE immediately. All security incidents will be documented on a security incident reporting form, kept by the LASO and retained for no less than a three year period.

Account Management
The College LASO is the point of contact for all accounts. The LASO shall manage information system accounts to include establishing, activating, modifying, reviewing, disabling, and removing user accounts on all Criminal Justice Information.

Account Modification
In the event of promotion, demotion, suspension, leave or voluntary or involuntary termination, the LASO will ensure the appropriate access changes are made to systems and applications

System Access Control
Access to College information system(s) are based on a user's right to know, authority, and user group. The College allow multiple concurrent sessions within the network.

Remote Access
Remote access to FDLE CJIS workstations is not allowed.

Personally Owned Information Systems Access
The College does not allow personally owned devices to access, store or transmit criminal justice information.

Authentication Strategy
This Password Policy applies to all information systems and applications that contain criminal justice information or services. This includes, but is not limited to:

- FDLE CJIS workstations.
- Mainframes, servers and other devices that provide centralized computing capabilities
- SAN, NAS and other devices that provide centralized storage capabilities.
- College issued desktops, laptops, or any other device that provides distributed computing capabilities.
- Routers, switches and other devices that provide network capabilities.
- Firewalls and other devices that provide dedicated security capabilities.
- Windows Domain Accounts, college e-mail accounts, as well as any other criminal justice information system or service.

Each account is set up with a temporary password. When the user initiates a first-time log-on, the temporary password will be entered and the user will be prompted to create a new password. The College dictates that each password and User-ID be unique and not be shared with any other individual. Users are forbidden to share their unique password or write it down. All passwords must be memorized.

Recommending Officer's Signature	Date:	President's Signature	Date:
Denese Edsall, PhD	09/25/2018		9/25/2018

Title: Criminal Justice Information Handling and Storage (Employee Handling of Employee Records)	Number: A6Hx2-3.55A
Policy Number: 6Hx2-3.55	Page: 4 of 6

Password Requirements

The College utilizes individual passwords for gaining access to criminal justice information and systems. As such, all passwords must follow the requirements outlined below:

- College user passwords must contain at least 8 characters
- The user may not use a proper name or a dictionary word as a password
- The user cannot use their user-id as the password
- The password is set to expire every 60 days
- The user cannot reuse the previous 10 passwords
- The password cannot be transmitted in the clear outside the secure location
- The password will not be displayed when entered

Authenticator Management

Each user that accesses criminal justice information must be uniquely identified prior to being given access to the system and information. The College uses standard authenticators (passwords) for accessing criminal justice information in a secure manner.

A temporary standard authenticator is given to the user via the LASO during the first active session the user has. The user then creates a new password outlined in the authentication strategy policy.

Media Protection Management

Physical media is restricted to authorized individuals. Only those users of the College who have undergone a fingerprint based record check and have appropriate security awareness training will be allowed to handle criminal justice information in any form.

Handling physical media - The College will ensure that only authorized individuals will be granted access to media containing criminal justice information. The media will be stored within the physically secured room and kept behind locked doors and locked cabinets.

Any media that is transported outside the physically secured location will be kept in a sealed envelope with evidence tape to ensure that the chain of custody is kept. When the media is released to another user, the user will document the transaction in a secondary dissemination log for validation purposes. At no time will the physical media be released to an unauthorized person or left without proper documentation.

Electronic Media Sanitization and Disposal

All electronic media must be properly sanitized before being transferred from the custody of the College. The proper method of sanitization depends on the type of media and the intended disposition of the media.

Hard Drives: The College will overwrite the hard drive utilizing a three pass wipe. This will ensure that the data on the drive is overwritten with patterns of binary ones and zeros. The sanitization of the hard drive is not complete

Title: Criminal Justice Information Handling and Storage (Employee Handling of Employee Records)	Number: A6Hx2-3.55A
Policy Number: 6Hx2-3.55	Page: 5 of 6

until the third wipe passes and a verification pass is complete. Destruction of the hard drive will incorporate drilling into the drive. This will be carried out or witnessed by authorized college employees.

Disposal of Physical Media

When no longer needed, physical media such as hard copy print-outs shall be disposed of by the following method:

1. Shredded using a College owned cross-cut shredder. The shredding will be done by authorized College employees.

Physical Protection

Physically Secure Location:

The Human Resources Office is deemed a physically secured location. Only authorized employees have access to the office. The office is equipped with badge swipe access for human resources employees. Visitors must sign in at the front desk and produce identification. The College does not allow unescorted access by any non-college employee. When escorted into the building and be accompanied by an authorized college employee. All physical media containing CJI will be locked in filing cabinet in a locked office. Only authorized employees will have a key to the cabinet. Any transportation of CJI will be done so securely. Only authorized employees can transport CJI. It will physically be with the employees. All College computers will be equipped with boundary protection tools and spam and spy ware to avoid any intrusion attacks.

Encryption

All encryption will be FIPS 140-2 certified and the certificate will be documented/kept by the LASO.

Voice over Internet Protocol

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) - A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

The FDLE CJIS workstations are not connected to internal networks.

Patch Management

FDLE CJIS workstations owned by the College must have up-to-date operating system security patches installed in order to protect the device and network from known vulnerabilities.

Recommending Officer's Signature	Date:	President's Signature	Date:
Denese Edsall, PhD	09/25/2018		9/25/2018

Title: Criminal Justice Information Handling and Storage (Employee Handling of Employee Records)	Number: A6Hx2-3.55A
Policy Number: 6Hx2-3.55	Page: 6 of 6

IT will manage the patching needs for the FDLE CJIS workstations. IT will routinely assess the compliance of the patching policy and will provide guidance to all employees of any security and patch management issues. IT also approves monthly and emergency patch deployments if necessary.

Security Alerts and Advisories

The IT Department will monitor and/or receive alerts and advisories from the locations listed below. If an alert is determined to be critical or pertinent to college infrastructure, the appropriate employees will be notified. All alerts and related actions will be recorded into an information log for college records.

The IT department has signed up for alerts and advisories from the following sites:

- www.us-cert.gov/ncas/current-activity
- https://tools.cisco.com/security/center/publication
- https://technet.microsoft.com/en-us/security

1. The College will receive information system security alerts and advisories
2. Once an alert has been received or detected and has been determined to be a credible threat, IT will notify the College LASO.
3. The College will receive information system security alerts and advisories
4. Once an alert has been received or detected and has been determined to be a credible threat, IT will notify the College LASO.
5. IT will take appropriate action depending on the alert. This could include updating security settings and/or issuing information to all relevant college employees with directions to ensure proper handling of the issue.
6. IT will document the details of the alert. The log will remain with IT for a period of four years.

Wireless Access Restrictions

Wireless technology is not utilized by the College to connect or transmit any of FDLE CJIS data.

Review of Wi-Fi Logs

Wireless technology is not utilized by the College to connect or transmit any of FDLE CJIS data.

Bluetooth

Bluetooth technology is not utilized by the College to connect or transmit any FDLE CJIS data.

Recommending Officer's Signature	Date:	President's Signature	Date:
Denese Edsall, PhD	09/25/2018		9/25/2018