Florida A & M University
Office of Human Resources

HR POLICY-PROCEDURE

Operating Procedure No: HR 1002

Operating Procedures for CJIS Compliance

Operating Procedure No. **HR-1002**	**Date of Adoption/Revision:** **March, 2017**
Subject	Employee Background Screening, Fingerprinting and Notification of Felony or First Degree Misdemeanor-associated with FAMU regulation 10.131
Authority	Sections: 1001.74, (19), 1001.75, 110.1127, 231.02, 282.0041, and 402.302, Chapter 777, Florida Statutes and Chapter 435, Florida Statutes. Florida A&M University Regulation 10.131
Applicability	This procedure sets the guidelines by which background screenings and criminal history checks will be conducted on job applicants who are being considered for employment, employees and volunteers who occupy positions of special trust or responsibility or are located in safety sensitive areas.

Table of Contents:

PURPOSE/OVERVIEW

The purpose of this policy is to specify the protocols and responsibilities of Florida A&M University (University) in conducting security checks/screenings on job candidates: (1) in which an offer of employment has been extended; (2) in specific cases for executive level or law enforcement positions where top candidates may be considered for final selection. In addition, this policy addresses security background checks involving current employees and notification to University management of any felony or certain first degree misdemeanors by current employees.

The University shall adhere at a minimum to the CJIS Security Policy, the University may augment or increase the standards, but will not detract from the CJIS Security Policy Standards.

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

Security background checks/screenings involving current employees and volunteers; and notification to University management of any felony or certain first degree misdemeanors by current employees if applicable to their positions are also addressed. This regulation supplements the employment and education verification process performed in support of the University's hiring process. This policy applies to all employees and volunteers in positions of special trust or responsibility or positions located in safety, informational, or fiscally sensitive areas. Its application is subject to the terms and conditions of any existing applicable collective bargaining agreements.

Definitions

Level 2 Background Check: Fingerprints processed through the Florida Department of Law Enforcement (FDLE) or other entities with the ability to do state and national fingerprint based criminal background checks.

Sensitive or Special Trust Positions: Positions including volunteers whose responsibilities may include, but are not limited to, one or more of the following duties: working with vulnerable populations; access to certain university assets, payroll processes and property; ability to process a payment or purchase, print or distribute.

National Child Protection Act: The purpose of the National Child Protection Act of 1993 is to encourage states to improve quality of their criminal history and child abuse records.

Lunsford Act: Florida legislation focused primarily on increasing the measures used to monitor sexual offenders or predators and put new pressure on public school districts to perform background checks on contractors and subcontractors (basically anyone given access to school exclude individuals from employment on the basis of their conviction records.

Green factors: EEOC guidelines that require the employer to evaluate whether an arrest record should exclude individuals from employment on the basis of their conviction records.

FDLE: The Florida Department of Law Enforcement

Personally Identifiable Information (PII) is information which can be used to distinguish or trace an individual's identity such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Responsibilities

1. A Level 2 background check shall be conducted on prospective new hires, volunteers or current employees including executive, staff and faculty who formally apply for a position designated as a Sensitive or Special Trust as a condition of employment, set forth in Section 8 below.
2. Level 2 checks are performed through the Office of Human Resources and utilize the applicant's fingerprints. Fingerprints are processed through the Florida Department of Law Enforcement (FDLE) or other entities with the ability to do state and national fingerprint based criminal history checks. Criminal history information will be used only for the purpose of verification of the prospective employee's criminal history background.
3. Positions with specific fiduciary responsibilities may require a credit check prior to employment if directly related to the position and aligned with The Fair Credit Reporting Act (FCRA).

a. Written permission from the individual whose credit report they seek to review must be obtain.

b. Notification before any adverse action (e.g. failing to hire, promote or retain an employee) based in whole or in part on any information in the credit report.

c. A copy of the credit report and a written summary of the consumer's rights along with this notification

d. Reasonable period (five working days) for the applicant to identify and begin disputing any errors in their credit report.

e. Notify the job applicant of the adverse action if no response.

4. Position descriptions for A&P, A&P Executive and USPS and Assignment of Responsibility (AOR) for Faculty positions and position advertisements shall provide notice to prospective employees that a criminal history background check or credit check will be conducted a condition of employment. OPS and volunteer positions must also provide notice when appropriate (working with vulnerable populations). Notice of a pending background check shall also be provided in any offer of employment that is extended prior to a criminal history background check being conducted. The post-offer, pre-employment background check/screening information may include:

    i. Name and Address Verification

    ii. Social Security Number Verification

    iii. Criminal History via Fingerprinting Search (state and/or national)

    iv. Credit Check if appropriate

If a candidate is rejected because a background check, upon request and with the University's archiving period of the document, they may obtain a copy of the FDLE background check report through the University Office of Human Resources.

5. Sensitive and Special Trust applies to all positions including volunteers whose responsibilities may include, but not be limited to, one or more of the following duties:

    a. Working with children/minors (National Child Protection Act 1993 as amended). A child/minor is defined as any person under the age of 18 in accordance with Section 827.01 and Chapter 1012 and Section 1012.465 Florida Statues;

    b. Access to cash, credit card numbers and/or demand deposits;

    c. Access to campus buildings, including residences as a result of being assigned building master keys;

d. Access to surplus property;

e. Ability to complete final processing of payroll or payroll corrections, investments, security access transactions or purchase orders;

f. Ability to process a payment, print or distribute checks;

g. Ability to update, prepare, generate or enter a transaction that will result in one of the following: refund, wire transfer, automatic clearing house transaction, vendor add/change or vendor address; or

h. Ability to access underlying codes/processing protocol supporting the University's Office of Information Technology (OTS) systems applications or complete final processing of OTS security access transactions.

6. A security background check/screening to verify that the candidate possesses a valid driver's license and verify the candidate's driving history will be performed on candidates offered positions whose duties include, but are not limited to operating licensed motor vehicles owned by the University at least one or more times per week. Drivers' license/driving record checks will be performed annually at the discretion of University management.

7. With the exception of any offense that precludes an applicant from employment as specified in federal or state statutes, if the security background check/screening reveals that an applicant has pled nolo contendere (no contest) to, or been convicted of, a first-degree misdemeanor or a felony, or adverse driving history where applicable, the following factors (Green factors) will be considered to determine whether the convictions are grounds for delaying or continuing employment or acceptance as a volunteer:

    a. The nature and gravity of the offense(s) for which convicted and/or restitution given;

    b. The time period that has lapsed since the conviction;

    c. The nature of the position being considered in relation to the offense;

    d. Falsification of employment and personnel-related documents pertaining to minimum qualifications of the position or information that would disqualify them from the position.

8. A security background check/screening may be conducted on a current employee: if University management has reason to believe an employee falsified his or her employment application and/or other personnel-related documents; if the employee occupies a position of special trust or responsibility or positions located in safety sensitive areas and a security background check/screening was not conducted at the time of hire; or for other justifiable reasons. Except for ongoing police investigations, the Office of Human Resources will be responsible for conducting any security background checks/screenings on current employees. Should a security background check/screening

reveal any felony or first degree misdemeanor convictions not previously divulged by an employee/volunteer, the Office of Human Resources will consult with the appropriate hiring authority regarding the individual's continued employment.

9. Current active employees and volunteers shall notify University management of any felony or first degree misdemeanor to which they have pled nolo contendere (no contest) or guilty or are convicted of, or if applicable to their position, if their driver's license is suspended subsequent to their employment or volunteer work with the University. Such notification must be made within three (3) working days of the conviction or driver's license suspension. Factors identified in section 7 above will be considered in determining the individual's continued employment.

SECURITY AWARENESS AND LOCAL SECURITY AGENCY OFFICER (LSAO) TRAINING

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI. The University will accept the documentation of the completion of security awareness training from another agency.

PERSONALLY IDENTIFIABLE INFORMATION (PII)

In circumstances where PPI may need to be extracted from criminal justice information (CJI), personnel must have written consent from Associate Vice President, Chief Human Resources Officer. Once PII has been used, personnel must dispose of all information properly. PII must not be disseminated to other agencies.

INFORMATION EXCHANGE

At this time, FAMU does not exchange or disseminate information.

Before dissemination of CJI FAMU will contact FDLE for written authorization to release to requesting agency.

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.

INFORMATION HANDLING

Information obtained from the Florida Department of Law Enforcement Secure Mail application, must only be used for statute mandated purposes only. Personnel must follow all CJIS Security Policy, state and federal rules and regulations regarding CJI information.

All personnel with access to CJI, audio as well as visual, shall receive the proper training within 30 days of hire. CJI or PII will not be transmitted via email unless encrypted. All information outlined in the information exchange and disposal of physical media shall be followed as well.

INCIDENT RESPONSE

Should an incidence occur involving any device (workstations, smart phones, laptops, tablets, etc.) that is on the University's network, the Local Agency Security Officer (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.

FAMU will identify the security breach by conducting the following:

1. Confirm the discovery of a compromised resource(s).
2. Evaluate the security incident.
3. Identify the system(s) of information affected.
4. Review all preliminary details
5. Characterize the impact on the agency as: minimal, serious, or critical.
6. Determine where and how the breach occurred.
    a. Identify the source of compromise and the time frame involved. Review the network to identify all compromised or affected systems.
7. Examine appropriate system and audit logs for further irregularities
    a. Document all internet protocol (IP) addresses, operating systems, domain system names and other pertinent system information.
8. Initiate measures to contain and control the incident to prevent further unauthorized access.
9. Document actions throughout the process from initial detection to final resolution.

PERSONALLY OWNED INFORMATION SYSTEMS

Personally owned devices are not allowed to access the agency's network. Therefore, a device that is not owned by FAMU, shall not access CJI.

MEDIA PROTECTION

Media in all forms shall be protected at all times. Electronic media (i.e. hard drives, disks, flash drives, etc.) shall be behind locked doors at all times with access granted only to authorized personnel only.

Physical media (i.e. physical documents) shall only be stored for case file and validation purposes. CJI stored will be placed in locked filing cabinets behind locked doors. Only authorized personnel will be granted access. All other forms of CJI shall be shredded when not in use.

DISPOSAL OF PHYSICAL MEDIA

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

PHYSICAL PROTECTION

FAMU's hardware, software, and media containing confidential information will be stored behind locked doors. Only authorized personnel with a "need to know" or "right to know" based on job duties will have access.

FAMU shall control physical access by authenticating all visitors before authorizing escorted access to the physically secure location. FAMU shall escort visitors at all times and monitor visitor activity.

PERSONNEL SANCTIONS

All personnel with FAMU shall adhere to all policies. Failure to do so will require review by the University President. Once reviewed personnel may receive disciplinary actions, up to and including termination and/or criminal prosecution