Florida Department of Law Enforcement

Policy # 2.5

INFORMATION TECHNOLOGY

INDEX:

RELATED REFERENCES:

FDLE Policy 2.3 – Use of Social Media

FDLE Policy 2.6 – Use of Information Technology

ITS Procedures:

8.300 Computer Security Incident Response

Federal Information Processing Standards (FIPS) Publication 199 - Security Categorization

FBI CJIS Security Policy

ISDM Quick Reference Guide

ISDM on the FDLE Web (www.fdle.gov/ISDM)

FDLE Member Remote Access Request Form

Non-FDLE Member Remote Access Request Form

Florida Statutes Section 112.313(6) – Code of Ethics for Public Officers and Employees

Florida Statutes Section 119.071 – Public Record

Florida Statutes Section 839.26 - Misuse of confidential information

Florida Statutes Section 282.318 - Communications and Data Processing

Florida Administrative Code Rule 71A-1 – Florida Information Technology Resource Security Policies and Standards

PROGRAM OF RESPONSIBILITY: Division of Information Technology Services

POLICY:

FDLE's information technology infrastructure is critical to the agency's mission. It is tightly woven into the essential business functions and is an integral part of all tasks. When the technology infrastructure is not available, critical services cannot be performed.

All members and persons accessing FDLE networks or applications must comply with federal and state law and rules in their operation and use of FDLE IT systems or equipment.

Appropriate security controls must be in place to support a standard process for reporting, responding to, mitigating, and documenting computer security incidents.

In order to achieve the agency mission, the technology resources - hardware, software, networks, other devices, and data - must be protected. Data and resources must be reliable and must be available to those members and agency customers who have permission to use them.

This security of information resources and protection from unauthorized access or improper disclosures are paramount to FDLE operations. All members are responsible for protecting the information resources of FDLE.

DEFINITIONS:

Agency-Managed Device: A device not owned by the agency; but, the agency ensures the device hardware and software are in compliance with agency standards.

Anti-Malware Software: Software installed on a computing device that protects it from malicious software.

Application Access Administrator: A member designated to administer user identification and access for an FDLE supported application or system.

Authentication (Password): The process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords.

Authentication (Mobile Computing Devices): The process of verifying that a user is who he/she purports to be. Authentication can consist of any of these three techniques: (1) something the user knows, such as a password or PIN; (2) something the user has, such as a smartcard or grid card; and (3) something that is part of the user, such as a fingerprint or the iris of the eye.

Authentication (Advanced): This is also known as Multi-Factor Authentication. It requires a user to present a minimum of two factors to authenticate his/her identity. Traditional user-ID/password combinations are considered to be single-factor because both are 'something a user knows'. A user-ID/password (something a user knows) combined with unique challenge-response grid card (something a user has) would be considered advanced (multi-factor) authentication.

Availability: The principle that authorized users have timely and reliable access to information and information technology resources

Computer Security Incident Response Team (CSIRT): A prearranged group composed of individuals with expertise from various Divisions tasked with responding to any incident that potentially threatens the confidentiality, integrity, or availability of FDLE's information assets, information systems, or information technology equipment and infrastructure. The team comprises, at a minimum, the Chief Information Officer, the Information Security Manager, and a member of the Office of the Inspector General.

Confidential Information and/or Confidential Data: Information/data that is exempted from disclosure requirements under the provisions of applicable state and federal law.

Confidentiality: Ensuring that information is accessible only to those authorized to have access.

Criminal Justice Information (CJI): Data provided by the FBI for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions.

Encryption: The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy.

Extranet: An extranet is a virtual network created by connecting two intranets. An organization that connects remote locations with a Virtual Private Network (VPN) creates an extranet by linking its intranets together to form one virtual network

Firewall: A product or combination of products that enforces a boundary that limits access between two or more networks.

Florida Information Security Officer (ISO): This position is required by the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy to act as the liaison between the FBI and Florida related to the security of CJI. The ISO is to assist interface agencies in developing and implementing security controls for compliance with the CJIS Security Policy.

Intrusion Detection System (IDS): A product or combination of products that can be implemented on host systems or as network devices to monitor for signs of intruder activity and attacks.

Incident Response: The mitigation of violations of security policies and recommended practices.

Information Custodian: The individual or program area that is ultimately responsible for maintaining an information system or data set in accordance with the prescribed requirements set forth by the information owner.

Information Owner: The manager of the business unit who is ultimately responsible for the collection, maintenance, and dissemination of a specific set of information.

Information Resource Request (IRR) Form: A document used to obtain approval from FDLE's CIO to acquire new information technology resources.

Information Security: Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction.

Information Systems Development Methodology (ISDM): A generic, tailorable, scalable process guiding the high level stages of computer applications development. The purpose of the ISDM is to improve quality, efficiency and security of software applications; increase communication among developers and customers; and improve documentation of software activities.

Information Security Manager (ISM): The member designated by the Commissioner who is charged with administering the security program of the Department for its data and information technology resources.

Information Technology Resources: FDLE Information Technology (IT) staff, IT services, computer hardware, software, networks, devices, connections, applications, and data.

Integrity: The trustworthiness of information over its entire life cycle - ensuring that information or data is accurate. Integrity involves "representational faithfulness" which is composed of four essential qualities or core attributes: completeness, currency/timeliness, accuracy/correctness, and validity/authorization.

Least Privilege: The principle that grants the minimum possible privileges to permit a legitimate action in order to enhance protection of data and functionality from faults and malicious behavior.

Login Banner: Information displayed on a personal computer when a person logs into a network or an application.

Media: (information or physical): Computer hard drives, tapes, compact disks (CD), digital video disks (DVD), optical disks, flash drives, and other devices used to store data or software.

Mobile Computing Device: A laptop, tablet, smartphone, or other portable device that can process data.

Mobile Devices: General term describing both mobile computing and mobile storage devices.

Mobile Storage Device: Portable data storage media including but not limited to, external hard drive, thumb drive, floppy disk, recordable compact disc (CD-R/RW), recordable digital videodisc (DVD-R/RW), smartphones, media player, cell phone or tape drives that may be easily attached to and detached from computing devices.

Need to Know: The principle that individuals are authorized to access only specific information needed to accomplish their individual job duties.

Operations/Maintenance: Work undertaken to operate or repair production systems or services. It also includes time devoted to research associated with daily up-keep of production systems or services.

Password Aging: The process of setting a member's password to automatically expire at the end of a fixed period.

Password History: The process of maintaining an automated history of passwords that a member has previously used to access a particular computing resource. This is done to prevent immediate reuse of an expired or compromised password.

Personal Firewall: Software installed on a computer or device which helps protect that system against unauthorized access.

Project: A temporary endeavor undertaken to create a unique product, service or result. A project requires specific start and finish dates. A project will generally introduce new or improved functions to production systems or services, but can include research efforts that focus on new systems, consolidation or expansion, or service/system improvement.

Regional Systems Administrator (RSA): An ITS Member assigned to one of FDLE's Regional Operations Centers tasked with providing technical support for information systems and information technology equipment.

Remote Access: Any access to FDLE's corporate network through a network, device, or medium that is not controlled by the agency (such as the Internet, public phone line, wireless carrier, or other external connectivity).

Security Incident: A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

Service Account: An account used by a computer process and not by a human (e.g., an account used by the backup process for file access). Normally service accounts may not log on to a system.

Short Message Service (SMS): Mobile-to-mobile text messages sent between mobile devices/cell phones by sending a message to the device's phone number.

Software: Instructions for a computer that is licensed for use by a public or private organization or individual. Major categories of software are system software, application development software, and application software. System software is made up of control programs such as the operating system and database management system. Application development software is used to build application software. Application software is any program that processes data for the user (inventory, payroll, spreadsheet, word processing, etc.).

Standards: A specific set of practices or procedures to regulate how a system or organization provides services - required practices, controls, components, or configurations established by a recognized authority.

System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, storing, reporting, printing, dissemination, or disposition of information.

System or Database Administrator: A member designated to administer user identification and access for a FDLE system or database.

Threat: The potential source of an adverse event

User: Any authorized agency member who uses information technology resources.

User-ID: An account name used to identify the user of a computer resource.

Virtual Private Network (VPN): Used to securely connect two networks or a network and a client system over an unsecure network, such as the Internet.

Wireless Network: Any type of computer network not connected by cables.

GENERAL PARAMETERS

A. Information Technology Services (ITS) is solely responsible for access control to all FDLE networks. The Chief Information Officer (CIO) or designee must authorize any network connection planned for any FDLE facility/site. ITS will retain management control over all incoming circuits to any FDLE facility/site. [CALEA 82.1.6 c] [CFA 34.06 c] [CFA 34.12 f,g]

B. All connections between FDLE's network and external networks (such as those of other agencies) must be approved by the CIO.

C. Computer security incidents include any actions or activities that compromise the confidentiality, integrity, or availability of agency information technology resources. FDLE will maintain a standard process for reporting, responding to, mitigating, and documenting computer security incidents.

D. FDLE will acquire, administer, secure, maintain, use, and dispose of information technology resources in compliance with federal and state laws and standards approved by the CIO.

E. All members are responsible for ensuring that only FDLE authorized software is used on computers assigned to them. [CALEA 11.4.4]

F. Each member is responsible for managing his/her access passwords for FDLE resources.

G. The FDLE Information System Development Methodology (ISDM) will be adhered to as a standard method for designing, developing, testing, and implementing custom written software. The ISDM will ensure the timely delivery of high quality products that meet stated requirements.

H. The use of mobile devices poses risks to the information they contain. Use of mobile devices on non-FDLE networks poses risks to agency information technology resources upon subsequent connection to the FDLE network. Appropriate security controls must be in place to mitigate security risks presented by using mobile devices.

I. This policy complements and reinforces FDLE Policy 2.6 – Use of Information Technology.

INFORMATION SECURITY [CFA 34.06] [CFA 34.12 g]

A. Information resources will be used in accordance with procedures/standards established by ITS to perform the business functions of FDLE. These procedures/standards are based on Chapter 71A-1, F.A.C. – Florida Information Technology Resource Security Policies and Standards; the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy, Version 5.2; 28 CFR Part 20 – Criminal Justice Information Systems; and 28 CFR Part 23 – Criminal Intelligence Systems Operating Policies.

B. Information security responsibilities are based on assigned security roles. For example, someone who administers a computer system will have different security duties than someone who uses the system to query or enter information. The information security roles at FDLE are:

1. Information Users are individuals who use or have access to FDLE's information resources, including members, interns, Other Personnel Services (OPS) temporary workers, contractors, vendors, and visitors. Anyone using any kind of FDLE information resource, or having access to any FDLE, client, or government data, is an Information User.

   FDLE members must review, understand, and accept their information security responsibilities as Information Users.

   a. Members must maintain awareness of information security policies by participating in the FDLE information security awareness training program.

   b. Members should discuss with their supervisor or the ISM any information security policies or procedures that they do not understand.

   c. Members must protect FDLE information resources in their possession from theft, loss, damage and unauthorized activities including disclosure,

modification, deletion, and misusage; and immediately report any loss, theft or damage to those resources.

d. Members must obtain, use, or disclose FDLE information only in an authorized fashion and only for authorized purposes.

e. Members must exercise due diligence to prevent accidental access, modification, or deletion of data.

f. Members must act responsibly to ensure the ethical use of FDLE information resources in compliance with FDLE Policy 3.33 – Values and Ethics.

g. Members must promptly report any suspected violations of FDLE security policies to the ISM, the Information Owner, or their supervisor.

2. Supervisors are FDLE members who have formal supervisory responsibility for members, contractors, or other Information Users. This includes managers, supervisors of contract staff, and other supervisory personnel. It is crucial that supervisors serve as a good example for their members to follow in addition to helping members understand and meet their information security responsibilities.

   Each supervisor has the responsibility to help maintain his/her members' information security awareness and to take an active part in protecting the FDLE information resources that they use.

   a. Supervisors will ensure that their members are knowledgeable and trained on information security responsibilities to include those topics required by the FBI CJIS Security Policy.

   b. Supervisors will assist the ISM with ensuring that their members comply with FDLE information security policies and procedures.

   c. Supervisors will review information security reports from the ISM regarding activities of their staff and taking appropriate action.

3. Information Owners are the individuals ultimately responsible for information resources, and are generally Division Directors or designated senior managers. The initial Information Owner is the individual who creates, initiates the creation or storage of information. Once created or installed, the individual's respective FDLE business unit becomes the owner with the appropriate Division Director taking official responsibility.

   Information Owners must exercise due diligence to protect the confidentiality, integrity, and availability of those resources.

   a. The Information Owner must ensure that IT resources are adequately protected, commensurate with their sensitivity, criticality, and level of risk. This includes the planning and implementation of technical, managerial, and operational security controls.

b. The Information Owner must ensure that information resources are in compliance with all FDLE information security policies, procedures and standards, as well as state and federal laws.

c. The Information Owner may delegate administration and maintenance of the resource, but must understand that he/she are still ultimately responsible for that resource, and thus need to actively monitor that custodianship.

d. The Information Owner must create and maintain thorough documentation of the information resource and the security measures employed to protect it.

4. Information Custodians are individuals who develop, implement, maintain, or administer information resources on behalf of Information Owners. For example, ITS staff (including system engineers, database administrators, application developers, etc.) often serves as custodians for systems or data owned by FDLE business units.

   Information Custodians implement and operate the security controls that have been prescribed for the application(s) or systems(s).

   a. Information Custodians will assist the Information Owner with planning safeguards to protect the resource and to ensure compliance with all FDLE information security policies.

   b. Information Custodians will maintain thorough, up-to-date documentation on the resources.

   c. Information Custodians will adhere to all FDLE information security standards and procedures for administration and maintenance of the resource (e.g., change control, backup requirements, etc.).

   d. Information Custodians will implement and operate the safeguards for the resource.

   e. Information Custodians will immediately report possible security incidents to the ISM.

   f. Information Custodians will assist the ISM with auditing resources under their management and (if requested) investigating security incidents which affect those resources.

   g. Information Custodians will assist with the recovery of resource functionality and integrity in the event of a disaster.

5. Application Access Administrators (AAA) are individuals designated by Information Owners to grant, modify, and revoke access to information systems (i.e., applications).

C. In addition to the general security roles, there are a few individual positions that have specific security responsibilities. These include:

1. The Information Security Manager (ISM) is the individual designated within FDLE to develop and operate the information security program. The ISM is responsible for ensuring that FDLE complies with federal information security requirements and other applicable laws, and that FDLE resources are adequately protected.

2. The FDLE Security Officer is the member responsible for the security of FDLE facilities, personnel, and classified information. The FDLE Security Officer may also assist the ISM with investigations of violations and is responsible for granting, denying, suspending, reducing, or revoking security clearances.

3. The Designated Approving Authority (DAA) is the person who certifies and accredits information systems for operation on the FDLE network. This role is filled by the CIO or designee.

4. The Florida Information Security Officer is the member responsible for assisting the agency to ensure its compliance with the FBI CJIS Security Policy.

D. All members must use computer software in compliance with the terms and conditions specified in the software license agreement and restrictions against unauthorized duplication or distribution. [CFA 34.06 c] [CFA 34.12 g]

E. Wireless transmission of agency data will be implemented using strong cryptography for authentication and transmission.

F. All devices (computers, laptops, smartphones, etc.) will be protected with an automated timeout of a maximum of 15 minutes. This fulfills the requirements of Chapter 71A-1, the State of Florida Information Technology Resource Security Policies and Standards as well as the FBI CJIS Security Policy, Version 5.2.

G. All users must take steps to avoid introducing viruses into FDLE's computing environment, including:

1. Never open any files attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately and empty the email trash folder.

2. Delete spam, chain, and other junk email without forwarding.

3. Never download files from unknown or suspicious sources.

4. Never install any software on, or connect hardware (e.g., smartphones) to, FDLE computers without specific permission from ITS.

H. Other than when specifically authorized by reason of official duties, members using FDLE equipment or infrastructure at FDLE facilities are prohibited from intentionally accessing, downloading, processing, or transmitting Internet, printed, video or audio material or messages of which the possession or use is a violation of law, regulation, or policy. Supervisors are charged with the duty of assuring that members under their supervision are in compliance with the stated restrictions.

I. All members are prohibited from the intentional or willful access, transmittal, communication, or display of sexually-explicit images, text, music or any other data that reasonably appears to be designed to cause sexual excitement. [CFA 34.12 b] Notwithstanding any previous Department response to similar violations, any FDLE member found to have violated this standard (other than as specifically authorized in an official criminal or internal investigation), will be suspended for not less than ten (10) workdays. Any subsequent incidents will result in dismissal from employment. [CFA 34.12 a]

J. Media Transportation and Storage

1. Members must never store sensitive or confidential information on portable media unless they are authorized to do so and take security precautions required by law.

2. Members must label any media containing sensitive data with special handling instructions.

3. Members must secure any media containing sensitive data when it is not in use or is unattended.

4. Members must double-seal the media with the outer envelope appropriately marked to reflect the level of sensitivity and the intended recipient when sending any media containing sensitive information through the mail or via a courier/messenger service.

5. The delivery and receipt of media containing sensitive data must be monitored and accounted for to ensure that data is not lost and potentially compromised while in transit.

6. Members must immediately report to the Customer Support Center (CSC), ISM, or CIO the loss, theft, tampering, unauthorized access, or damage of any storage media that contain critical or sensitive FDLE data.

7. Members may not store or share files using online services (i.e., “Cloud Storage” providers such as DropBox, Microsoft SkyDrive, or Google Drive) without the written consent of the CIO.

8. Members who are authorized to use cloud storage services must notify the CIO and the Information Owner if the purpose or intent for using cloud storage changes from that which was originally authorized.

K. Information media will be sanitized or destroyed prior to disposal. ITS will document and implement procedures for the destruction of information media that satisfy the requirements of the CJIS Security Policy and State rules and regulations.

L. The security of an information system will be ensured through a joint effort between the information owner and the information custodian. Information owners will prescribe requirements to protect the confidentiality, integrity, and availability of information that are commensurate with the criticality of the information. Information custodians will implement controls to maintain the systems hosting the information in a manner consistent with the prescribed requirements.

M. Electronic transmission of information that is exempt from public disclosure as defined in Section 119.071, F.S. (General exemptions from inspection or copying of public records) or that meets the definition of CJI must be encrypted when transmitted outside of FDLE's internal network (e.g., via mobile device or over the Internet).

N. The ISM will implement and maintain an ongoing information security awareness program.

1. At a minimum, members will receive annual information security awareness training related to:

   - Florida Statutes and Florida Administrative Code
   - CJIS Security Policy
   - FDLE Policies and Procedures as they relate to information security and acceptable use.

   Records of completion will be maintained according to FDLE Policy 3.14 – Employee Development, Education, and Training.

2. New members will receive initial information security awareness training within 30 days of their employment start date.

3. Members whose job duties bring them into contact with confidential and/or exempt information will receive further specialized training.

4. The ISM will periodically issue information notices to FDLE members to remind them of basic security practices (e.g., protecting passwords). The ISM will also provide briefings on special topics (e.g., spam filtering).

O. The Florida ISO will ensure that Members complete specialized CJIS information security awareness training when such is required based on their assigned job duties. The ISM will assist the ISO as needed.

P. Risk Assessment and Management

1. FDLE's Information Owners, Information Custodians, and the ISM will categorize production systems according to the Federal Information Processing Standards (FIPS) Publication 199, based on the magnitude of harm that would occur if confidentiality, integrity, or availability were compromised.

2. FDLE will maintain a documented risk management plan for all systems categorized as high-impact systems.

3. FDLE will conduct a comprehensive risk assessment once every three years.

4. FDLE will implement a risk mitigation plan to address the findings of risk assessments to reduce the identified risks to the agency.

5. The ISM will monitor and document risk assessment and risk mitigation activities.

Q. Audit

FDLE regularly audits the use of information resources to ensure accountability, detect security violations, and to proactively scan for vulnerabilities. All use of FDLE information resources may be monitored by FDLE at any time. **Users have no expectation of privacy or anonymity while using FDLE information resources, including email and Internet access.**

1. Automated records of access to and alteration of information systems and data are maintained in order to enforce information usage policies and security measures, and to be able to investigate security incidents. To accomplish this, a record of activity (a "log" or "audit trail") of system and application processes and user activity of systems and applications is maintained. This is used to investigate security incidents, monitor use of FDLE resources, provide accountability for transactions, track system changes, and assist in detection of system anomalies. Audit trails also assist in detecting security violations, performance problems, and flaws in applications.

2. Information Systems Custodians (on behalf of Information Owners) have the ability to audit network logs (via server, application, router, firewall and other major network device transaction logs), employ monitoring tools, and perform periodic checks for misuse. The ISM or Office of the Inspector General (OIG) or other specifically authorized personnel will be granted access to review audit logs containing accountability details.

COMPUTER SECURITY INCIDENT RESPONSE

Security incidents include any actions or activities that compromise the confidentiality, integrity, or availability of agency information technology resources. FDLE will maintain a standard process for reporting, responding to, mitigating, and documenting computer security incidents.

Examples of information security incidents include (but are not limited to):

1. Suspected violations of any FDLE information security policies or FBI CJIS Security Policy, or other State rules and regulations

2. Loss or theft of laptops, mobile devices (such as tablets), security tokens, or other items, or compromise of login credentials (i.e., usernames/passwords) that may provide access to FDLE information resources or contain FDLE data

3. Attempts by unauthorized individuals to gain access to FDLE information or systems

4. Accidental disclosure, modification, or destruction of information

A. All Information Users must immediately report any suspected information security incidents so that FDLE may respond in a timely manner to correctly handle the incident, minimize disruption of critical information services, and minimize loss or theft of sensitive and mission-critical information. Suspected computer security incidents should be reported to the ISM and to the CSC.

B. FDLE has established a Computer Security Incident Response Team (CSIRT) that is responsible for responding to information security incidents. The team will convene at least quarterly to review the agency's response posture, reporting to the CIO.

C. The CSIRT will determine the appropriate response required for each suspected computer security incident.

D. As needed, the CSIRT may enlist additional members with specific knowledge or expertise from FDLE's various Divisions.

E. Computer security incidents must be documented, escalated, and reported as specified in the CSIRT procedure.

F. Computer security incidents must be reported to the CIO and the Office of Executive Director (OED). It will be the responsibility of the ISM to make such reports. The CJIS Director, as Florida's CJIS Systems Officer, and the Florida ISO must be notified if criminal justice information is affected by the incident.

G. A report of each suspected computer security incident, including findings and corrective actions, must be documented and maintained as specified in the CSIRT procedure.

H. Computer security incident documentation is exempt from public disclosure (282.318, F.S.).

ACCESS TO FDLE INFORMATION SYSTEMS

Access to FDLE's information systems is controlled at two levels. The first level is the network – which is controlled by ITS. The second level is the individual application (i.e. Florida Crime Information Center (FCIC), Computerized Criminal History, or Evidence Management System) managed by Application Access Administrators (AAA) with support from ITS.

A. Level 1 - Gaining Access to FDLE Network

1. To obtain a network user account for a new member or authorized contractor, a supervisor must submit a written request to the CSC, preferably through the Self-Service Helpdesk. This request must include the following information:

    - First Name, Middle Initial, and Last Name of FDLE member or contractor
    - Position Title
    - Assigned Division and Office
    - Office Street Address
    - Telephone Number
    - Projected Start Date

2. Only FDLE-owned or FDLE-managed computing devices, whether fixed or mobile, will be allowed to directly connect to the FDLE network.

3. With the exception of the FDLE intranet website, users must not browse through FDLE computer systems or networks. For example, curious searching for interesting files and/or programs in the directories of other users is prohibited. Steps taken to legitimately locate information needed to perform one's job are not considered browsing. This statement on browsing does not apply to external networks such as the Internet.

4. No privately-owned devices (e.g., smartphones, MP3 players, thumb drives, printers) will be connected to FDLE information technology resources or internal networks without documented authorization from ITS.

B. Level 2 – Access to Individual Applications

1. System and Database Administrators may not grant application access without permission from the data owner.

2. Initial Member/Contractor Access - The member's or contractor's supervisor is responsible for requesting member access to any specific applications necessary for the member/contractor to complete his/her duties. The supervisor will contact the appropriate system Application Access Administrator (AAA) to obtain access for a member.

3. Member/Contractor Transfers/Reassignments – The Office of Human Resources (OHR) will forward the Employee Status Report to the AAA(s) on a regular schedule. This report provides a list of all separations, reassignments, promotions, demotions, and new hires for the period since the last report.

4. ITS will forward a Contractor Status Report to the AAA(s) on a regular schedule.

5. The AAA(s) will review the reports and check any member/contractor movements against the system access files. If the status reports indicate that a member/contractor should not need access to a system to which he/she currently has access, the AAA will contact the member's/contractor's supervisor to confirm. Upon confirmation by the supervisor, the AAA will inactivate or remove member/contractor access to the system.

6. Member Arrest - If a member is arrested, the member's supervisor will be notified through his/her chain of command. Upon notification, the supervisor is responsible for contacting the appropriate AAA(s) to revoke or restrict access to any systems/databases the member is no longer authorized to access based on his/her criminal history. The supervisor must also contact the CSC to suspend of the member's network access account. The CJIS Director must be notified in order to determine continuance of CJIS access.

7. AAA(s) will perform an access audit of each information system semiannually.

C. Terminating Access to FDLE Information Systems

1. As they occur, the OHR will provide ITS with an email of member terminations. This email will be used to identify network accounts that are to be terminated and forwarded to the AAA list to terminate application/system access.

2. It is the responsibility of each member's immediate supervisor to notify ITS CSC when a non-FDLE member (such as a task force member or contractor) is terminating employment with FDLE. FDLE supervisors will notify the CSC via e-mail or fax. The supervisor will also notify the FDLE AAA(s) via email to remove application/system access.

3. The OHR will provide the Employee Status Report that lists promotions, demotions, transfers, and terminations each month to the ITS and AAA(s).

4. ITS's Production Systems Bureau, Database Management Section, and FDLE AAA(s) will terminate user accounts.

D. Network Remote Access

Remote access to FDLE internal networks is not a privilege and may be revoked at any time for cause including the normal revocation reasons (termination or reassignment), unsatisfactory performance, or non-compliance with security policies.

Members are prohibited from establishing remote access connections to the FDLE network from personally-owned computing devices, including but not limited to desktop computers, laptop computers, tablets, and smartphones.

1. Access to FDLE internal networks from remote locations including homes, hotel rooms, and other offices must be requested through the FDLE Member Remote Access Request Form or Non-FDLE Member Remote Access Request Form.

2. These request forms are available in the Related References of this policy or on the FDLE corporate website - see ITS Forms, Member Remote Access Request Form or Non-FDLE Member Remote Access Request Form.

3. FDLE Member Remote Access Request

    a. FDLE members requesting access must review and understand this policy and FDLE Policy 2.6 Use of Information Technology.

    b. All request forms must be approved (signed) by the requestor's immediate supervisor(s).

4. Non-FDLE Member Remote Access Requests

    a. In strictly controlled situations, FDLE may allow non-FDLE members temporary access to the agency's internal network and connected computer systems.

    b. This request for access must start with successful completion of a background investigation - only then can the non-FDLE Member request remote access by submitting a non-FDLE Member Remote Access Request Form.

c. All non-FDLE members requesting access must review and understand FDLE Policy 1.4 Use of FDLE Resources and FDLE Policy 2.5 Information Resources.

d. The FDLE supervisor approving access must also sign the Non-FDLE Member Remote Access Request Form (in addition to the non-FDLE supervisor or manager). The non-FDLE member's FDLE supervisor and non-FDLE supervisor must be aware of, and approve, the remote access request.

e. All non-FDLE members are required to renew their remote access privileges every six months by completing a new Non-FDLE Remote Access Request Form. This is to ensure that access to resources is reviewed and modified if necessary based on need such as a transfer to a new work area or other change in job responsibilities. All access changes will be captured in the space provided on the Non-FDLE Member Remote Access Form.

f. Privileges for non-FDLE members will be strictly limited to only the system(s) and information needed to achieve predefined business objectives. Space has been provided on the form to list any systems that the non-FDLE member might need to access.

g. Non-FDLE member accounts are set to expire automatically at the end of six months.

5. Third Party Vendor Access

a. Third party vendors that provide FDLE with hardware, software, or communications services are not automatically granted access to FDLE internal computers and/or networks.

b. At a minimum, ITS will require a memorandum of agreement between the third party and FDLE that will outline the type of connection, hours of service and required access levels. The memorandum must be approved by the FDLE CIO.

c. All vendor personnel with access to this remote connection must pass a background check and complete the Non-Member Remote Access Request Form as outlined in this section.

6. Submission and Approval

a. Remote Access Request Forms should be submitted to the CSC via interoffice mail, e-mail, or fax.

b. The written request (FDLE member and non-FDLE member) will be reviewed, authenticated, and approved or denied (with signature) by the ISM acting as the designee for the CIO.

c. Notification will be sent to the member and his/her immediate supervisor once final access has been granted.

d. Any questions concerning the request should be e-mailed to the ISM.

7. Suspension Due to Foreign Travel

    a. Remote access will be temporarily suspended for any user traveling outside of the U.S.

    b. Exceptions will be considered by the CIO on a case-by-case basis when foreign travel is required as part of a user's assigned duties. It will be the responsibility of a Member's supervisor to request an exception.

8. Revocations

    a. The CIO, ISM, or any supervisor has the right to revoke remote access privileges.

    b. The request for revocation can be made by any means necessary.

    c. Revocation requests should be made to the CSC by phone, e-mail, or fax. If the revocation request is considered urgent, the CSC will contact an on-call ITS member for immediate action.

    d. The requestor, CIO, and the ISM will receive notice of the revocation, the reason for the revocation, and the service ticket tracking number.

9. Terminations

    a. Termination of remote access follows the same procedure detailed in section C above.

    b. Since remote access is an additional access privilege that requires (and is linked to) an active network account, the already established process of disabling a user's network account will also disable his/her ability to gain remote access.

10. Audit

    a. To assist with auditing and reviewing access accounts with remote access privileges, ITS will provide each division director with a list that identifies members and non-FDLE members in his/her division that have remote access privileges to FDLE computing resources. This list will be distributed annually for FDLE members and semi-annually for non-FDLE members by the CIO.

    b. The ISM will coordinate with the division directors to complete the review and verification effort.

    c. Upon receipt of the verified list of users, the ISM will take appropriate action to remove members and notify division directors within 30 days. [CALEA 82.1.6]

11. Advanced Authentication

a. All remote access to FDLE networks and systems on or after September 1, 2014 will require the use of advanced authentication using unique challenge-response grid cards.

b. Users are responsible for ensuring the security of their grid cards; because they are part of the authentication process, they must be afforded the same due care as a password:

- Grid cards must be stored in an appropriate manner so as to prevent theft or loss of confidentiality.

- Grid cards are not to be shared with any other user. Gaining remote access through the use of another's grid card is strictly prohibited.

c. Proper storage of grid cards

i. Unique grid cards are issued during the remote access enrollment process as a password-protected (encrypted) PDF file. This file may be stored on any device directly within the user's control, including the device used for remote access; however, the PDF file and its password must never be stored together.

- Examples of approved storage locations might include the user's laptop computer, an agency-issued smartphone, a user's personal smartphone, etc.

- The PDF file and its password should be treated like a bank card and its PIN.

ii. Users are permitted to print a physical copy of their grid card if they so wish. This physical copy must be stored on or about the user's person such that it remains in their physical control at all times. It must never be stored with the device used for remote access (e.g., taped to the lid of a laptop computer or stored in a laptop bag).

- Examples of approved storage locations might include a wallet or handbag, or securely affixed to the reverse of a security badge.

iii. Users are permitted to create an [unencrypted] image of their grid card (i.e., using a smartphone's camera or screen capture). This image may be stored on any device directly within the user's control, excluding the device used for remote access.

- If a personal device is used to store the unencrypted image, the device must be enabled with a passcode to prevent unauthorized access.

d. Grid cards are valid for 1 year from the date of issue, and must be renewed annually.

e. Grid cards that are lost or compromised must be deactivated immediately to prevent unauthorized use. Users must report loss or compromise by contacting either the ISM or the CSC (850-410-8412 or 1-800-292-3242) immediately.

E. Information Technology Services Members

1. ITS members will be granted elevated access privileges to FDLE information systems only when such access is required for assigned duties (based on the principles of "Need to Know" and "Least Privilege").

2. Information security activities such as monitoring, sniffing, and related security activities will be performed only by members who are given explicit consent based on their job duties and responsibilities.

3. Maintenance or repair of information technology equipment will be carried out only by members whose position descriptions authorize such activities or with the authorization of the CIO.

4. Members will not procure outside maintenance or repair services for information technology equipment (e.g., data recovery services for failed storage devices, damaged mobile devices, etc.) without the authorization of the CIO. This applies to both on-site and off-site services.

F. Physical Access Protection

1. FDLE information systems and technology resources will be protected by physical access controls that are appropriate to the size and criticality of the system/resource.

2. Physical access to the FDLE data center, wiring/telecom closets, and other locations housing information technology infrastructure will be restricted to authorized personnel. Access to the data center is granted by the CIO or designee. The list of individuals with access to the data center will be reviewed and updated each year as determined by the CIO or designee. All visitors to the data center must log in at the FDLE Headquarters entrance and again at the entrance to the data center.

3. FDLE will document security controls required to protect information technology resources and infrastructure.

INFORMATION TECHNOLOGY RESOURCE STANDARDS

A. The CIO is responsible for standards for the acquisition, installation, security, maintenance, support, use, and disposal of all information technology resources. These standards are based on federal and state law and rules.

1. ITS will dispose of all media (associated with obsolete software or data) in a manner consistent with the applicable license and federal and state law and rules on the retention and destruction of IT assets.

2. Physical information media (such as hard drives, tapes, CDs, DVD, disks, optical platters, etc.) containing information will be destroyed on-site by a FDLE member or third-party vendor. Destruction by a third-party vendor must be witnessed by the Property Custodian who will maintain documents from the vendor attesting to the destruction of the physical media.

B. Prior to information publication on FDLE's Web Sites (Internet, Intranet, or CJNet), the content must be approved by a designee from the relevant division and by the FDLE Webmaster for formatting and layout consideration.

C. Regional Systems Administrators will work in concert with Customer Service Administration at FDLE Headquarters to coordinate the daily administration, maintenance, and support of regional information technology resources in accordance with standards established by the CIO and state and federal licensing and usage laws.

D. Special Agents in Charge are responsible for ensuring compliance with all state and federal laws and with FDLE information technology resource standards within their regions.

E. The CIO will provide daily administration, maintenance, and support of FDLE information technology resources.

SOFTWARE MANAGEMENT AND ACCOUNTABILITY

A. FDLE will establish central control over the review, acquisition, installation, use and disposal of computer software. [CALEA 11.4.4] ITS will administer the FDLE's software management procedures.

B. FDLE will establish procedures for maintaining records of all purchased software and conduct periodic inventories of software.

C. ITS will maintain a list of standard software products that are authorized for FDLE's computers on FDLE's corporate intranet web site. [CALEA 11.4.4]

D. Software Procurement

1. All planned purchases of software must be reviewed by the CIO or designee. Members planning to purchase software must complete an Information Resource Request (IRR) form and submit this form to the CIO for review. The IRR Form is included in the Related References of this policy and is available on FDLE's corporate intranet web site.

2. FDLE purchasing authorities will issue purchasing card orders, purchase orders, or contracts for IT products or services only after receiving an approved IRR form signed by the CIO.

3. ITS will maintain records of software purchases until they are obsolete, superseded, or administrative value are lost.

4. Any additional software requested by a member, including freeware, trial applications, and any other software acquired by any member, must be approved for

installation by the member's supervisor (in writing) and approved by the CIO or designee.

E. Software Installation, Transfer or Removal

1. All software must be installed, transferred, or removed only by members granted specific authority by the CIO. If a member wishes to have a software product installed, transferred, or removed, he/she must submit a request to the CSC. The request will be referred to an authorized installer for completion.

2. If not specifically authorized above, any Member wishing to install, transfer, or remove software must have his/her supervisor submit a request to the CSC with detailed information about the member, the software to be installed, the computer on which it will be installed, and the reason for the installation exemption request.

F. It is the policy of FDLE to respect all computer software copyrights and to adhere to the terms of all software licenses to which FDLE is a party. Members will not install or duplicate any licensed software or related documentation for use either on FDLE premises or elsewhere unless FDLE is expressly authorized to do so by agreement with the licenser. Unauthorized installation or duplication of software may subject members and/or FDLE to both civil and criminal penalties under the United States Copyright Act. [CALEA 11.4.4]

1. Questions regarding software license agreements must be referred to the Office of the General Counsel (OGC) for resolution.

2. Any public request to inspect or copy software will be treated as a public records request and referred to the OGC for resolution.

3. Members may not give software to any clients, contractors, and others unless expressly authorized to do so by agreement with the licenser and the CIO.

4. Members may use software on local area networks or on multiple machines only in accordance with applicable license agreements. [CALEA 11.4.4]

IDENTITY AND PASSWORD MANAGEMENT

Under Chapter 71A-1, the State of Florida Information Technology Resource Security Policies and Standards and the FBI CJIS Security Policy, Version 5.2, FDLE defines the criteria for selecting and using user-IDs and passwords and the requirement for annually inspecting systems and applications to ensure compliance.

A. Identity and User Account Management - Identity management addresses the requirements for user accounts on FDLE computing resources. Each member is assigned a unique user-ID, this allows all activities to be traced to an accountable individual.

B. Passwords - Password management addresses the requirements for choice and use of passwords on FDLE computing resources.

1. User authentication will be requested during login to a FDLE computer resource.

2. ITS will ensure that vendor-supplied default passwords are changed before equipment is put into production. A System Administrator will enter the initial user password. Immediately thereafter, the member/user must change all passwords.

3. A password must be individually owned rather than owned in common by a group of individuals in order to provide individual accountability within a computer system.

4. Passwords must be re-set every 60 days and an electronic history will be maintained by the system to prevent the reuse of any of the previous 10 passwords.

5. Where technology permits, members must use a complex password that does not contain all or part of the member's network user-id or the member's full name.

6. Passwords must:

    a. Be at least EIGHT characters in length

    b. Contain characters from three of the following four categories:

        - English uppercase characters (A through Z)
        - English lowercase characters (a through z)
        - Base 10 digits (0 through 9)
        - Non-alphanumeric characters (!, $, #, %, etc...)

7. Mobile communication devices (i.e., smartphones) must be protected by a password consisting of five characters (alpha or numeric). These devices will also be equipped with a departmental screensaver with a 15 minute timeout period.

8. In the event a member is unable to access the FDLE network with his/her password, notify the CSC. Upon verification of the member's identity, the CSC will unlock the member's account and instruct the member to change his/her password upon successful access to the network.

9. In the event a member is unable to access an authorized application with his/her password, the member must notify the AAA of that system. Upon verification of user identification, the AAA will unlock the member's account and instruct the member to change his/her password upon successful access to the system.

10. ITS will conduct annual reviews to ensure that the applications, systems, and networks are configured to promote compliance with this password policy. The audit will be performed by inspecting the application, system, and network components that validate and process passwords. The OIG will perform periodic audits to ensure that ITS is meeting these requirements. [CALEA 82.1.6]

11. Service accounts may be exempted from password aging requirements provided they are never used for interactive sessions.

APPLICATION DEVELOPMENT STANDARDS

FDLE will adhere to the approved Information Systems Development Methodology (ISDM) for all development projects. The ISDM is available on the ITS Intranet web site.

A. It is the responsibility of the project manager to:

1. Ensure that project documentation is prepared during each appropriate phase;
2. Maintain all project-related documentation;
3. Provide verification that the project team adhered to this procedure. If any part of the ISDM is not followed for a specific project, the project manager will provide appropriate rationale for eliminating this part of the ISDM;
4. Ensure that security requirements are addressed during each phase of the development lifecycle;
5. Ensure that Service Level Agreements (SLA) for non-agency-provided technology services ensure appropriate security controls are established and maintained.

B. Periodically, ITS will review the ISDM to ensure it continues to meet the needs of FDLE.

C. Where possible, FDLE will ensure that software applications purchased, leased, or developed will be based on secure coding guidelines as identified in Chapter 71A-1, F.A.C. (e.g., OWASP, CERT).

D. Application developers will incorporate validation checks into applications to detect data corruption that may occur through processing errors or deliberate actions.

E. Development and/or test infrastructures will be physically or logically separated from the production infrastructure.

F. Confidential or exempt information will not be used as test data unless authorized by the information owner; security controls are in place on the test system to provide for restricted access; and data is removed entirely from the system when testing is complete.

SECURITY OF FDLE SYSTEMS

A. It is the responsibility of application owners and ITS to define the security requirements for an information system.

B. Applications or systems with a FIPS 199 categorization of moderate or higher will require a documented system security plan. These plans will be developed upon major revision to any existing system or the implementation of any new system.

C. The Information Owner and ITS are responsible for ensuring that they develop, document, and formally approve these system security plans.

D. System security plans must be marked, handled, and controlled as part of the overall FDLE Information Security Plan and are confidential and exempt from public records by section 282.318, F.S.

E. It is the responsibility of the Information Owner and ITS to ensure that systems are thoroughly tested prior to placing them in the FDLE production operating environment.

F. System patches and security updates must be applied in a timely fashion in accordance with FDLE patch management guidelines.

G. Unnecessary services will be disabled (e.g., if a mail server does not need to allow File Transfer Protocol [FTP], then FTP should be disabled).

H. Auditing and logging will be enabled on the server to provide information on access to, and alteration of, information systems and data.

I. Antivirus software will be installed, maintained, and configured on all servers and workstations.

J. Vendor default passwords will be changed prior to deployment or implementation (CJIS Security Policy, Version 5.2).

K. Any changes made to the configuration of the server will be performed in accordance with ITS Procedure 5.100 – Configuration Change Control Board.

L. An application security review must be approved by the application owner, ISM, and CIO or designee before a new application or technology is placed into production or before application or technology modifications are placed in production.

SECURITY OF MOBILE COMPUTING DEVICES [CALEA 11.4.4]

A. FDLE-provided mobile communications devices are issued to FDLE-authorized users for official (FDLE business) use only.

B. FDLE is responsible for enforcing a policy that meets the requirements of Chapter 71A-1, F.A.C., Florida Information Technology Resource Security Policies and Standards, and the CJIS Security Policy, Version 5.2.

1. FDLE owned mobile computing devices will be tracked by the FDLE.

2. FDLE owned mobile devices will be configured and maintained according to FDLE standards.

3. Only FDLE-owned or FDLE-managed mobile storage devices may store agency data.

4. Only FDLE-approved software purchased according to the IRR process will be installed on FDLE-owned mobile computing devices.

5. Members must not manipulate, alter, or delete current software running on FDLE-owned mobile devices.

6. Users may remotely connect mobile computing devices directly to the FDLE network only through FDLE approved and secured remote access methods.

7. Security and privacy policies applicable in the FDLE corporate network apply when using or connecting to FDLE information technology resources from outside the FDLE facilities.

8. Mobile computing devices require user authentication. Device users are responsible for password authentication when using mobile devices. Mobile communication devices (i.e., smartphones) must be protected by a password consisting of 5 characters (alpha or numeric).

9. Wireless access to FDLE's internal networks will require user authentication.

10. Information Users must obtain approval from the CIO before using or deploying any wireless technology to access the FDLE network. This rule applies regardless of whether these devices are owned by FDLE.

11. Mobile computing devices will be secured with a password-protected screensaver with the automatic activation feature set at no more than 15 minutes.

12. Mobile computing devices connecting to the FDLE network must use current and up-to-date anti-virus and anti-malware software, where technology permits.

13. Mobile device users must activate an FDLE approved personal firewall, where technology permits, when connecting state-owned computing devices to the Internet.

14. Members must take reasonable precautions to protect mobile computing devices in his/her possession from loss, theft, tampering, unauthorized access, and damage.

15. To prevent unauthorized users from accessing sensitive FDLE information via open ports, remote access sessions and open terminal windows must never be left unattended. Users must log out rather than terminate a remote session when finished. Users must wait for confirmation of log-out command from the remotely connected FDLE machine before leaving the computer.

16. Members must not make unauthorized changes to FDLE computer resources, including installation of unapproved software/hardware or interference with security measures (e.g., audit trail logs and antivirus software). Members must report theft of mobile devices immediately to the user's supervisor. In addition, the Regional Systems Administrator and CSC should be notified so services to that device can be turned off, if necessary. Supervisors are to notify the agency ISM.

17. To prevent loss of data, the mobile device user is responsible for ensuring FDLE data stored on mobile computing devices is backed up. Where technology exists, the agency will back up user data. Where the technology does not exist, the users are responsible for backing up their own data.

18. Mobile computing devices used with information that is exempt from public disclosure as defined in Section 119.071, F.S. (General exemptions from inspection or copying of public records) require encryption, unless specifically exempted by the FDLE CIO. Encryption technology must satisfy the requirements of the FBI CJIS Security Policy, Version 5.2.

19. Electronic transmission of information that is exempt from public disclosure as defined in Section 119.071, F.S. (General exemptions from inspection or copying of public records) must be encrypted when transmitted from a mobile device and the transport medium is the Internet, or the transport medium is not owned or managed by FDLE.

20. Mobile storage devices with confidential FDLE data must have encryption technology enabled such that all content resides encrypted. This requirement includes USB devices.

C. FDLE considers communications via email and SMS (text messaging) to be subject to the applicable public records laws and may therefore be subject to disclosure under the state's Sunshine Laws.

CONTIGENCY PLANNING AND DISASTER RECOVERY

A. Data and software essential to the continued operation of critical FDLE functions will be mirrored to an off-site location or backed up regularly to an off-site location

B. To prevent loss of data, FDLE will establish a procedure to ensure that data, including unique copies of agency data on workstations and mobile devices, is backed up regularly. Members possessing stand-alone data files (not on shared directories) must back up these files on a regular basis.

C. FDLE will establish security controls over backup resources that are appropriate to the criticality, confidentiality, and cost of the primary resource.

D. FDLE will maintain disaster recovery plans for information systems identified as critical to continuity of operations in the event of a disaster. Such plans will be tested at least annually.