CF OPERATING PROCEDURE
NO. 50-2

STATE OF FLORIDA
DEPARTMENT OF CHILDREN AND FAMILIES
TALLAHASSEE, May 17, 2024

Systems Management

SECURITY OF DATA AND INFORMATION TECHNOLOGY RESOURCES

This operating procedure outlines the processes for department employees (including other personnel services [OPS] employees), community-based providers connecting to the department's network, and contractors and subcontractors to follow to ensure the security of departmental data and other information resources and the measures to follow in the reporting of a security event. This operating procedure will be reviewed as deemed appropriate, but no less frequently than every 365 days. The review will be performed by the department's Information Security Manager.

BY DIRECTION OF THE SECRETARY:

(*Signed copy on file*)

COLE SOUSA
Chief Information Officer

SUMMARY OF REVISED, DELETED, OR ADDED MATERIAL

Updated Chapter 2, sections 2-3(c) and added 2-3(c) Exception Encryption using Transfer Layer Security (TLS) protocols.

This operating procedure supersedes CFOP 50-2, dated April 22, 2024.
OPR: ITS

TABLE OF CONTENTS

Chapter 1 - GENERAL

1-1. Purpose. This operating procedure defines the processes to be used to protect the confidentiality, integrity, availability, and reliability of information technology resources used to support the needs of our clients and the missions of the Department, and to implement and enforce the level of security which will provide for the protection of data and information technology resources from accidental or intentional unauthorized disclosure, modification, or destruction by persons within or outside of the Department. Federal and State laws, rules, regulations, policies, and procedures governing the confidentiality of data are not superseded, abridged, or amended by this operating procedure.

1-2. Scope. This operating procedure applies to anyone who has access to information and data through the use of Department-owned information technology resources including all information technology resources used to support or implement the mission of this Department and any other automated data processing systems in our custody whether owned, purchased, contracted from or to, or leased by the Department. This operating procedure also applies to any information technology resources connecting to the Department's network whether used in offices, in the field, or at telecommuting sites.

1-3. Authority.

a. Section 282.318, Florida Statutes, *State Cybersecurity Act*.

b. Section 501.171, F.S., *Security of Confidential Personal Information*.

c. Rule Chapter 60GG-2, Florida Administrative Code (F.A.C.), *Florida Cybersecurity Standards.*

d. ARRA Title XIII Section 13402, "Notification in the Case of Breach."

e. 45 CFR Parts 160 and 164, Subparts A and C, Health Information Portability and Accountability Act (HIPAA) Privacy and Security Rules.

f. The Centers for Medicare & Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E) 2.2 Requirements.

g. 5 U.S.C. 552a, *Privacy Act of 1974 - Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration* (SSA*)*.

h. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 r5, "*Security and Privacy Controls for Information Systems and Organizations*."

i. Internal Revenue Services (IRS), Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, (11-2021).

j. Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, (02-2004).

1-4. Definitions. Terms used in this operating procedure are defined below:

a. Confidential Information. Information that is exempted from disclosure requirements under the provisions of applicable state and federal law, e.g., the Florida Public Records Act, s.119.07 F.S.

b. Data. A collection of facts; numeric, alphabetic and special characters which are processed or produced by an information technology resource.

c. Data Processing Systems. Any process that includes the use of a computer program to enter data, record data, sort data, calculate data, summarize data, disseminate data, analyze data or otherwise convert data into useful information.

d. Department. The State of Florida's Department of Children and Families.

e. Employee. Any person employed by the Department in an established position in the Senior Management Service, Selected Exempt Service, Career Service, or paid from Other Personal Services (OPS) funds. Also, for the purposes of this operating procedure, the definition of employee includes any non-OPS temporary staff hired by the Department who have access to Department IT resources, including contracted staff and contracted vendor staff.

f. Event. An event is an observed change to the everyday operations of a network, system, environment, process, workflow or a person indicating that a security procedure may have been violated or a security control may have failed.

g. Incident. An event or unintentional action that is escalated to incident status as it results in compromised data confidentiality, a danger to the physical safety of technology resources or personnel, misuse of Department information technology resources, and/or electronic denial of technology resource services.

h. Information Security Manager. The Information Security Manager (ISM) is the person designated by the Secretary of the Department to administer the Department's information technology security program and serve as the process owner for all ongoing activities that serve to provide appropriate access to and protect the confidentiality and integrity of information in compliance with Department and statewide policies and standards and in accordance with §282.318, Florida Statutes, and Chapter 60GG-2, F.A.C.

i. Information Technology Resources. Data processing hardware (including desktop computers, laptops, tablets, smartphones and associated devices), software and services, supplies, personnel, facility resources, maintenance, training, or other related resources.

j. Mobile Devices. Devices such as laptops, smart phones, tablets, thumb drives, CDs, DVDs, external hard drives, or flash cards designed to be portable and capable of storing large quantities of data.

k. Office of Information Technology Services (OITS). Department of Children and Families Office of Information Technology Services.

l. Principle of Least Privilege. The requirement that each business system process, a user, or program must be able to access only the information and resources that are necessary for its business legitimate purpose.

m. Protected Health Information (PHI). Individually identifiable health information that is created by or received by the Department, including demographic information that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

(1) Past, present or future physical or mental health or condition of an individual;

(2) The provision of health care to an individual; or,

(3) The past, present, or future payment for the provision of health care to an individual.

n. System Owner(s). The entity that owns the data and that has the primary responsibility for decisions relating to a particular data processing system's specifications and usage.

o. System Users. Any person who, through State employment, contractual arrangement, charitable service or any other service arrangement, and with appropriate approvals, would have access to DCF facilities, the Department's information technology resources, or the Department's data for the purpose of conducting business or providing services.

p. United States of America. Primarily located in North America and consists of 50 states, including the District of Columbia and Puerto Rico. This term excludes the listed unincorporated territories (American Samoa, Guam, the Northern Mariana Islands, and the U.S. Virgin Islands).

1-5. Policy Statement. Department information technology resources shall not be used for any activity which adversely affects the confidentiality, integrity, or availability of information technology resources. Employees shall be held responsible for information security, especially involving the access, transport or storing of confidential information. Violations of information security may be cause for disciplinary action, up to and including dismissal as well as civil or criminal penalties.

Chapter 2 - SECURITY OF DATA AND INFORMATION TECHNOLOGY RESOURCES

2-1. System Security and Access to Data.

a. Onboarding Process.

(1) Prior to using the Department's information technology resources, system users will sign form CF 114, "Security Agreement Form" (available in DCF Forms), to acknowledge receipt of and confirm agreement to abide by the minimum DCF security requirements specified therein.

(2) The Department employee's supervisors should sign and forward the original copy of CF 114 to the Office of Human Resources for placement in the employee's personnel folder. Employees will retain a duplicate copy of CF 114 and attachments. In addition, DCF employees must sign form CF 114 within ten days of employment and annually there that to acknowledge receipt of and confirm agreement to abide by 'the minimum DCF security requirements specified therein.

(3) After system users and their supervisor have signed form CF 114, complete the necessary information on the digital Access Authorization Request (AAR) Form 138 and attach the appropriate documents before clicking the 'Submit' button to generate an IT Statewide Help Desk request for assignment of a unique personal identifier (User ID and Password) to each person who uses information technology resources to access the Department data processing systems and Department data by means of information technology resources owned, purchased, or leased by the Department. It is the policy of this Department that system users shall complete Security Awareness Training within 24 hours of being assigned a personal identifier and within the first 10 days of employment by the Department. The Identity Access Management (IAM) and ACCESS IT staff are responsible for provisioning accounts for the agency.

b. Deboarding (Separation) Process. Upon receipt of written or verbal notification of a system user's resignation or separation from the Department, supervisors and managers are responsible for notifying:

(1) OITS Identity and Access Management. At a minimum, by the system user's last day of work, the supervisor/manager (or designee) should take necessary actions to retrieve Department IT resources (e.g., workstations, phones, keyfobs, ID Badges) and remove barriers that prohibit account deactivation. Complete and submit an AAR-138 Form by selecting 'Separation,' completing the appropriate fields, and listing all system/data accounts that require deactivation, including any Administrative Accounts.

(a) The submission of the digital (online) AAR-138 form automatically creates a DCF IT Statewide Help Desk ticket, which notifies the appropriate OITS staff (IAM).

(b) OITS staff shall take action to update (**inactivate**) the system user's access accounts (De-provisioning Request) within three (3) days (non-business days excluded) of receipt.

(c) A description of the access removal process in the ticketing system should include the name of each IT resource deactivated, including the date and time of the access removal.

(d) If OITS staff **cannot** deactivate the system user's account access, the IT ticket should be documented with the name of the IT resource.

NOTE: When necessary, the supervisor/manager may contact the DCF Statewide Help Desk directly to request emergency removal of access, for example, if the system user fails to return Department-issued property (e.g., workstation, smartphone) by their last day of work or involuntary separation (e.g., violation of Department policy), then submit an AAR Form 138.

(2) Human Resources. Coordinate with Human Resources to ensure the timely submission of the employee's separation package to the Human Resources Shared Services Center (HRSSC) for review and processing, per CFOP 60-70, Chapter 1.

c. Position/Job Description Changes. Within five days of a DCF employee changing from one position description to another at the Department, the employee's supervisor shall evaluate the system user's access to IT resources and take appropriate action to remove IT resources no longer required by that employee to perform their new job duties by completing an AAR Form 138. Supervisors and managers should contact the OITS Identity and Access Management (IAM) Team with any questions about the removal of access process for IT resources that are no longer required.

d. Unique Identifier(s). The identifier(s) will permit access to the data that the person has a need and right to know and will control inquiry and update capabilities. The system owner will determine and authorize system access according to the principle of least privilege, with no access given that is not absolutely necessary for business needs.

e. Rules of Behavior.

(1) It is the responsibility of the employee to secure and protect his/her personal identifier and any other authentication methods used to access Department resources. Employees shall not disclose their Department accounts, passwords, personal identification numbers, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes.

(2). System users will be held responsible for events that occur using their personal identifier. Employees are required to lock their workstations prior to leaving their work area and save work to reduce the risk of losing work. Department-owned workstations will receive scheduled patches and updates when applicable; refer to Chapter 5, Patching and Rebooting of Information Technology Resources.

(3). The use of service accounts for interactive sessions is prohibited at DCF. Any legacy DCF systems using this methodology must have mitigating controls in place.

(4). The use of vendor-supplied default passwords is prohibited at DCF.

(5). User accounts shall be authenticated at a minimum by a complex password on all systems that support complex password enforcement, refer to 2-1(g). User accounts shall have inactivity timeouts in place that terminate sessions on all systems that support session timeouts.

(6). Users must not store their passwords in clear text, nor are they allowed to automate pre-filling of passwords on any DCF computing device.

(7). System users shall not share their personal identifier, Department account information, remote access account information, passwords, personal identification numbers, security tokens, smart cards, identification badges, or any other devices used for identification and

authentication purposes. Information sharing should be handled through administrative methods rather than sharing passwords. Administrative methods include:

(a) Establishing individual email rules and alias assignments to permit sharing of electronic mail.

(b) Obtaining access rights to special directories (network folders) to share files with one or more people.

(c) Using mainframe security features to give supervisors appropriate access rights to their employees' cases and files, if required.

(8). System users will immediately report lost security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes to their supervisor who is then responsible for reporting instances of loss to the Regional Security Officer / Administrator or the ISM.

(9). Employees shall lock their workstations (CTRL/ALT/DELETE) before leaving their work area and appropriately save work to reduce the risk of losing work. Department-owned workstation shall receive weekly scheduled patches and updates when applicable, refer to Chapter 5, Patching and Reboot policy.

(10). To prevent loss of data, system users shall ensure unique copies of Department data stored on workstations or mobile devices are backed up to network shares and ensure that all mobile devices are appropriately encrypted. Employees should contact the IT Statewide Help Desk with questions about encryption and backup options.

f. USB Encryption Exception. The DCF ISM shall permit a USB encryption exception for Department staff on a case-by-case basis. Before deactivating encryption protocols, the immediate supervisor (or designee) of the employee must submit an encryption exception request via the IT Statewide Help Desk ticketing system. The request must be reviewed and approved by the DCF ISM before any action is taken.

g. Network/Business System Settings.

(1) Systems will automatically disable user IDs that have not been used for a period of 30-60, days, depending on risk level. Business systems must force users to change their passwords every 30-90 days. Network system users must change passwords every 90 and configuration settings support password requirement. Network systems shall enforce a minimum password age restriction of one day, when applicable. Business systems shall enforce minimum password age restrictions based on applicable standards, best practices, and system capabilities.

(2). Network-level passwords shall adhere to complexity standards per Rule 60GG-2, federal requirements, and best practices. Business-level passwords shall adhere to complexity standards when system functionality permits.

(3) The Department shall secure workstations with a network-level password-protected screensaver with the automatic activation feature set at no more than 15 minutes. Workstations used to access protected health information shall be placed in secure areas away from access by the public and display screens positioned to minimize unauthorized viewing and/or access.

2-2. DCF Security Awareness Policy.

a. The purpose of cyber-security awareness training at DCF is to provide, at a minimum, all employees with annual and on-going security awareness education and so as to reinforce DCF security practices and ensure employees perform their information security-related duties and responsibilities in a manner consistent with Department policies and procedures.

b. The scope of this fundamental cyber-security awareness training includes all DCF employees and DCF third-party stakeholders and business partners.

c. The Department's hiring procedures and processes and annual employee training procedures and processes conducted by DCF Human Resources have incorporated security awareness into their course offerings. These procedures and processes include annual course content review and revision and making the training available to DCF employees on the Department Intranet via an approved training management system (TMS). DCF Human Resources also coordinates the annual and on-going security awareness training, notifying employees as to when the training period begins and ends, tracking employee response and compliance, and working with DCF supervisors and managers to ensure full compliance.

d. The Department's Information Security Manager, in support of DCF Human Resources, is responsible for maintaining a statewide Security Awareness Training program that will ensure employees are aware of the importance of information security. At a minimum, this program must provide upon-hire and annual refresher security awareness training to all system users and monthly informational training via newsletter or the DCF Intranet.

e. All system users will be required to complete Security Awareness training within ten (10) days of hire and then annually thereafter as a refresher. The Department approved training management system used to track employee participation and compliance. DCF supervisors and managers are required to assist DCF Human Resources in ensuring their employees complete the required training within the specified time frame.

f. All DCF employees must complete Security Awareness Training before accessing Department production applications. Supervisors and security administrators are responsible for ensuring that employees receive any additional applicable program office security training and receive appropriate access according to the principle of least privilege.

g. Community Based Care agencies, vendors, providers and other DCF business partners are responsible for ensuring their employees complete this mandatory training (see DCF Standard Contract, paragraph 5.5) and are responsible for tracking compliance and documenting an audit trail.

2-3. Systems and Communications Protection for Confidential Data.

a. All media containing confidential data or Federal Tax Information (FTI) data must be encrypted during transmission of the data. This includes all types of thumb drives and other portable media.

b. The Department has established security controls that restrict access to FTI data areas. Individuals who enter FTI data areas must not bypass access controls or allow unauthorized entry of other individuals. DCF employees must report unauthorized attempts to security personnel.

c. If the business need requires the transfer of Social Security Numbers (SSNs), only then shall SSNs be copied from the system. When transferring files containing SSNs, they shall be encrypted to prevent unauthorized disclosure by typing **encrypt** as the first word in the email 'Subject' line. The Department shall monitor all SSNs that are removed from the system by logging such actions, including the name of the user and data details. The Department shall implement tools to monitor and log or encrypt such actions.

d. Transport Layer Security (TLS) Encryption. If standard encryption methods encounter challenges, the Department shall employ a forced Transport Layer Security (TLS) protocol. To prohibit unauthorized disclosure during communication with external partners. TLS acts as an additional layer of security, safeguarding sensitive and confidential information while in transit.

2-4. Destruction Methods for Confidential and Federal Tax Information (FTI) Data. Confidential or FTI data that is on paper must be destroyed by burning, mulching, pulping, shredding or disintegrating. If shredding is used, the paper must be shredded to effect 5/16 inch wide or smaller strips. Microfiche and microfilm must be shredded to effect a 1/35 inch by 3/8 inch strips. If shredding is a part of the overall destruction process, strips can be ½ inch; however, the strips must be safeguarded until it reaches the stage where it is unreadable. All shredding or destruction of paper and magnetic media must be witnessed by a DCF employee.

2-5. Prohibit System and Data Access Outside the United States of America (USA) and Canada (Geolocking). All Department system users shall only access Departmental IT systems and data from within the United States of America (USA) and Canada. The Department shall implement geographical locking (geolocking) technology that restricts access to Department system and data based upon the user's location. The geolocking scheme identifies the user's location using Internet geolocation techniques, such as but not limited to checking the user's IP address and measuring the end-to-end delay of a network connection to estimate the physical location of the user. Access is approved or denied based on the result of this check. Failure to adhere to the system and data accessing policy constitutes a security violation and may result in disciplinary action.

Chapter 3 – EVENT AND INCIDENT REPORTING

3-1. Purpose. This chapter defines the processes to be used by employees in the event of a security event or incident. Federal and State laws, rules, regulations, policies, and procedures governing the confidentiality of data are not superseded, abridged, or amended by this operating procedure.

3-2. Security Event and Incident Reporting and Tracking.

a. System Owners. System owners are responsible for ensuring that their business application system and the data contained therein have documented security guidelines and rules included in a user guide or application manual, and that all users of their system(s) have access to this documentation. The user guide must document what is expected of the user, what constitutes security violations, and how the supervisor will handle suspected or known violations.

b. System Users/Employees. DCF employees who know or suspect that a security event, incident, or policy violation has occurred are responsible for informing their supervisor, the Regional Security Officer/Administrator, the DCF Information Security Manager or the IT Statewide Help Desk immediately. Failure by employees to report may result in disciplinary action up to and including dismissal, as well as possible legal action.

c. Supervisors/Managers. Supervisors are required to notify their manager who is to evaluate the report and confer with their Regional Security Officer/Administrator, the DCF Information Security Manager, the IT Statewide Help Desk or the DCF Office of Inspector General (OIG) and determine which to immediately notify of any suspected or known security events, incidents, or violations. Managers may also report events and incidents directly to the DCF ISM, who will then take responsibility for routing the report to the correct DCF office(s). Supervisors and managers will cooperate and coordinate to immediately ensure information technology resource integrity in securing DCF business systems, including placing any affected and applicable equipment in a secure and locked location. Failure of the supervisor or manager to notify and cooperate with the above named personnel may result in disciplinary actions up to and including dismissal. Information Technology Services personnel will follow Inspector General guidance to ensure appropriate Chain of Custody compliance. The DCF OIG will be notified at intake email address IG.Complaints@myflfamilies.com.

d. Regional Security Officers/Administrators and Information Technology Services Management. Regional Security Officers/Administrators and Information Technology Services management staff are responsible for evaluating and then reporting any security events, incidents, or violations to the DCF Information Security Manager and/or the IT Statewide Help Desk. The Regional Security Officer/Administrator is responsible for tracking and resolving or disposing of all incidents reported to or referred by the IT Statewide Help Desk for their area. The Regional Security Officer/Administrator is responsible for maintaining a log or record of all reported security events, incidents, or violations and using this information to determine actions steps that could deter or mitigate the impact from future incidents of a similar nature. The log or record should also contain a disposition for the incident and an estimate of how much damage/cost was incurred, if any. The Regional Security Officer/Administrator shall provide disposition information to the IT Statewide Help Desk so that any associated event or incident ticket can be closed. Incident log or record data collection requirements include:

(1) Date event or incident reported;

(2) Date event or incident occurred;

(3) Reported by;

(4) Contact email;

(5) Contact phone;

(6) Reported to, contact information, and how contacted; and,

(7) Event or incident description and details. This description should include the approximate number of records impacted, the data classification, and descriptions of persons affected by the event or incident.

e. IT Statewide Help Desk. The DCF IT Statewide Help Desk is responsible for consolidating the reported events and incidents. The IT Statewide Help Desk is also responsible for contacting or notifying the DCF Information Security Manager (ISM) when a report or disposition is received.

f. Special Requirements for Florida Statute 501.171, "Security of Confidential Personal Information." Florida Statute 501.171 addresses the confidentiality of personal information and defines the terms "breach of security" and "breach." Covered entities, including the Department, should identify when unauthorized access of electronic data containing personal information occurs. If such an event has occurred and affects 500 or more individuals in the state, section 501.171(3)(a), F.S., requires DCF management to report the breach to the Department of Legal Affairs (DLA). Reporting must be provided as "expeditiously as practicable" but no later than 30 days (section 501.171(3)(a), F.S.) after the determination of the breach or reason to believe a breach occurred.

g. Special Requirements for Internal Revenue Service Notification. The Department must notify the Treasury Inspector General for Tax Administration (TIGTA) and IRS immediately, but no later than 24-hours after identification of a possible issue involving Federal Tax Information (FTI). Any employee or contract employee that suspects a possible improper inspection or disclosure of FTI must report the event to their supervisor immediately. Supervisors and managers are responsible for reporting these events to the Department's Information Security Manager, who is, in turn, responsible for notifying the IRS Office of Safeguards at SafeguardReports@irs.gov and the DCF Office of Inspector General, as per DCF SOP S-4, Computer Security Incident Response Team (CSIRT) Operating Procedures.

If the supervisor is unavailable, employees or contract employees should report suspected possible improper inspection or disclosure of FTI to TIGTA using the contact numbers listed above. Then, follow up using the Department's internal notification process.

h. Special Requirements for Social Security Administration Data. Any employee or contract employee that experiences or suspects a breach or loss of Personally Identifiable Information must report the event to their supervisor immediately. Supervisors and managers are responsible for notifying the Department's Information Security Manager who is in turn responsible for notifying the United States Computer Emergency Readiness Team (www.us.cert.gov), the Social Security Administration's System Security contact named in the CMPPA agreement, and the DCF OIG.

i. Special Requirements for Centers for Medicare and Medicaid Services Data. Any employee or contract employee that experiences or suspects a breach or loss of CMS data must report the event to their supervisor immediately. Supervisors and managers are responsible for notifying the Department's Information Security Manager who is in turn responsible for notifying the CMS IT Service Desk and the DCF OIG.

Chapter 4 – USE OF WIRELESS TECHNOLOGY AND MOBILE DEVICES

4-1. Purpose. This chapter states the Department's policy concerning the use of mobile devices and the minimum security responsibilities regarding the use of mobile wireless technology when accessing Department data.

4-2. Mobile Devices and Wireless Networks. Mobile devices can present a significant risk to information security and data security as, if the appropriate security applications and procedures are not applied, they could present an opportunity for unauthorized access to Department data and IT infrastructure. The Department's minimum security requirements for use of this technology are listed below. Other State or Federal data security standards may be required beyond those listed here.

a. Mobile devices, such as smartphones and tablets, are important tools for the organization and their use is supported to achieve business goals. Employees issued mobile devices by the Department are responsible for ensuring the physical security of the mobile device and the security of any data or information stored on the mobile device.

b. Technical Requirements.

(1) DCF mobile devices must store all user-saved passwords in an encrypted password store.

(2) Mobile devices must be configured with a secure password that complies with DCF password requirements.

(3) With the exception of those mobile devices managed by DCF, devices are not allowed to be connected directly to the myflfamilies-staff DCF network.

(4) All Department provided mobile devices must be encrypted.

(5) Devices must be kept up to date with manufacturer or network provided patches. DCF OITS will regularly provide all appropriate patches to DCF mobile devices.

(6) Mobile devices (except smart phones) for Department employees must be purchased and approved through MyFloridaMarketPlace. The MyFloridaMarketPlace requisition for mobile devices (except smart phone) must include proper justification, have supervisory approval, and require proper encryption configuration. The purchase of smart phones must be done through the appropriate Headquarters or Region staff designated to purchase phones.

c. Only department-owned information technology resources may be used by DCF employees to access DCF applications and data, with the exception of email over the internet. Those who access email from a personal computer must continue to abide by department security policies and procedures. Contractors with DCF may be approved to use contractor-owned resources to access DCF applications and data, provided that these resources meet DCF minimum security policies and procedures and that the requirement to meet these standards is included in the Department contract with these entities. As appropriate, evaluation of the ability to meet these standards may be part of the procurement process. Such evaluations shall include the DCF Information Security Manager.

d. System users must always physically secure Department-assigned mobile devices when not in their possession. A mobile device left in the passenger compartment of a van or sports utility vehicle

must be concealed and the vehicle must be locked. A mobile device left in a passenger vehicle must be secured in the trunk.

e. System users must report any lost or stolen devices immediately to their supervisor, their Regional Security Officer/Administrator and the IT Statewide Help Desk. The Regional Security Officer/Administrator must notify the DCF Information Security Manager and affected employees must file a police report. The DCF Information Security Manager is responsible for notifying the DCF OIG about confirmed incidents of this type via the DCF OIG intake email IG.Complaints@myflfamilies.com. Each report of a lost or stolen device must contain:

(1) Date reported;

(2) Employee making the report (including email address and phone);

(3) Lost or stolen device property custodian name/employee name (include email address and phone);

(4) Region/location of lost or stolen device;

(5) Associated program office;

(6) Make/model of device;

(7) Property tag number;

(8) Device serial number;

(9) How lost/stolen (vehicle, home, office);

(10) Name of law enforcement agency notified;

(11) Police report number (or other unique identifying criteria);

(12) Encryption enforced (Y/N);

(13) Confidential data (Y/N); and,

(14) Recovery efforts and results.

f. Mobile Device User Requirements. The following procedures must be followed:

(1) DCF devices must not be connected to non-DCF devices or PCs.

(2) Data, including confidential data, may not be stored on unencrypted devices. Department employees may only use DCF purchased, encrypted devices on Department-owned information technology resources.

(3) Users must only load data essential to their job duties onto their mobile device(s). Users should not use DCF mobile devices for document archival and should make sure all appropriate work records are backed up to the DCF network.

(4) Modifying the Department device operating system (e.g., “jailbreaking” or “rooting” devices, etc.), or having any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user, is prohibited.

(5) Users must not load pirated software or illegal content onto their devices.

(6) Applications must only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden. If a user is unsure if an application is from an approved source, the user must contact their supervisor and their Regional Security Officer/Administrator.

(7) Users must be cautious about the use of email on their devices. Users must ensure that DCF data is only sent through the Department email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, the user must notify their supervisor and their Regional Security Officer/Administrator immediately.

g. Personal Home Wireless Network. When connecting Department-owned information technology resources to a home wireless network, compliance with the following criteria is required to ensure wireless network security. Employees should contact their Regional Security Officer /Administrator with any questions about these criteria.

(1) Change Default Administrator Passwords (and Usernames) on the personal access point or router.

(2) Turn on and configure wireless encryption (WEP or preferably WPA or WPA2). To operate properly, all devices on a personal wireless network must share identical encryption settings; therefore, “lowest common denominator” settings may be required.

(3) Additional wireless security precautions to consider:

(a) Change the default network name (SSID).

(b) Enable MAC address filtering. Each piece of hardware that connects to a home wireless network possesses a unique identifier called the “physical address” or “MAC address.” Many access point and router products offer the owner an option to input the MAC addresses of their home equipment in order to restrict access to the home wireless network to only those devices.

(c) Disable SSID broadcast.

(d) Assign static IP addresses to devices.

(e) Position the router or access point safely near the center of the home and away from windows.

4-3. Access Control Measures.

a. Least Privilege. The Department shall implement access control measures that appropriately limit access to information technology resources to only those individuals authorized to see or use the information based on a legitimate business purpose.

b. Remote Access. DCF has implemented Virtual Private Networks (VPNs) for even greater added security for data transmission. Department employees must use a DCF VPN secure encrypted

tunnel from their mobile device to the Department's network. All DCF employees must utilized DCF approved technology when remotely accessing the network either through VPN or other means.

Chapter 5 - PATCHING AND REBOOT OF INFORMATION TECHNOLOGY RESOURCES

5-1. Purpose. This chapter states the Department's policy to ensure Department-owned IT resources are proactively management and patched with appropriate security updates.

5-2. Scope. This policy applies to all IT resources which are owned by the Department. It also applies to Department-issued Windows endpoints bound to Active Directory (AD).

5-3. Scheduling and Deployment. Software vendors release security patches on a regular schedule. Applicable patches will be tested and validated by OITS before deployment. Once validated, OITS will schedule and deploy validated patches to end points during off peak hours, every third Sunday. Communication to Department resource users will be done through DCF Statewide Help Desk announcements.

5-4. Installation and Validation. A system reboot is required to successfully install most security patches.

5-5. Exceptions. There are no exceptions to this policy.