STATE OF FLORIDA
DEPARTMENT OF
CHILDREN AND FAMILIES
TALLAHASSEE, May 31, 2013

CF OPERATING PROCEDURE
NO. 50-2

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, contractors and subcontractors to follow to ensure the security of departmental data and other information resources and the measures to follow in the event of a security incident.

BY DIRECTION OF THE SECRETARY:

(Signed original copy on file)

SCOTT STEWART
Assistant Secretary for
Administration

SUMMARY OF REVISED, DELETED, OR ADDED MATERIAL

Added Health Information Portability and Accountability Act and ARRA Section 13402 to paragraph 1-4; added definition of protected health information (PHI); specified placement of workstations used to access PHI; specified controls for media containing confidential information during transmittal and destruction; included special requirements for reporting breaches of Federal Tax Information and breaches of PHI; and added paragraph 2-6 to cover management of hard drives on multi-function devices.

This operating procedure supersedes CFOP 50-2 dated August 31, 2012.
OPR: ITS
DISTRIBUTION: A

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 Federal and State laws, rules, regulations, policies, and procedures governing the confidentiality of data are not superseded, abridged, or amended by this operating procedure.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. Policy Statement. Agency information technology resources shall not be used for any activity which adversely affects the confidentiality, integrity, or availability of information technology resources. (71A-1.019(41), F.A.C.) 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 under chapters 119, 812, 815, 817, 839, or 877, Florida Statutes, or similar Federal laws including provisions for HIPAA and Personal Health Information. (71A-1.019(2), F.A.C.)

1-3. Scope. This operating procedure applies to anyone who has access to 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.

1-4. Authority. Section 282.318, Florida Statutes, "Security of Data and Information Technology Resources," Chapter 815, Florida Statutes, "Florida Computer Crimes Act," Florida Administrative Code, Chapter 71A-1, "Florida Information Resource Security Policies and Standards," ARRA Title XIII Section 13402, "Notification in the Case of Breach," and 45 CFR Parts 160 and 164, "Health Information Portability and Accountability Act (HIPAA) Privacy and Security Rules."

1-5. Definitions. Terms used in this operating procedure are defined below:

a. Confidential and Personally Identifying Information. Information that has specific statutory exemption from the public records laws. Specific requirements for appropriate levels of data security remain under the purview of each agency.

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. Data Sanitization. A method by which a data destruction program overwrites the data on a hard drive or other storage device erasing confidential data, files and records permanently.

e. Department. The State of Florida, Department of Children and Families.

f. Department Information. Any data that goes into or comes out of Department systems.

g. 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.

h. Incident. An event or unintentional action that 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.

i. Information Security Manager. The person designated by the Secretary of the Department to administer the Department's data and information technology resource security program.

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

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

l. Input Sources. The media used to collect and record data that are subsequently transferred to an automated information system.

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

n. Output Products. The media generated as a result of the processing of data by an automated information system.

o. 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.

p. Security Incident. An intentional or unintentional action that results in compromised data confidentiality, a danger to the physical safety of technology resources or personnel, misuse of state technology resources, and/or electronic denial of technology resource services.

q. Security Violation. An intentional or unintentional violation of one or more of the Department's security policies, rules, operating procedures or regulations, or a computer crime as described in Florida Statutes.

r. 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 specification and usage.

s. 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.

Chapter 2

SECURITY OF DATA AND INFORMATION TECHNOLOGY RESOURCES

2-1. Purpose. This operating procedure defines the processes to be used to protect the confidentiality, integrity, availability, and reliability of all information technology resources used to support the needs of our clients and the missions of the department, and to implement and enforce that 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.

2-2. System Security and Access to Data.

a. 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 agreement to abide by the minimum security requirements specified therein. (71A-1.019(3), 71A-1.019(4), F.A.C.)

b. Department employee supervisors will sign and forward the original copy of CF 114 to the Office of Human Resources and the Office of Human Resources will place the original in the employee's personnel folder. Employees will retain a duplicate copy of CF 114 and attachments.

c. After system users have signed form CF 114, a security officer will assign 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. (71A-1.019(11), F.A.C.) System users shall complete IT Security Awareness Training within 24 hours of being assigned a personal identifier.

d. 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.

e. It is the responsibility of the employee to secure and protect his/her personal identifier. (71A-1.019(15), F.A.C.)

f. System users will be held responsible for events that occur using their personal identifier. (71A-1.019(12), F.A.C.)

g. User accounts shall be authenticated at a minimum by a complex password on all systems that support complex password enforcement. (71A-1.019(13), F.A.C.)

h. System users shall not share their personal identifier, agency 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. (71A-1.019(16), 71A-1.019(17), F.A.C.) Information sharing should be handled through administrative methods rather than sharing passwords. Administrative methods include:

(1) Establishing individual e-mail rules and alias assignments to permit sharing of electronic mail.

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

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

i. System users will immediately report lost security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes to their supervisor. (71A-1.019(19), 71A-1.014(13), F.A.C.)

j. Systems will automatically revoke user IDs that have not been used for a period of 60 days. System users must change passwords every 45 days or systems will automatically lock the system user's account. (71A-1.019(14), F.A.C.)

k. System users shall log off or lock their workstations prior to leaving the work area. (71A-1.019(29), F.A.C.)

l. Workstations shall be secured with a password-protected screensaver with the automatic activation feature set at no more than 15 minutes. (71A-1.019(30), F.A.C.) 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.

m. To prevent loss of data, system users shall ensure unique copies of Department data stored on workstations or mobile devices are backed up and ensure that all mobile devices are encrypted. Contact the DCF Service Desk with questions about backup options. (71A-1.019(10), F.A.C.)

2-3. Security Awareness.

a. The Department's Information Security Manager is responsible for maintaining a statewide Security Awareness Training program that will ensure that employees are aware of the importance of information security. This program must provide annual security awareness training to all system users.

b. All system users will be required to complete this training annually. The region and institution IT Managers are responsible for tracking training in their respective regions and institutions.

c. All employees must complete Security Awareness Training before accessing Department production applications. Supervisors and security administrators are responsible for ensuring that employees receive training and appropriate access.

d. CBCs, vendors, providers and other DCF business partners are responsible for completing and tracking this mandatory training (see DCF Standard Contract, paragraph 28).

2-4. Systems and Communications Protection for Confidential Data.

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

b. To ensure compliance with rules pertaining to the disposition of confidential information, employees must ensure data sanitization prior to the disposal, surplus, reuse, or off site repair of any information technology resource. Employees must seek data sanitization support from the DCF Service Desk, their local Information Systems Security Officer or the region/institution IT Manager. Prior to seeking data sanitization support, employees shall backup and remove all documents and confidential information prior to releasing the information technology resource from their possession. Contact the DCF Service Desk with any questions.

c. If the media is being reallocated, care should be taken to ensure that residual data cannot be recovered or accessed by unauthorized users. Overwriting all data tracks a minimum of three times is recommended.

d. Only authorized personnel shall prepare information technology devices that have contained confidential information for disposal, surplus, reuse, or off site repair. Authorized personnel shall document when, how, and what method was used for data sanitization. All surplus PCs and any removed disk drives or other small removable storage devices must have a label applied that indicates the date the authorized personnel performed the data sanitization and the method used for data sanitization.

e. Social Security Numbers (SSN) shall not be copied from the system unless there is a business need that requires the transfer of SSNs. When files containing SSNs are transferred, they shall be encrypted to prevent unauthorized disclosure. The encrypted files shall not be readable from non-Department owned machines. The Department shall monitor all SSNs that are removed from the system. Such actions will be logged with details including the name of the user and the data that was copied. The Department shall implement tools to monitor and log or encrypt such actions.

2-5. 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.

2-6. Multi-Function Devices. DCF shall own the hard drive on all leased multi-function devices. Whenever these devices are surplused or off-lease, General Services shall notify IT staff. The vendor will remove the hard drives on leased equipment and store them in a secure on-site location until IT staff take possession. IT staff shall sanitize the hard drives or destroy them in one of the above mentioned methods.

Chapter 3

INCIDENT REPORTING

3-1. Purpose. This chapter defines the processes to be used by employees in the event of a security 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 Incident Reporting and Tracking.

a. System Owners. System owners are responsible for ensuring that their application and the data contained therein has 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. A system user/employee who knows or suspects that a security incident or violation has occurred is responsible for informing his/her supervisor immediately of the suspected or known incident or violation. Failure by employees to report security incidents may result in disciplinary action up to and including dismissal, as well as possible legal action. (71A-1.019(18), F.A.C.)

c. Supervisors. Supervisors are required to notify their manager, region or institution IT Manager, Information Systems Security Officer, Department Information Security Manager and the Inspector General immediately of any suspected or known security incidents or violations. If necessary and at the direction of the Inspector General, supervisors will coordinate with Information Technology Services personnel to immediately ensure information technology resource(s) integrity by placing the equipment impacted in a locked location. Failure of the supervisor to notify the above named personnel and to coordinate with Information Technology Services personnel to secure the equipment may result in disciplinary actions up to and including dismissal. Information Technology Services personnel will follow Inspector General direction to ensure appropriate Chain of Custody compliance.

d. Region and Institution Information Systems Security Officers and Program Office Supervisors. Region, institution and headquarters Information Systems Security Officers and Information Technology Services management staff are responsible for reporting any security incidents or violations to the Information Systems Security Manager and the DCF Service Desk. The region or institution Information Systems Security Officer is responsible for tracking and resolving or disposing of all incidents reported to or referred by the DCF Service Desk. Functioning as the Region Security Coordinator, the region or institution Information Systems Security Officer or delegate is responsible for maintaining a log of all reported security violations or incidents, and using this information to determine actions steps that could deter or mitigate the impact from future incidents of a similar nature. The report in the log should also contain a disposition for the incident and an estimate of how much damage/cost was incurred, if any. The Information Systems Security Officer shall provide disposition information to the DCF Service Desk. Incident log data collection requirements include:

(1) Date incident reported;

(2) Incident date;

(3) Reported by;

(4) Contact e-mail;

(5) Contact phone; and,

(6) Incident description and details.

e. DCF Service Desk. The DCF Service Desk is responsible for consolidating reported incidents. The DCF Service Desk is also responsible for contacting the Information Security Manager (ISM) or designee when a report or disposition is received.

f. Special Requirements for Florida Statute 817.5681. In accordance with Florida Statute 817.5681, if client information is contained an unencrypted mobile device and that device is lost or stolen, the Department must ensure that all clients whose information may have been compromised are notified and that the notification occurs within 45 days. The use of unencrypted devices in the performance of the Department's work is prohibited.

g. Special Requirements for Internal Revenue Service Notification. Any employee or contract employee that suspects a possible improper inspection or disclosure of Federal Tax Information (FTI) should report to the Treasury Inspector General for Tax Administration (TIGTA) in Atlanta at 1-404-338-7449. In addition to notifying the TIGTA, the agency must notify the IRS office of safeguards. The agency must document the specifics of the incident including all relevant facts and the report must be emailed to safeguardreports@IRS.gov. Reports must be sent electronically and encrypted with the subject line "Data Incident Report." The agency must contact TIGTA and IRS immediately, but no later than 24-hours after identification of a possible issue involving FTI. A post incident review must be conducted after the incident has been addressed and any issues remediated.

h. Special Requirements for Social Security Administration Data. Any employee that experiences or suspects a breach or loss of Personally Identifiable Information shall notify the the Department's Information Security Manager. The Department must notify the United States Computer Emergency Readiness Team (www.us.cert.gov) within one hour of discovering the incident. The Department must notify the Social Security Administration's System Security contact named in the CMPPA agreement. If within one hour the Department has been unable to make contact with SSA's Systems Security contact, the Department must contact the Division of National Network Services and Operations, Customer Service Center at (877) 697-4889.

i. Special Requirements for Breaches of Unsecured Health Information. No later than 60 days after the discovery of a breach, the Department and/or business partner shall make notifications as required by ARRA Title XIII, Section 13402, "Notification in the Case of Breach," which includes notices to individuals, to the media if more than 500 individuals are affected, and to the Secretary of the U.S. Department of Health and Human Services (HHS). The Secretary of HHS must be notified immediately in breaches of more than 500 individuals; otherwise a log of smaller breaches shall be maintained and reported annually.

Chapter 4

USE OF WIRELESS TECHNOLOGY AND MOBILE DEVICES

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

4-2. Mobile Devices and Wireless Networks. 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. Employees issued mobile devices 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. Only department-owned information technology resources may be used by DCF employees to access DCF applications and data, with the exception of e-mail over the internet. Those who access e-mail from a personal computer must continue to abide by department security policies and procedures. Contractors with DCF may 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 agency contract with these entities. As appropriate, evaluation of the ability to meet these standards may be part of the procurement process. Such evaluations shall be conducted by the DCF security officer or designee.

c. System users must always physically secure 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.

d. System users must report any lost or stolen devices immediately to their Information Systems Security Officer and the DCF Service Desk. (71A-1.014(12), F.A.C.) The Information Systems Security Officer must notify the Agency Information Security Manager, the CIO and the Inspector General immediately and affected employees must file a police report. Each report of a lost or stolen device must contain:

(1) Date reported;

(2) Employee making the report (including e-mail address and phone);

(3) Lost or stolen device property custodian name/employee name (include e-mail 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.

e. Mobile Devices. If Department employees are issued mobile devices, the employee must maintain the password, virus protection and encryption configuration provided. If system users keep data on a mobile device, any media, including flash cards, memory sticks, or external hard drives must be stored in a secure location when not in use. In addition the following procedures must be followed:

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

(2) Mobile devices for Department employees must be purchased and approved through MyFloridaMarketPlace or through the Automated Requisition Tracking System (ARTS), which includes proper justification, supervisory approval and the assurance of proper encryption configuration.

f. Wireless Cards/PDAs/Blackberries/etc. Only wireless technology issued by the Department is authorized for Department employee business activities in order to ensure the use of 128-bit encryption. The Department will use centralized encoding of wireless cards to achieve control for these devices while allowing interoperability at various Department office locations.

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. Questions should be referred to the region or facility Information Systems Security Officer.

(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.