

CF OPERATING PROCEDURE
NO. 50-2

STATE OF FLORIDA
DEPARTMENT OF
CHILDREN AND FAMILIES
TALLAHASSEE, March 10, 2009

Systems Management

SECURITY OF DATA AND INFORMATION TECHNOLOGY RESOURCES

This operating procedure outlines the processes to follow to ensure the security of Departmental data and other information resources; department and contract provider responsibilities to ensure this security; and the measures to follow in the event of a security incident.

BY DIRECTION OF THE SECRETARY:

(Signed original copy on file)

ELWOOD MCELHANEY
Acting Assistant Secretary for
Administration

SUMMARY OF REVISED, DELETED, OR ADDED MATERIAL

This operating procedure updates, reorganizes, and consolidates the following operating procedures into a single document: CFOP 50-2, Security of Data and Information Technology Resources; CFOP 50-6, Security; and CFOP 50-19, Policy on Security Incident Reporting and Tracking. A portion of CFOP 21 on Wireless Networks is also included in this new operating procedure. CFOP 50-3, Client Information System Security Responsibilities, is now obsolete.

This operating procedure also includes wording changes to reflect the department's current organizational structure and to meet the Governor's plain language initiative criteria.

This operating procedure supersedes CFOP 50-2 dated July 1, 2007; CFOP 50-6 dated April 8, 2002; and CFOP 50-19 dated August 1, 2006. The operating procedure also supersedes those portions of CFOP 50-21 dealing with wireless networks.

OPR: ITS

DISTRIBUTION: A

CONTENTS

Paragraph

Chapter 1 – GENERAL

Purpose.....1
Scope.....1
Authority.....1
Definitions.....1

Chapter 2 – SECURITY OF DATA AND INFORMATION TECHNOLOGY RESOURCES

Purpose.....2
System Security.....2
Physical/Site Security.....6
Input/Output Security.....7
Orientation.....7
Training.....7
Security Awareness.....7
Audit and Certification.....8
Release of Information.....8

Chapter 3 – DEPARTMENT AND CONTRACT EMPLOYEE ACCESS TO DATA

Purpose.....9
Policy Statement.....9
Procedure.....9

Chapter 4 – SECURITY INCIDENT REPORTING AND TRACKING

Purpose.....10
Background.....10
Responsibilities for Reporting and Handling Actual or Suspected
Security Incidents/Violations.....10

Chapter 1

GENERAL

1-1. Purpose. This operating procedure outlines the processes to follow to ensure the security of Departmental data and other information resources; system users' responsibilities to ensure this security; and the measures to follow in the event of a security incident.

1-2. Scope. This operating procedure applies to anyone who has access to data through the use of computer-related media. The resources covered by this operating procedure includes 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 includes such resources used in offices, in the field, or at telecommuting sites.

1-3. Authority. Section 282.318, Florida Statutes, "Security of Data and Information Technology Resources," Chapter 815, Florida Statutes, "Florida Computer Crimes Act," and, Florida Administrative Code, Chapter 60DD-2, "Florida Information Resource Security Policies and Standards."

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

- a. Confidential and Sensitive 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 a computer.
- c. Data Center(s). For security purposes, any site designated as such by the Information Security Manager.
- d. Departmental Data Processing Systems. Systems that are maintained and operated at the DCF Data Center, and other departmental data processing sites.
- e. Information Security Manager. The person designated by the Secretary of the Department to administer the department's data and information technology resource security program.
- f. Information Technology Resources. Data processing hardware, software and services, supplies, personnel, facility resources, maintenance, training, or other related resources.
- g. Input Sources. The media used to collect and record data that are subsequently transferred to an automated information system.
- h. Local Application Software. Local data processing software that is the responsibility of the individual using the software at that location.
- i. Micro-sites. Region data processing sites that are not large enough to be declared data centers, but represent a hub of processing, or contain a significant amount of data processing equipment and other information technology resources that, if lost, would result in an extreme hardship on the Department to achieve its goals.
- j. Output Products. The media generated as a result of the processing of data by an automated information system.

- k. Security 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 state technology resources, and/or electronic denial of technology resource services.
- l. Security Violation. An intentional 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.
- m. Security Officer(s). The person(s) designated by the Department's Information Security Manager, Program Administrator, or Region Management Systems Director to administer a security program.
- n. Removable Media. Removable storage devices such as a thumb drives, CDs, diskettes, external hard drives, or flash card designed to be very small, highly portable and can store large quantities of data. The drives generally use USB interfaces. The flash cards may be used in computers or cameras; both could contain confidential data.
- o. Stand-Alone Equipment. Information-processing equipment (e.g., PCs, LAN Servers, Unix Systems) which uses local application software and is not dependent upon a central data processing system.
- p. System Owner(s). The entity that owns the data and has the primary responsibility for decisions relating to a particular data processing system's specification and usage.
- q. 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, DCF computer systems, or DCF data for the purpose of conducting business or providing services and who must comply with Standard Contract Section I.H, "Confidentiality of Client Information."

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.

a. DCF Technology Center.

(1) Each person who uses equipment to access the systems resident at the DCF Technology Center or access any departmental data by means of information technology resources owned, purchased, or leased by the department will have a unique personal identifier(s). A security officer will assign and control personal identifier(s). This identifier(s) will be confidential. Prior to obtaining a personal identifier, the owner must sign form CF 114 and complete the computer based Security Awareness Training course (within 10 days of employment for new hires).

(2) 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. This initial security measure will ensure a general level of security across all systems. The system owner may implement additional levels of security if the system owner makes a request and the Information Security Manager approves the request.

(3) It is the responsibility of the user to secure and protect their personal identifier (i.e., userid and password).

b. Stand-alone Equipment. Security measures for systems on stand-alone equipment will be the responsibility of the Security Officer in the Region or Headquarters location **and** the individual generating and using the data in those systems. The use of a unique identifier for each individual user of stand-alone equipment is recommended and may be required based on the level of security as identified by the owner of the data.

c. Network Security. Network security is divided into three separate areas of control: Statewide Networks, DCF Technology Center networks, and Local Area Networks. Both Headquarters and Region staff will follow network security procedures which the Office of Information Technology Services' Production Services network staff may designate and update to maintain and enhance network security in accordance with this operating procedure.

(1) The Florida Department of Management Services (DMS), Division of Communications, controls statewide Networks. DCF and many other state agencies utilize the DMS statewide telecommunication backbone to supply on-line computer systems access and internet access. Systems such as the Florida On-line Recipient Integrated Data Access System (FLORIDA) and Florida Safe Families Network (FSFN) utilize this as the primary communications line. No other access to the internet is allowed without specific approval from the DMS through the DCF Office of Information Technology Services' Central Office Network Control. Security of the network is the sole responsibility of the DMS.

(2) DCF Technology Center networks refer to any statewide telecommunication lines utilized to provide on-line systems access that are not part of or controlled by the DMS. These networks include Metropolitan (MAN), Local Area Networks (LAN), Wireless LAN (WLAN), and State of Florida Internet Access (SOFIA) for inbound internet traffic to the Technology Center DMZ. There are no other independent connections to the internet from these networks, only connections via the DMS approved internet connections are permitted. Security of these networks is the sole responsibility of the DCF. (See CFOP 50-13.)

(3) Local Area Networks refer to all Region controlled WLAN, LAN and MAN circuits. Local Area Networks may access DCF application systems, but connectivity cannot be from an independent internet service. Region/Institution IT Managers and/or local system administrators have responsibility to maintain the security for these networks.

(4) Connecting unauthorized equipment and personal electronics (IPOD, cameras, hard drives, thumb drives, etc) to DCF equipment and/or networks is forbidden. Violation of this may result in disciplinary action.

(5) All equipment must have the approved DCF standard anti-virus software installed and configured to download automatically the current signature file. The anti-virus software must be set to scan emails and file downloads in real time as well as do a full system scan once a day. Additionally, all Windows based computing equipment must have Microsoft Updates set to automatically download and install any critical update. Violation of this may result in disciplinary action.

d. Removal of Sensitive Data. The following procedures are to be followed:

(1) Prior to the disposal, off site repair of an IT device (server, storage, or client, network components, operating system or application software, and storage), or “reuse” by another agency, or for “reuse” by another system within the same agency, the owner shall backup any necessary files then remove all sensitive data from the IT devices (servers, storage, clients), network components, operating system or application software, and storage media. Similarly, the owner, as defined by the agency, should remove all sensitive data from the IT device (server, storage, and client), network components, operating system or application software, or storage media prior to its disposal.

(2) Staff may overwrite meaningful data with meaningless data on reusable storage devices if the meaningful data cannot be recovered. The minimum criteria for overwriting are 7 successful passes. Staff may not use operating system commands such as FDISK, FORMAT utilities, or DELETE, etc. to overwrite data, as data overwritten in this manner may be recovered. CFOP 50-7 contains a list of approved vendor software for data overwriting.

(3) Disposal of storage devices must meet HIPAA regulations.

(4) When storage devices are permanently removed from service for disposal, staff must destroy the physical medium to prevent devices from potentially retrieving information from it.

(5) Any magnetic media that contains sensitive or confidential information must be sanitized by one of the above methods prior to release to outside vendors for repair/maintenance. If the data owner determines that the media is not sanitized, the media should not be released.

(6) Only authorized personnel should remove sensitive data from IT devices permanently or temporarily removed from department use. The authorized personnel should document on the appropriate form, i.e. surplus form or log, when, how, and what method was used for sanitizing. All surplus PCs and any removed disk drives or other small removable storage devices must have a label applied that indicates the date staff cleaned the drive, name of the person who cleaned the drive, and the method used for cleaning.

e. Removable Media. If employees use removable media, the employee must protect the data by using a biometric lock, password, or encryption. If employees keep data on this type of media, the media, including flash cards, must be stored in a secure location when not in use. In addition the following procedures are to be followed:

(1) Confidential data may NOT be stored on ANY unencrypted mobile device (laptops, thumbdrives, CDs, disk, etc).

(2) Staff may only use agency purchased, encrypted thumbdrives on state owned hardware.

(3) Media devices must have encryption and must be purchased and approved through the normal IRR process, which includes proper justification and supervisory approval.

(4) Removable media used in conjunction with state business must also comply with disposal and data removal policies. Employees must seek technical expertise from Tier 1 support staff, their local Security Officer or the Region IT Manager for disposal and data removal.

f. Diagnostic Equipment Security. The following procedures are to be followed in using diagnostic tools on data communications circuitry upon which Department of Children and Families data traverses:

(1) Only personnel approved by the security and network staff of DCF will operate Network diagnostic equipment such as data scopes, hardware and software sniffers.

(2) Staff will not leave diagnostic equipment, when not in use, attached to any portion of the network.

(3) Staff will store diagnostic equipment in a specified secure location when the equipment is not in use.

(4) When a technician checks out diagnostic equipment for use at Northwood, the technician will contact the DCF Help Desk open a ticket, which will record who has the equipment, where it will be used on the network, and the purpose. The Help Desk will close completed tickets and erase the equipment memory and logs to prevent the next technician from seeing confidential data. When regional staff check out diagnostic equipment, the regional technician will contact the Region IT Manager or designee to record who has the equipment, where it will be used on the network, and the purpose. Upon completion of use, the technician will contact the Region IT Manager or designee, who will erase the equipment memory and logs to prevent the next technician from seeing confidential data.

g. Laptops and Wireless Networks. This technology is easy to move from secure locations and therefore, pose a data security risk. Individual users should understand these risks. Below are the Department's minimum security requirements for use of this technology. Other state or federal data security standards may be required beyond those listed here.

(1) Laptop Security. Users of laptops are responsible for ensuring the physical security of the laptop and the security of any data or information stored on the laptop. No confidential information may be stored on an unencrypted laptop. As with any desktop computer, users should remove any documents from a laptop that is surplus or disposed of. Employees must seek technical expertise from Tier 1 support staff, their local Security Officer, or the Region IT Manager if they are not familiar with the special overwriting process to follow when disposing of or surplus a laptop. Users must always physically secure laptops when not in their possession. Employees must set Bios passwords on all department laptops assigned to them. Staff should contact local Region IT Office to have this password set. Information Technology Services will not approve the purchase of laptops without Computrace LoJack for Laptops software for the life of the laptop, which will help protect confidential data. Staff must report any thefts, losses, or compromised security immediately to the Region IT Manager and then the Information Security Manager. The Information Security Manager must notify the Inspector General and the CIO immediately and affected staff should file a police report.

(2) Wireless Cards/PDAs/Blackberries/etc. Wireless technology shall use a minimum 128 bit encryption. The Department will use centralized encoding of wireless cards to achieve control for these devices while allowing interoperability at various state office locations. Staff will not transmit confidential data unencrypted via wireless devices or across unsecured public lines. Any e-mail containing confidential data sent via wired or wireless means must use at least 128 bit encryption and meet Department software standards as described in the Statewide Office Automation Standards (CFOP 50-7). Staff should place highly sensitive information into an MS Word document, locked using the Word document lock feature, and then included as an attachment to the e-mail. Staff should give the document password to the e-mail recipient over the telephone and NOT via e-mail.

(3) Personal Home Wireless Network. If you connect DCF equipment to your home Wireless network, you must make sure you have followed basic steps in order to ensure transmissions over your network are secure. The steps below summarize what you should do to improve the security of your home wireless LAN.

(a) Change Default Administrator Passwords (and Usernames). At the core of most Wi-Fi home networks is an access point or router. To set up these pieces of equipment, manufacturers provide Web pages that allow owners to enter their network address and account information. Web page owners must enter a username and password in a login screen to access these web tools.

However, for any given piece of equipment, the logins provided are simple and very well-known to hackers on the Internet. Change these settings immediately.

(b) Turn On (Compatible) Encryption (WEP or WPA). All Wi-Fi equipment supports some form of “encryption.” Encryption technology scrambles messages sent over wireless networks so that humans cannot easily read the messages. Several encryption technologies exist for Wi-Fi today. Naturally, you will want to pick the strongest form of encryption that works with your wireless network. To function, though, all Wi-Fi devices on your LAN must share the identical encryption settings. Therefore, you may need to find a “lowest common denominator” setting.

(c) Change the Default SSID. Access points and routers all use a network name called the “SSID”. Manufacturers normally ship their products with the same SSID set. For example, the SSID for Linksys devices is normally “linksys.” True, knowing the SSID does not by itself allow anyone to break into your network, but it is a start. More importantly, when someone finds a default SSID, they see it is a poorly configured network and are much more likely to attack it. Change the default SSID immediately when configuring your LAN.

(d) Enable MAC Address Filtering. Each piece of Wi-Fi gear possesses a unique identifier called the “physical address” or “MAC address.” Access points and routers keep track of the MAC addresses of all devices that connect to them. Many such products offer the owner an option to key in the MAC addresses of their home equipment that restricts the network to allow only connections from those devices. Do this, but also know that the feature is not as powerful as it may seem.

(e) Disable SSID Broadcast. In Wi-Fi networking, the access point or router typically broadcasts the network name (SSID) over the air at regular intervals. This feature was designed for businesses and mobile hotspots where Wi-Fi clients may come and go. In the home, this feature is unnecessary, and it increases the likelihood an unwelcome neighbor or hacker will try to log in to your home network. Fortunately, most Wi-Fi access points allow the network administrator to disable the SSID broadcast feature.

(f) Assign Static IP Addresses to Devices. Most home networkers gravitate toward using dynamic IP addresses. DHCP technology is indeed quick and easy to set up. Unfortunately, this convenience also works to the advantage of network attackers, who can easily obtain valid IP addresses from a network’s DHCP pool. Turn off DHCP on the router or access point, set a fixed IP address range, then set each connected device to match. Use a private IP range (like 10.0.0.x) to prevent computers from being directly reached from the Internet.

(g) Position the Router or Access Point Safely. Wi-Fi signals normally reach to the exterior of a home. A small amount of “leakage” outdoors is not a problem, but the further this signal reaches, the easier it is for others to detect and exploit. Wi-Fi signals often reach across streets and through neighboring homes. When installing a wireless home network, the position of the access point or router determines its reach. Try to position these devices near the center of the home rather than near windows to minimize this leakage.

2-3. Physical/Site Security.

a. Data Center(s). Each Region shall conduct, at a minimum, an annual analysis/review at each data center to determine the adequacy of physical/site security. It will take into account controlled physical access to the area, the need for disaster contingency planning, and other appropriate security requirements. The results of this review will be sent to the Information Security Manager as part of the Region Annual Security Report (ASR).

b. Micro-sites (and other locations with independent processing units not designated as data centers). The Security Officer responsible for site security should use preventive measures necessary

to minimize the risk of destruction, theft and other losses of equipment, software, and data. The Security Officer should evaluate the physical location and conditions surrounding the site and take the necessary precautions to protect it (e.g., locks may be required for each area where equipment is housed). The Region IT Manager shall annually evaluate the effectiveness of the site's security and report the findings in the ASR.

c. Terminal and Printer Sites. The person(s) responsible for the terminal and/or printer sites should use prudent physical security to protect the equipment and data from destruction, theft, and other losses through limited physical and visual access. The aim is to protect physically the equipment and data from accidental disclosure, modification, or destruction. When an employee leaves a workstation unattended, they must password protect the workstation, (i.e., lock your workstation within Windows).

2-4. Input/Output Security.

a. The physical/site security guidelines found in paragraph 2-3 of this operating procedure will govern the security for input sources, output products, system documentation, and manuals.

b. All federal and state laws, rules, regulations, policies, and procedures governing the confidentiality of data apply within any data processing site. It is the responsibility of the individual using the data to maintain appropriate confidentiality and the responsibility of the individual's supervisor to ensure that the employee has adequate training on protection of information.

c. Confidentiality Notice on E-mail. The following text is automatically included on all e-mail messages sent from the Department to external parties:

“CONFIDENTIALITY NOTICE: This message and any attachments are for the sole use of the intended recipient(s) and may contain confidential and privileged information that is exempt from public disclosure. Any unauthorized review, use, disclosure, or distribution is prohibited. If you have received this message in error please contact the sender (by phone or reply electronic mail) and then destroy all copies of the original message.”

d. Users must change all default usernames and passwords to department standards.

e. System owners will review system security logs.

2-5. Orientation. The Department's Information Security Manager will be responsible for providing rules, policies, procedures, and guidelines on departmental information security. All new employees will review this material during new employee orientation sessions through the use of the computer based security awareness training course. All system users must complete this course within 10 days of hire.

2-6. Training. This operating procedure requires all new system users review applicable state and federal rules and regulations that pertain to data confidentiality and information security as a part of their pre-service training. Human Resources will advise supervisors and their employees of the specific security requirements of their positions. Human Resources and supervisors will notify employees of any changes to confidentiality laws or changes to Departmental security rules, policies, procedures, and/or guidelines, or any specific security requirements of their positions by their supervisor and/or Security Officer as well as annual refresher training.

2-7. Security Awareness. The Department's Information Security Manager is responsible for implementing and maintaining a statewide Security Awareness Training program that will ensure that employees are aware of the importance of information security. This program will provide annual security awareness training to Office of Information Technology Services staff and Headquarters staff, as well as all Region staff that utilize confidential data or automated systems. All system users will be

required to complete this training annually. The Region IT Managers are responsible for tracking training in their respective Regions. 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. CBCs, vendors, providers and other DCF business partners are responsible for completing and tracking this mandatory training (see DCF Standard Contract, paragraph W).

2-8. Audit and Certification.

a. The department will conduct regular internal audits and evaluations of the security of data and information technology resources and sites.

b. All Region IT Managers and Headquarters will submit an Annual Security Report to the Information Security Manager. These reports will certify that security in each Region and Headquarters conforms to the rules, policies, procedures, and guidelines developed for the department. Certification is required on or before June 1 of each year beginning June 1, 2000. Each annual report shall include:

(1) Location of all data processing centers and micro-sites, date of the physical security site review, and report findings for each.

(2) Any Security Awareness Training that was conducted in addition to the mandatory on-line training including dates the training was conducted, sites where conducted, name of the trainer, and number of staff trained at each session.

(3) Number of reported security breaches since the last annual report. This would include loss from malicious physical equipment damage and/or loss of data due to malicious actions or virus infections, thefts, wireless intrusions, etc. The report must include details for any outstanding or unresolved security breaches for that year or any that resulted in losses in excess of \$5,000 and any incident of significant data compromise or events causing significant user downtime.

(4) A list of all regional owned or developed data processing systems.

(5) Certification that the Region's Information Systems Disaster Recovery Plan has been reviewed and updated within the past twelve months.

(6) An updated listing of all security officers, location, contact information, and application(s) they support.

(7) Results of the Physical/Site Security review done by local security staff and correction action for security audits under paragraph 2-3 of this operating procedure.

(8) An updated listing of all Region backups processes. This list will include systems, server name, IP address, backup schedule, customer, etc.

(9) Certification that all department computers, laptops, and mobile devices are setup using Department security procedures.

2-9. Release of Information. The system owner will make any decisions relating to the release and distribution of information in any form (e.g., on-line inquiry, printed reports, microfiche, or any magnetic media). No information will be released without the system owner's prior approval. In an emergency situation (e.g., the Inspector General's office is investigating the death of a child under DCF protection), the DCF Chief Information Officer (CIO) may grant an exception to this requirement.

Chapter 3

ACCESS TO DATA

3-1. Purpose. This operating procedure states the Department of Children and Families' policy concerning minimum security responsibilities regarding access to data. Adherence to this policy will help ensure personal accountability pertaining to the security of access to data using computer-related media.

3-2. Policy Statement.

a. Every system user shall be held responsible for information security, especially involving the access, transport or storing of sensitive and confidential information. Fulfillment of security responsibilities shall be mandatory and violations may be cause for disciplinary action, up to and including dismissal, civil penalties, or criminal penalties under chapters 119, 812, 815, 817, 839, or 877, Florida Statutes, or similar laws.

b. Security Agreement Form. All system users with access to data through computer-related media, will receive a copy of the "Florida Computer Crimes Act (Chapter 815, Florida Statutes)," the DCF Security Agreement Form (CF 114), and a copy of CFOP 50-2. All system users will acknowledge receipt of the minimum security requirements in the "Florida Computer Crimes Act (Chapter 815, Florida Statutes)" and departmental policy and procedures and agree to abide by the requirements by signing the CF 114 form.

c. Password Security. Information sharing with selected employees 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 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.

d. Emergency Password Sharing. For special emergency needs to conduct official state business, an e-mail password may be divulged to a trusted individual of the password owner's choosing, but only if it becomes absolutely necessary to conduct such business. The password owner shall consider the shared password compromised and shall change the e-mail password as soon as possible.

e. User ID and Password Expiration. Systems will automatically revoke user IDs that have not been used for a period of 60 days and will require Security Officer intervention for reactivation. The Security Officer will verify current or continued employment. Users must change passwords every 45 days or systems will automatically lock the user's account.

3-3. Procedure.

a. State Employees. The supervisor will provide a copy of the DCF Security Agreement Form (CF 114) to each employee who has access to data through the use of computer-related media (e.g., printed reports, microfiche, system inquiry, on-line update, or any magnetic media). The supervisor will sign and forward the original copy to the personnel office and the personnel office will place the original in the employee's personnel folder. All department employees will retain a duplicate copy of the form and a copy of the "Florida Computer Crimes Act (Chapter 815)".

b. Contract Provider Security Requirements. The department's contract manager will determine whether the provider should have access to data using computer-related media. The contract provider will identify an individual to function as its Data Security Officer. This Data Security Officer will act as a liaison to the department's security staff. The provider will obtain signed CF 114 forms from each of its employees who have access to data at least annually. *Note: For multi-year contracts, each provider employee must submit newly signed forms upon the contract's renewal.* The provider is responsible for maintaining the signed CF 114 forms for its employees who have access to data and will make the forms available to authorized department staff upon request. All provider employees will retain a duplicate copy of the form and a copy of the "Florida Computer Crimes Act (Chapter 815)".

c. Supervisors are responsible for immediately notifying the local Security Office upon the termination, transfer, or resignation of any DCF or contract employee for the purpose of system access adjustment or termination.

Chapter 4

SECURITY INCIDENT REPORTING AND TRACKING

4-1. Purpose. This chapter outlines responsibilities for reporting, tracking, handling, and resolving incidents that result in damage, release of confidential information, and/or electronic denial of data processing services or security violations that could potentially lead to a breach of security.

4-2. Background. Computer systems are subject to a wide range of mishaps from corrupted data files to viruses to natural disasters. For example, frequently occurring events (e.g., a mistakenly deleted file) can usually be readily repaired (e.g., by restoration from the backup file). More severe mishaps, such as outages caused by natural disasters, are normally addressed in an organization's contingency plan. Other damaging events result from deliberate malicious technical activity (e.g., the creation of viruses or system hacking). A computer security incident or violation can result from a computer virus, other malicious code, or a system intruder, either an insider or an outsider. It can more generally refer to those incidents that, without technically expert response, could result in severe damage. The primary benefits of an incident handling capability are containing and repairing damage from incidents, and preventing future damage.

4-3. Responsibilities for Reporting and Handling Actual or Suspected Security Incidents/Violations.

a. System Owners. System owners are responsible for ensuring that their application 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 violations.

b. System Users. A system user who knows or suspects that a security incident or violation has occurred is responsible for informing their supervisor immediately of the incident or violation. Failure to do so may result in disciplinary actions as prescribed in the Employee Handbook (CFP 60-1) for state employees and removal from the contract for contracted employees as well as possible legal action.

c. Supervisors. Supervisors are required to notify immediately their manager, Region IT leader, and the Inspector General of any suspected or confirmed security incidents or violations. At the direction of the Inspector General, supervisors will coordinate with Office of Information Technology Services personnel immediately to ensure the equipment security by placing it 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 as prescribed in the Employee Handbook (CFP 60-1). Office of Information Technology Services

personnel will examine the equipment, if necessary, with consent from the Inspector General using the Chain of Custody Form.

d. Region IT Leaders and Program Office Supervisors. Region IT Leaders are responsible for reporting any security incidents or violations to the Information Security Manager and the Office of Information Technology Services' Helpdesk (487-9400/SC 277-9400). Headquarters program office supervisors should report to the Information Security Manager and the Office of Information Technology Services' Helpdesk. The Region IT Leader is responsible for tracking and resolving or disposing of all incidents reported to him/her, or referred back to the Region IT Leader by the Helpdesk. Functioning as the Region Security Coordinator, the Region IT Leader 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.

e. Helpdesk. The Helpdesk is responsible for entering reported incidents into its tracking system and for following up on these reports until they are closed. The Helpdesk is also responsible for contacting the Information Security Manager (ISM) or designee when a report is received. The Helpdesk will generate monthly reports and send the reports to the Office of Information Technology Services' Security Administrator.

(Note: To view the following graphic on your computer, you must be in "page layout view.")

Process for Handling Potential Security Violations

