STATE OF FLORIDA
DEPARTMENT OF
CHILDREN AND FAMILIES
TALLAHASSEE, February 26, 2024

CF OPERATING PROCEDURE
NO. 50-14

Systems Management

POLICY ON VIRUS PREVENTION, CONTROL, REPORTING, AND RECOVERY

This operating procedure establishes a cybersecurity framework by which to secure Department of Children and Families (Department) information technology resources, includes but not limited to Chapter 60GG-2, Florida Administrative Code (FAC).

BY DIRECTION OF THE SECRETARY:

(Signed copy on file)

COLE SOUSA
Chief Information Officer

SUMMARY OF REVISED, DELETED, OR ADDED MATERIAL

Annual review and revision completed; revised the operating procedure to reflect the Department's current virus policy and processes by incorporating sections five through seven (renumbered section 5); created subsection 5.3, Procedure for Handling Denial of Services (DoS) Attacks, and renumbered sections eight and nine (6 and 7).

This operating procedure supersedes CFOP 50-14 dated October 6, 2022.
OPR: ITS
DISTRIBUTION: A

Contents Page

1. Purpose. This operating procedure outlines the Department of Children and Families (DCF or Department) policy to minimize damage from computer viruses, denial of service attacks, and provides instructions for preventing, controlling, reporting, and recovering from cyber-attacks.

2. Scope. This operating procedure applies to all Department employee and contractors.

3. Authority.

a. Section 282.318, Florida Statutes (F.S.), "State Cybersecurity Act."

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

c. Chapter 815, F.S., "Florida Computer Crimes Act."

d. Chapter 60GG-2, Florida Administrative Code, "Florida Cybersecurity Standards."

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

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

g. 26 U.S. Code § 6103, "Confidentiality and disclosure of returns and return information."

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

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

j. NIST 800-83 r1, "Guide to Malware Incident Prevention and Handling for Desktops and Laptops."

4. Definition.

a. Confidential Information and/or Confidential Data. Information not subject to inspection by the public that may be released only to those persons and entities designated in Florida statute; information designated as confidential under provisions of federal law or rule, including but not limited to, Federal Tax Information (FTI), Health Insurance Portability and Accountability Act (HIPAA) Protected Health Information (PHI), Personally Identifiable Information (PII), Social Security Numbers (SSN), and drivers' license information and/or photographs.

b. Denial of Service (DoS). A type of cyber attack in which a malicious actor aims to render a device (e.g., computer, telephone, printer, fax) to its intended users by interrupting the device normal function.

c. 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 this operating procedure, the definition of employee includes any non-OPS temporary staff hired by the Department who have access to DCF IT resources.

d. Information Security Manager/Officer. A person designated by the Secretary of the Department to report to the Chief Information Officer (CIO) and administer DCF's information technology security program, serving 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 per section 282.318, F.S., and Chapter 60GG-2, F.A.C.

e. Information Technology Resources. Data processing hardware (including desktop computers, laptops, tablets, smartphones, and associated devices), software, and services.

f. Malware. Programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy, exploitation, unauthorized access to system resources, and other abusive behavior. Malware is a general term used to mean a variety of forms of malicious, intrusive, or annoying software or program code, including viruses, worms, rootkits, and Trojan horses.

g. Mobile Device. Any non-stationary electronic device with a singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images; includes but is not limited to laptops, personal digital assistants, pocket personal computers, MP3 players, smartphones, and video cameras.

h. Virus. A computer program or code that self-replicates by inserting copies of itself into host programs or data files. A virus might corrupt, destroy, or modify existing data or software files, consume computer hard drive space, or memory-making system processing difficult or impossible. This type of program can attach itself to other pieces of software, firmware, or hardware.

5. General. Almost daily new viruses are created. The Department deploys and manages Enterprise-level anti-virus software and applications, in addition, Department staff shall utilize the procedures described below to prevent and mitigate the effects of viruses to IT resources.

5.1. Procedures for Preventing Viruses.

a. Companies that create virus-scanning software update their virus patterns (DAT/Signature) regularly. However, there will be occasions when staff may have a virus, and the appropriate and up-to-date scanning software will not be able to detect the virus. To keep such instances at a minimum, the Department should maintain current virus scanning software on all devices managed by OITS to identify weaknesses and remediate flaws. The Department uses automated security technologies to perform weekly scans and generate reports every other hour to identify system vulnerabilities.

b. All DCF owned/leased information technology resources shall have Department approved anti-virus protection software installed to:

(1) Automatically scan removable media received from another person, whether from inside or outside of the person's immediate office area, for viruses; and

(2) Automatically scan files transferred onto their PC from any outside source for viruses.

c. All DCF employees and contractors using remote connectivity to access the DCF Network shall adhere to CFOP 50-29, Wireless Access.

5.2. Procedure for Handling Viruses.

a. DCF employees and contractors should report any suspicious or unexplained system behavior on any DCF owned/leased equipment to the DCF Statewide Help Desk. The DCF Statewide Help Desk staff will attempt to assist the employee or contractor in identifying the problem or coding it as a suspected virus. The DCF Statewide Help Desk staff will create a service request ticket notifying

the Office of Information Technology Services (OITS) Enterprise support team (i.e., Security Risk Management Team, DCF Operations, and the ISM) of the alleged computer security incident. The system user's device will be isolated from the Network and remain isolated until notified otherwise.

b. The Security Risk Management and DCF Operations (Network & voice Services/ Region IT Managers/Staff; Server, Messaging & Cloud Administration; Data Security) will collaborate to:

(1) Make every reasonable effort to track the virus to its source and determine if the virus has spread to other system; and,

(2) Investigate suspected viruses and facilitate containment, eradication, and post-infection monitoring after virus detection,

(3) Document information discovered during the computer security investigation, using available tools and resources including but are not limited to how the system was infected, the path the virus took, and estimate the Department's incurred damage/cost in the helpdesk ticket, when applicable; includes notifying the ISM.

c. DCF Information Security Manager shall:

(1) Coordinate and/or perform incident reporting and activities with external state and federal partners, and any other DCF stakeholders and community partners.

(2) Submit any reports required by the Florida Department of Management Services (DMS) Florida Digital Services [DS] per Chapter 60GG-2, Florida Administrative Code.

d. Desktop Support shall:

(1) Assist system users in reestablishing connection to DCF IT resources by but not limited to resetting authentication mechanisms and reimaging devices.

(2) Document virus troubleshooting and disposition of computer security incident in the DCF Statewide Help Desk ticketing system.

5.3. Procedures for Handling Denial of Service (DoS) Attacks.

The Department shall take appropriate measures to prohibit or reduce the impact of DoS attacks aimed at disrupting business operations. OITS Enterprise staff shall monitor all devices managed by OITS to identify capacity abnormalities and, when applicable notify the Department CSIRT, per section 5.2. Make every effort to determine the DoS source, facilitate containment, and document information discovered during the investigation in the DCF Statewide Help Desk ticketing system.

6. Enforcement.

Violations of information security policies and procedures may result in loss or limitation on use of DCF IT resources, disciplinary action, up to and including termination of employment or contractual relationship, and referral for civil or criminal prosecution as provided by law.

7. Review and Revision.

This operating procedure will be reviewed and updated no less frequently than every 365 days or when a significant policy change occurs, whenever occurs first by the Department's Information Security Manager.