STATE OF FLORIDA
DEPARTMENT OF
CHILDREN AND FAMILIES
TALLAHASSEE, March 25, 2024

CF OPERATING PROCEDURE
NO. 50-29

Systems Management

WIRELESS ACCESS

This operating procedure describes the security requirements that Department of Children and Families (Department or DCF) information technology wireless access users shall follow to prevent the loss of confidentiality, integrity, or availability of DCF information received, processed, or transmitted through wireless technologies.

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, no substantive changes.

This operating procedure supersedes CFOP 50-29 dated October 6, 2022.
OPR: Information Technology Services

Contents

1. Purpose. This operating procedure establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access at the Department of Children and Families (DCF or Department). This operating procedure also provides the minimum security requirements for wireless access to prevent the loss of confidentiality, integrity, or availability of DCF information received, processed, or transmitted through wireless technologies.

a. All use of wireless access to the DCF network and business information systems must be authorized before allowing such connections.

b. The DCF Office of Information Technology Services (OITS) regulates and manages all wireless access points and the radio frequency bands used by wireless technology to ensure fair and efficient allocation and minimize collision, interference, unauthorized intrusion, and failure of the DCF wireless network.

c. This operating procedure provides compliance with MARS E 2.2 and IRS Publication 1075.

2. Scope. This operating procedure applies to all DCF employees, contractors, and vendors who work with the development or maintenance of the DCF systems and networks. All users employing wireless methods of accessing department technology resources must adhere to department defined processes, using department approved access points. Unauthorized access to the wireless network is not allowed.

3. References.

a. CFOP 50-2, Security of Data and Information Technology Resources.

b. Section 282.318, Florida Statutes, “State Cybersecurity Act.”

c. Section 501.171, Florida Statutes, “Security of Confidential Personal Information.”

d. Chapter 815, Florida Statutes, “Florida Computer Crimes Act.”

e. Chapter 60GG-2, Florida Administrative Code, “Florida Cybersecurity Standards.”

f. Title XIII, Section 13402, “Notification in the Case of Breach.”

g. Internal Revenue Service (IRS), Publication 1075, “Tax Information Security Guidelines for Federal, State and Local Agencies’ (11-2021).

h. Centers for Medicare & Medicaid Services (CMS), Minimum Acceptable Risk Safeguards for Exchanges (MARS-E) Document Suite, Version 2.2.

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

4. Definitions. For this operating procedure, the following definitions shall apply:

a. Access Point. A device that logically connects wireless client devices operating in infrastructure and provides access to a distribution system, if connected, is typically an organization’s enterprise wired network.

b. 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. They have access to Department IT resources, including contracted staff and contracted vendor staff.

c. Federal Tax Information (FTI). Federal tax returns and return information owned by the Internal Revenue Service (IRS) and utilized by DCF. FTI is confidential and may not be used or disclosed except as expressly authorized by the Internal Revenue Code

d. 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.

e. Personal Identifying Information (PII). Any information about an individual maintained by a department or agency, including (1) any information used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information linked or linkable to an individual, such as medical, educational, financial, and employment information.

f. Personal Information (PI). Any recorded information about an identifiable individual that may include name, address, email address, phone number, race, nationality, ethnicity, origin, skin color, religious or political beliefs or associations, age, sex, sexual orientation, marital status, family status, identifying numbers, codes, symbols, fingerprints, blood type, inherited characteristics, health care history, including information on physical/mental disability, educational, financial, criminal, employment history, and personal views.

g. Protected health information (PHI). Under US law, any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity) that can be linked to a specific individual.

h. Wireless Access Point. A device that acts as a conduit to connect wireless communication devices allows them to communicate and create a wireless network.

i. Wireless Application Protocol. A standard that defines the way in which Internet communications and other advanced services are provided on wireless mobile devices.

j. Wireless Local Area Network (WLAN). A wireless computer network links two or more devices using wireless communication within a limited area such as an office building.

5. Access Control Measures. The Department protects wireless access to the system by using access control measures that appropriately limit access to information technology resources to only those authorized to see or use the information based on a legitimate business purpose.

a. The DCF Security Awareness Training for new hires and the annual refresher must cover the usage restrictions for wireless access and remote access by DCF employees and be updated annually by the ISM in this regard. This training must be provided before new hires are allowed onto the DCF wireless network.

b. Only wireless technology issued by the Department is authorized for DCF employee business activities on the DCF wireless network to ensure the required use of high-level encryption (256 or higher, based on risk). Also:

(1) The Department requires centralized management of wireless technology. The DCF Network Manager and the Chief Information Officer must approve all new wireless technology.

(2) Wireless network passwords must be changed regularly at 90 to 180 days, based on risk level.

(3) The Department will develop and maintain WLAN procedures that include addressing the use of the reset function on access point devices.

(4) DCF employees must utilize DCF issued and managed devices on the DCF wireless network, as is required on the wired DCF network.

c. DCF program offices retain the right to further restrict the use of wireless access by their staff.

d. DCF program offices that receive, process, store, or transmit sensitive or confidential information that include but is not limited to PI, PII, PHI, and FTI retain the right to have other programmatic security conditions that must be met by their staff and managers.

e. DCF establishes usage restrictions and implementation guidance, including authentication and encryption requirements, for wireless technologies.

6. Authentication and Encryption. The department protects wireless access to the DCF network and business information systems by requiring authentication of DCF users and by having encryption in place. Only DCF owned devices should be on the DCF wireless network. Whenever technically possible, the department should protect wireless access to the DCF network and business information systems by requiring authentication of DCF devices.

7. Monitoring the Network and Systems for Unauthorized Connections. DCF OITS Network Team should perform the following duties:

a. Monitor the DCF wireless network to detect:

(1) Attacks and indicators of potential attacks to be reported and handled via DCF event response procedures.

(2) Unauthorized local, network, and remote connections to be reported and handled via DCF event response procedures.

b. Identify unauthorized use of the network and report these events according to DCF procedures for operational security review and response processes to implement DCF incident reporting procedures as appropriate.

c. Deploy monitoring devices:

(1) Strategically within the DCF network to collect essential network activity information.

(2) At ad hoc locations within the system to track specific types of transactions activity to the Department.

d. Protect information obtained from DCF intrusion-monitoring tools from unauthorized access, modification, and deletion.

e. Increase the level of wireless network monitoring activity whenever there is an indication of increased risk to DCF resources based on law enforcement information, intelligence information, or other credible cybersecurity information sources.

f. Conduct wireless monitoring activities consistent with Florida Statutes, Federal Law, Executive Orders, DCF policies, or other State and Federal regulations.

g. Provide information about the DCF wireless network as required for DCF business purposes.

8. Disable Non-Required Wireless Networking. DCF should disable wireless networking capabilities internally embedded within information system components before issuance and deployment when it is known the capabilities will not be required for DCF business purposes.

9. Restrict Configurations by Users. DCF identifies and explicitly authorizes the specific OITS network staff that can configure DCF wireless networking capabilities. The Network Services Team configures wireless networking capability within the DCF network and business information systems.

10. Transmission Power Levels.

a. DCF should select radio antennas and calibrate transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

b. Actions taken by DCF to limit unauthorized use of wireless communications outside of department-controlled boundaries should include:

(1) Reducing the power of wireless transmissions so that the transmissions are less likely to emit a signal that adversaries outside of the physical perimeters of DCF can use;

(2) Employing measures to control wireless emanations; and

(3) Using directional/beam forming antennas reduces the likelihood that unintended receivers will intercept signals.

(4) Before taking such actions, DCF OITS staff should conduct periodic wireless surveys to understand the radio frequency profile of organizational information systems as well as other systems that may be operating in the area.