Purchase Agreement #SCG25

Between

Central Florida Cares Health System, Inc.

And

Seminole County Government

THIS AGREEMENT "Agreement" is entered into by and between **CENTRAL FLORIDA CARES HEALTH SYSTEM, INC.**, hereinafter referred to as "CFCHS" or the "Company" and **SEMINOLE COUNTY GOVERNMENT** hereinafter referred to as the "COUNTY", (Company and COUNTY shall be jointly referred to herein as the "Parties").

FOR AND IN CONSIDERATION of the mutual undertakings and agreements hereinafter set forth, the Parties agree as follows:

1. General Description

The Florida Department of Children and Families, hereinafter referred to as the "Department", is requiring of the Managing Entities to oversee the implementation and administration of the Florida's Coordinated Opioid Recovery (CORE) Network of Addiction Care program. This shall require that Network Service Providers, Emergency Medical Providers, and Emergency Departments participating in a CORE project adhere to the service delivery and reporting requirements identified by The Department.

The CORE program requirements are as follows:

1. Provide a 24/7 access point where an individual can access medication assisted treatment (MAT), including weekends.
2. Ensure a clinic provider is available to receive individuals in need of services from the 24/7 access point, and that first responders can provide MAT until the individual can be seen in the clinic.
3. Provide treatment for co-morbid alcohol and benzodiazepine use disorders.
4. Ensure individuals receiving services have access to higher levels of care if needed, including outpatient detox.
5. Ensure the availability of clinical experts in addiction medicine, including licensed therapists in outpatient services and access to primary care for all individuals served.
6. Perform necessary lab work on all individuals to identify any infectious diseases.
7. Ensure individuals served have access to psychiatric care at the providers clinic or in the community.
8. Ensure availability of peer support staff to assist in navigating the CORE network and other supportive services needed.

9. Ensure care coordination is available based on an individual's need.
10. Ensure access to a variety of MAT, including buprenorphine (Buprenorphine) and Vivitrol, and referrals for methadone, if appropriate.
11. Capacity to continue prescribing MAT as long as the prescriber determines the medication is clinically beneficial, without any arbitrary limits on length of care.
12. Approach to dosing MAT that considers the specific circumstances and use pattern of the individual.
13. Availability to test biological specimens (e.g., urine, blood, hair) for fentanyl at the 24/7 access point and the receiving clinic.
14. Network Service Providers, Emergency Medical Providers, and Hospital Emergency Departments shall use the established clinic intake process.
15. Network Service Providers, Emergency Medical Providers, and Hospital Emergency Departments shall use the established protocol for induction on buprenorphine.
16. Naloxone kits shall be available to individuals without specific conditional requirements.
17. Provide access to group and individual therapy and recovery support groups facilitated by recovery peer specialists, where appropriate.
18. Procedures to address phases of treatment.
19. Ability to provide care to pregnant and parenting women.
20. Consistent monitoring of outcome measures and data including the use of the Brief Addiction Monitoring (BAM) tool and reporting as outlined in Section VIII of this document.

The Department requires that CFCHS enter into agreements with identified organizations under CORE. The purpose of this Agreement is for a service array to positively impact the Seminole County opioid crisis. Services that meet the program requirements, which could include but not limited to inpatient detoxification, outpatient detoxification, inpatient residential services, community residential services, and ambulatory medication-assisted treatment will be provided by Seminole County Government.

2. COUNTY Qualifications

COUNTY staff assigned to this agreement must possess the following minimum qualifications and experience:

a. Experience with harm reduction models of treatment to opiate addiction.

b. Experience with provider systems, including electronic health records and prescription drug monitoring programs.

c. Ability to work collaboratively within a team environment.

d. Appropriate credentials and licensing for their scope of service as defined by Florida Administrative Code: F.A.C. 65D and F.A.C. 65E.

3. Service Tasks

The COUNTY shall perform the following tasks in the time and manner specified and in compliance with *DCF Guidance Document 41*:

a. Ensure patients receiving treatment for substance use disorder (SUD) receive the appropriate level of treatment as determined by the American Society of Addiction Medicine (ASAM) that is delivered by qualified practitioners and substance use specialists that include licensed psychiatrists, psychiatric mental health nurse practitioners, counselors, case managers, peer support specialists, and medical assistants throughout the Purchase Agreement term.

b. For the patients referenced in **Exhibit A - Seminole County Coordinated Opioid Response (CORe) Plan** prepare a quarterly report that includes the use of a recognized psychometric assessment tool such as the Brief Addiction Monitor or the Functional Assessment Rating Scale to include summarizing the utilization of:

i. Inpatient Detoxification

ii. Inpatient Residential Level I

iii. Residential Level II

iv. Medication Assisted Treatment

- Psychiatric services
- Individual and Group Therapy
- Care Coordination
- Peer Support
- Pharmacy Services

c. Submit a quarterly report for individuals served, regardless of payer source, that are referenced in **Exhibit A - Seminole County Coordinated Opioid Response (CORe) Plan**. At a minimum, the report will include the following information and be submitted with the invoice:

- Length of time from referral date to first offered appointment
- Length of time from referral date to first kept appointment
- Length of time between follow-up appointments
- Length of time in treatment by program and covered services

d. Submit a quarterly report of the number of patients referenced in **Exhibit A - Seminole County Coordinated Opioid Response (CORe) Plan**, who were referred to other community resources listed below, as applicable. The report is to be submitted with the invoice.

- Housing
- Parenting

- Life skills training
- Employment assistance
- Name of Agency Referral
- Patient's funding status

e. Provide the Company a progress report of the number of individuals receiving treatment in the various programs across the continuum of care and submit with the invoice.

f. Provide the Company an aggregated progress report of client treatment through each program level and service level and submit it with the invoice.

g. Provide the Company a report regarding the access and availability to care and submit it with the invoice.

h. Provide the Company a report regarding linkages to other community support and agencies and submit it with the invoice.

4. **Data Security and Confidentiality Task**: The COUNTY, its employees, subcontractors, and agents must comply at all times with all Department data security procedures and policies in the performance of this scope of work.

5. **Contract Deliverables**

   a. The COUNTY will complete and submit the following deliverables to CFCHS in the time and manner specified:

      i. Quarterly: Provision of overdose patients' treated through services in the time and manner specified in **Sections 3.a. - 3.i.**

6. **Method of Payment**

   a. This is a fixed price Agreement. CFCHS shall pay the COUNTY in accordance with the conditions of this Agreement, a prorated amount each month, for a total amount not to exceed **$1,000,000.00**, subject to the availability of funds.

   b. COUNTY must submit on a quarterly basis, report with actual expenditures from the previous quarter.

   c. CFCHS shall reduce or withhold funds pursuant to Rule 65-29.001, F.A.C., if the COUNTY fails to comply with the terms of the Agreement.

   d. The COUNTY shall request payment monthly within five (5) days after the first day of the month following services. The invoice must contain the following information:

      i. Purchase Agreement (PA) number;

      ii. COUNTY name and address;

      iii. COUNTY Federal Identification Number;

      iv. Deliverables due during the period of service provision;

      v. Dates of service provision;

vi. Total hours billed for the invoice;

vii. Invoice amount; and

viii. Signature of the COUNTY's authorized representative and date signed.

e. CFCHS may require any other information from the COUNTY that it deems necessary to verify performance of the COUNTY under the Purchase Agreement.

f. CFCHS reserves the right to request supporting documentation at any time after the invoice has been submitted.

7. Performance Measures and Financial Consequences

All deliverables and related tasks must be completed 100% as specified. Failure to satisfactorily complete or submit a deliverable in the time and manner specified will result in a financial consequence as indicated below:

a. Failure to complete and submit the task outlined in **Section 5.a-i.** in the time and manner specified will result in a payment reduction equal to five percent of the quarterly invoiced amount.

b. Failure to comply with the Data Security and Confidentiality task will result in a payment reduction equal to five percent of the quarterly invoiced amount.

8. COUNTY Information

a. ANNUAL APPROPRIATIONS: CFCHS's obligation to pay under this contract is contingent upon an annual appropriation by the legislature.

b. BACKGROUND SCREENING: The COUNTY shall comply with the staffing qualifications and requirements (including background screening), required by this Agreement and as required by applicable law, rule, or regulations, including without limitation, the regulations of the Department.

The COUNTY shall comply with the provisions of s. 448.095(5), F.S. The COUNTY will use the E-verify system established by the U.S. Department of Homeland Security to verify the employment eligibility of its employees and the COUNTY's subcontracted employees performing under this Agreement.

Mental Health: The COUNTY shall provide employment screening for all mental health personnel and all chief executive officers, directors, and chief financial officers of COUNTY using the standards for Level II screening set forth in Chapter 435, and Section 408.809 Florida Statutes (F.S.), except as otherwise specified in Sections 394.4572(1)(b)-(c), F.S. For the purposes of this Agreement, "mental health personnel" includes all program directors, professional clinicians, staff members, clubhouse staff, drop-in center staff, and volunteers working in public or private mental health programs and facilities who have direct contact with individuals held for examination or admitted for mental health treatment, or who have access to client funds, personal property, or living areas. In addition, employment screening described in this paragraph may include a local criminal records check conducted through a local law enforcement agency.

Substance Abuse: The COUNTY shall ensure compliance with background screening in accordance with Section 397.4073, F.S. This statute requires employment screening for:

i. Owners, directors, chief financial officers and clinical supervisors of service providers.

ii. All service provider personnel who have direct contact with children receiving services or with adults who are developmentally disabled.

iii. All peer specialists who have direct contact with individuals receiving services are screened in accordance with Section 397.417(4), F.S.

Individuals subject to Mental Health and Substance Abuse screening in this section shall be re-screened within five (5) years from the date of their last screening results and every five (5) years thereafter.

At the time of the initial level 2 background screening, and with every 5-year re-screening, the COUNTY shall require mental health and substance abuse personnel to complete the current version of DCF Affidavit of Good Moral Character. The current version of the form CF 1649 (April 2021) is incorporated by reference an available at https://www.flrules.org/Gateway/reference.asp?No=Ref-15275.

c. **CONFIDENTIALITY:** The COUNTY shall comply with all confidentiality and non-disclosure requirements contained in Attachment I or required by applicable law, rule or regulation. Further, each party shall not use or disclose to any unauthorized person any information relating to the business or affairs of the other party or of any qualified individual, except pursuant to the express written consent of the other party or the qualified individual, as applicable, by court order, or as required by law, rule, or regulation.

d. **DATA SECURITY:** The COUNTY shall comply with the following data security requirements:

An appropriately skilled individual shall be identified by the COUNTY to function as its' Data Security Officer. The Data Security Officer shall act as the liaison to the Managing Entity's and the Department's security staff and will maintain an appropriate level of data security for the information the COUNTY is collecting or using in the performance of this Agreement. An appropriate level of security includes approving and tracking all COUNTY employees that request or have access to any Managing Entity or Departmental data system or information. The Data Security Officer will ensure that user access to the data system or information has been removed from all terminated COUNTY employees or employees on leave for more than thirty (30) days.

The COUNTY shall provide the latest Managing Entity or Departmental security awareness training to its staff and subcontractors who have access to Managing Entity or Departmental information.

All COUNTY employees who have access to Managing Entity or Departmental information shall comply with, and be provided with, a copy of CFOP 50-2, and shall sign the Department's Security Agreement form CF-112 annually. A copy

of CF-112 may be obtained from the Contract Manager.

The COUNTY shall make every effort to protect and avoid unauthorized release of any personal or confidential information by ensuring both data and storage devices are encrypted as prescribed in CFOP 50-2. If encryption of these devices is not possible, then the COUNTY shall assure that unencrypted personal and confidential Managing Entity or Departmental data will not be stored on unencrypted storage devices. The COUNTY shall require the same of all its subcontractors.

The COUNTY shall at its own cost provide notice to affected parties no later than thirty (30) days following the determination of any potential breach of personal or confidential Departmental data as provided in Section 501.171, F.S. The COUNTY shall require the same notification requirements of all its subcontractors. The COUNTY shall also at its own cost implement reasonable measures deemed appropriate by the Managing Entity or Department to avoid or mitigate potential injury to any person due to a breach or potential breach of personal and confidential Managing Entity or Departmental data.

e. **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT:** The COUNTY shall, where applicable, comply with the Health Insurance Portability and Accountability Act (42 U.S.C. 1320d.) as well as all regulations promulgated thereunder (45 CFR Parts 160, 162, and 164).

f. **INDEMNIFICATION:** The COUNTY, as a political subdivision of the state of Florida, shall not be obligated to indemnify, defend, or hold harmless the Department or CFCHS beyond the limits prescribed by Section 768.28, Florida Statutes, as this statute may be amended from time to time.

g. **INDEPENDENT COUNTY:** In performing its obligations under this Agreement, the COUNTY shall at all times be acting in the capacity of an independent contractor and not as an officer, employee or agent of CFCHS or the Department. Neither the COUNTY nor any of its agents, employees, or assignees shall represent to others that it is an agent of or has the authority to bind CFCHS or the Department by virtue of this Agreement.

h. **INSURANCE:** The COUNTY shall obtain and provide proof to the Managing Entity of comprehensive general liability insurance coverage (broad form coverage), specifically including premises, fire and legal liability to cover COUNTY and all of its employees.

The limits of the COUNTY's coverage shall be no less than $300,000 per occurrence with a minimal annual aggregate of no less than $1,000,000.

The Managing Entity and the Department shall be exempt from, and in no way liable for, any sums of money that may represent a deductible or self-insured retention under any such insurance. The payment of any deductible on any policy shall be the sole responsibility of the COUNTY.

All such insurance policies of the COUNTY shall be provided by insurers licensed or eligible to do and that are doing business in the State of Florida. Each insurer must have a minimum rating of "A" by A.M. Best (or an equivalent

rating by a similar insurance rating firm) and shall name the Managing Entity and the Department as additional insured parties under the policy. All such insurance policies of the COUNTY shall be primary to and not contributory with any similar insurance carried by the Managing Entity. The COUNTY shall notify the Contract Manager within 30 calendar days if there is a modification to the terms of insurance including but not limited to, cancellation or modification to policy limits.

The COUNTY shall use its best good faith efforts to cause the insurers issuing all such liability insurance to use a policy form with additional insured provisions naming the Managing Entity and the Department as an additional insured or a form of additional insured endorsement that is acceptable to the Managing Entity in the reasonable exercise of its judgment.

Proof of insurance shall preferably be in the form of an Association for Cooperative Operations Research and Development (ACORD) certificate of insurance. All such current insurance certificates will be submitted to the Contract Manager, prior to expiration, as insurance policies are renewed each year.

i. **LAW AND VENUE:** This Agreement is executed and entered in the State of Florida and will be construed, performed, and enforced in all respects in accordance with Florida law, excluding Florida provisions for conflict of laws, and applicable Federal law. Venue for any action regarding this Agreement shall be in Orange County, Florida.

j. **MONITORING:** The COUNTY shall permit all persons who are duly authorized by CFCHS or the Department of Children and Families to inspect and copy any records, papers, documents, facilities, goods, and services of the COUNTY which are relevant to this Agreement, and to interview any clients, employees, and subcontractor employees of the COUNTY to assure CFCHS of the satisfactory performance of the terms and conditions of this Agreement.

k. **PUBLIC ENTITY CRIMES:** Chapter 287.133(2)(a) states: A person or affiliate who has been placed on the convicted vendor list following a conviction for a public entity crime may not submit a bid on a contract to provide any goods or services to a public entity, may not submit a bid on a contract with a public entity for the construction or repair of a public building or public work, may not submit bids on leases of real property to a public entity, may not be awarded or perform work as a contractor, supplier, subcontractor, or consultant under a contract with any public entity, and may not transact business with any public entity in excess of the threshold amount provided in s.287.017 for CATEGORY TWO for a period of 36 months from the date of being placed on the convicted vendor list.

l. **PUBLIC RECORDS:** The COUNTY shall allow public access to all documents, papers, letters, or other public records as defined in Subsection 119.011(12), F.S. as prescribed by Subsection 119.07(1) F.S., made or received by the COUNTY in conjunction with this Agreement except those public records which are made confidential by law and must be protected from disclosure. It is expressly understood that the COUNTY's failure to comply with this provision

shall constitute an immediate breach of this Agreement for which CFCHS may unilaterally terminate this Agreement.

The COUNTY shall retain all client records, financial records, supporting documents, statistical records and any other documents (including electronic storage media) pertinent to this Agreement for a period of six (6) years after completion of this Agreement or longer when required by law. In the event an audit is required by this Agreement, records shall be retained for a minimum period of six (6) years after the audit report is issued or until resolution of any audit findings or litigation based on the terms of this Agreement.

m. **SCRUTINIZED COMPANIES:** The COUNTY shall refrain from any of the prohibited business activities with the Governments of Sudan and Iran as described in Section 215.473, F.S. Pursuant to Section 287.135(5), F.S., CFCHS will immediately terminate this Agreement for cause if the COUNTY is found to have submitted a false certification or if the COUNTY is placed on the Scrutinized Companies with Activities in Sudan List or the Scrutinized Companies with Activities in the Iran Petroleum Energy Sector List during the term of the Agreement. CFCHS will terminate this Agreement at any time the COUNTY is found to have been placed on the Scrutinized Companies that Boycott Israel List or is engaged in a boycott of Israel.

n. **SPONSORSHIP AND PUBLICITY:** The COUNTY and partners shall, in publicizing, advertising or describing the sponsorship of the program, state: "Sponsored by Central Florida Cares Health System, Inc., and the State of Florida, Department of Children and Families." If the sponsorship reference is in written material, the words "State of Florida, Department of Children and Families" and "Central Florida Cares Health System, Inc." shall appear in the same size letters or type as the name of the organization.

o. **TRAVEL REIMBURSEMENT:** Reimbursement for travel expenses is authorized only when approved in advance by the CFCHS Program Manager and conducted in accordance with s. 112.061, F.S.

p. **USE OF FUNDS FOR LOBBYING PROHIBITED:** The COUNTY agrees to comply with the provisions of section 216.347, Florida Statutes, which the expenditure of contract funds for the purpose of lobbying the Legislature or a state agency.

9. Incorporated Documents:

a. The following Attachments and Guidance Documents, or the latest revisions thereof, are incorporated herein and made a part of this Subcontract:

   i. **Attachment I** – DCF Master Contract GHME1

   ii. **Department of Children and Families Guidance Document 41** – Coordinated Opioid Recovery Network of Addiction Care (CORE Network)

10. Term and Termination

This Agreement shall begin on **April 1, 2024**, and will continue in effect until **JUNE 30, 2025**, at which point it shall terminate, unless the Term is extended or terminated earlier in a written document signed by both parties.

Either Party to this Agreement may terminate this Agreement at any time upon providing fifteen (15) days written notice to the other party.

All remedies including indemnification in **Section 8.f.** Indemnification shall survive termination of this Agreement.

THE PARTIES HERETO by and through their duly authorized representatives, whose signatures appear below, have caused this Agreement to be executed.

CONTRACTOR

Central Florida Cares Health System, Inc.

_____

Signature

Maria Bledsoe, CEO

Date:_____

SUBCONTRACTOR

Signatures on following page

BOARD OF COUNTY COMMISSIONER
ATTEST:

SEMINOLE COUNTY, FLORIDA

By: _____
JAY ZEMBOWER, Chairman

Date: _____

_____
GRANT MALOY
Clerk to the Board of
County Commissioners of
Seminole County, Florida.

For the use and reliance
of Seminole County only.

As authorized for execution by the Board of
County Commissioners at its _____
20_____, regular meeting.

Approved as to form and
legal sufficiency.

_____
County Attorney

Attachments:
Exhibit A – Scope of Services
Exhibit B – Security Agreement (SAMPLE)
Exhibit C – Children & Families Operating Procedures (CFOP-50-2)

SEMINOLE COUNTY
FLORIDA'S NATURAL CHOICE

Exhibit A

Seminole County Coordinated Opioid Response (CORe) Plan

Seminole County is in East Central Florida just north of Orlando. With an estimated population of 478,772 in 2022, 1522 persons per square mile in a 309 square miles area, Seminole County is the thirteenth most populous county in Florida. The county is comprised of seven cities and six unincorporated areas represented by 26 zip codes and 86 census tracts as of the 2010 Decennial Census. 51.2% of the population is female, 20.4% are under 18 year of age, 16.7% are 65 years old and older. Non-Hispanic white residents represent the highest percentage of the population at 56.4%(US Census Bureau). In Seminole County, 11% of the population lives in poverty (US Census Bureau).

The total population in Central Florida has grown by a large margin over the last 10 years. Florida experienced a nearly 12% increase in population between 2010 and 2019, the second-largest increase in population after Texas. Seminole County's population is projected to reach more than 500,000 by the end of 2024. The rapid population growth in Central Florida was identified as one of the top challenges in the qualitative research conducted during the most recent Seminole County Community Health Needs Assessment.

Seminole County seeks to deploy Florida's Coordinated Opioid Response (CORe) addiction care services in collaboration with Central Florida Cares, the local Managing Entity (ME). Seminole County intends to engage services with local area hospitals and community service providers ("Provider") to offer services in alignment with the CORe model program standards. The Seminole County Fire Department Emergency Medical Services (EMS) will provide rescue response services to individuals in need of addiction care. Services will include stabilization and Medication for Opioid Use Disorder (MOUD) induction. Following EMS intervention, area hospital providers will provide treatment to include stabilization, medication assisted treatment, treatment for emergency medical needs and navigation to a long-term treatment provider. Seminole County will engage with community providers to plan for the provision of a continuum of addiction care services post hospital release.

Contracted services shall be provided in an engaging and positive environment and will facilitate access to needed services, ensure appropriateness of care, and promote client satisfaction with services. Services shall be assessment driven and individualized with a focus on evidenced based interventions.

Regional Opioid Settlement Funding funds medical, psychological, and social support services, which include expanding access to Medication for Opioid Use Disorder (MOUD), psychological treatment, counseling services, social support/case management services, and community outreach (collectively referred to as "Services").

The provision of Services shall be for Seminole County Clients who have been diagnosed with an Opioid Use Disorder or co-occurring substance use and mental health disorder.

Eligibility Requirements and Provider Responsibilities

Eligibility

Seminole County, Florida, residents experiencing opioid use disorder (OUD) and co-occurring mental health disorders.

Provider Responsibilities

The Provider shall ensure its compliance with the following:

- The Provider shall ensure that Services are provided by qualified professionals licensed and certified, as applicable, with the State of Florida. Service provider licenses and certifications shall be current and remain valid during the term of this Contract. Copies of Service provider licenses and certifications shall be provided to the County upon request.
- The Provider will support medically at-risk patients with opioid use and/or any other co-occurring substance use disorder/ mental health conditions to obtain, improve, and retain the skills, knowledge, tools, and support they need to recover. The overall project objectives are as follows:
    - Identify individuals who have a substance use disorder and are at the most significant risk of death from overdose
    - Enhance screening of the identified patients utilizing a variety of evidence-based practices,
    - Increase patient access to evidence-based treatment, including MOUD, case management, outreach, and aftercare services.
- The Provider will be responsible for referring patients with opioid use and/or any other co-occurring substance use disorder/ mental health conditions to medical practices that provide Medication for Opioid Use Disorders (MOUD) and mental health therapy. Hospital-based Opioid Navigators will refer clients to Community-Based Opioid Navigators for social support resources and case management.
- The Provider shall provide monthly reports by the sixth (6th) of each month for the previous month, which includes the following information to the Seminole County Community Health Division, which reflects the monthly total of:
    - The number of program referrals received.
    - The number of client evaluations completed.
    - The number of clients engaged in community-based MAT/CBT.
    - The number of clients retained in community-based MAT/CBT.
    - The number of referrals to social support services (self-help groups, job training, transportation).

- The number of clients on active caseloads.
- The number of successful discharges.
- The number of unsuccessful discharges.

Seminole County Government is committed to ongoing performance measurement to ensure quality service provision. Regular and ongoing communication will occur between the County and contracted providers. Providers are expected to regularly communicate with Seminole County regarding any barriers to service provision or changes in service capacity.

Outcome Measures and Indicators: At a minimum, all Service Providers shall adopt the Outcomes and Indicators established by the funding source and/or Department of Children and Family and/or the County.

1. Program data will be collected from several sources to track progress on key performance measures and project objectives.
2. Care coordinators and healthcare providers collect data, and the evaluators may conduct surveys/interviews.
3. All data will be provided to the program evaluators, who will securely manage, clean, and analyze data and prepare reports.

The following page depicts a sample contracted provider scope of service and cost proposal.

SEMINOLE COUNTY
FLORIDA'S NATURAL CHOICE

SCOPE OF SERVICE & COST PROPOSAL

AGENCY NAME:
POINT OF CONTACT:
CONTACT PHONE NUMBER:
CONTACT FAX NUMBER:
CONTACT E-MAIL:

The above agency will provide the following services for the residents of Seminole County during Fiscal Year 2024-2025:

Program Description:

Service	# of Units/Services to be Provided with County Funding	Unit/Service Cost	Total Unit Cost

- Funds may be transferred within the line items with the approval from Seminole County Community Services without an amendment to this Agreement

TOTAL UNIT COST CANNOT EXCEED
THE GRANT AWARD AMOUNT OF $XXX

EXHIBIT B SAMPLE

SECURITY AGREEMENT FORM

The Department of Children and Families has authorized you:

_____
Employee's or Contractor's Name/Organization

to have access to sensitive data using computer-related media (e.g., printed reports, microfiche, system inquiry, on-line update, or any magnetic media).

Computer crimes are a violation of the department's Standards of Conduct. In addition to departmental discipline, committing computer crimes may result in Federal or State felony criminal charges.

I understand that a security violation may result in criminal prosecution according to the provisions of Federal and State statutes and may also result in disciplinary action against me according to the department's Standards of Conduct in the Employee Handbook.

By my signature below, I acknowledge that I have received, read, understand and agree to be bound by the following:

- The Computer Related Crimes Act, Chapter 815, F.S.
- Sections 7213, 7213A, and 7431 of the Internal Revenue Code, which provide civil and criminal penalties for unauthorized inspection or disclosure of Federal tax data.
- 6103(l)(7) of the Internal Revenue Code, which provides confidentiality and disclosure of returns and return information.
- CFOP 50-2.
- It is the policy of the Department of Children and Families that no contract employee shall have access to IRS tax information or FDLE information, unless approved in writing, by name and position to access specified information, as authorized by regulation and/or statute.
- It is the policy of the Department of Children and Families that I do not disclose personal passwords.
- It is the policy of the Department of Children and Families that I do not obtain information for my own or another person's personal use.
- I will only access or view information or data for which I am authorized and have a legitimate business reason to see when performing my duties. I shall maintain the integrity of all confidential and sensitive information accessed.
- "Casual viewing" of employee or client data, even data that is not confidential or otherwise exempt from disclosure as a public record, constitutes misuse of access and is not acceptable.
- The Department of Children and Families will perform regular database queries to identify misuse of access.
- Chapter 119.0712, Florida Statutes, and the Driver Privacy Protection Act (DPPA).

PRIVACY ACT STATEMENT: Disclosure of your social security number is voluntary, but must be provided in order to gain access to department systems. It is requested, however, pursuant to Section 282.318, Florida Statutes, the Security of Data and Information Technology Resources Act. The Department requests social security numbers to ensure secure access to data systems, prevent unauthorized access to confidential and sensitive information collected and stored by the Department, and provide a unique identifier in our systems.

Print Employee/Contractor Name	Signature of Employee/Contractor	Date
Print Supervisor Name	Signature of Supervisor	Date

CHAPTER 815: COMPUTER-RELATED CRIMES

815.01 Short title. The provisions of this act shall be known and may be cited as the "Florida Computer Crimes Act."
(History: s. 1, ch. 78-92.)

815.02 Legislative intent. The Legislature finds and declares that:
(1) Computer-related crime is a growing problem in government as well as in the private sector.
(2) Computer-related crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime.
(3) The opportunities for computer-related crimes in financial institutions, government programs, government records, and other business enterprises through the introduction of fraudulent records into a computer system, the unauthorized use of computer facilities, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great.
(4) While various forms of computer crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which proscribes various forms of computer abuse.
(History: s. 1, ch. 78-92.)

815.03 Definitions. As used in this chapter, unless the context clearly indicates otherwise:
(1) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.
(2) "Computer" means an internally programmed, automatic device that performs data processing.
(3) "Computer contaminant" means any set of computer instructions designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. The term includes, but is not limited to, a group of computer instructions commonly called viruses or worms which are self-replicating or self-propagating and which are designed to contaminant other computer programs or computer data; consume computer resources; modify, destroy, record, or transmit data; or in some other fashion usurp the normal operation of the computer, computer system, or computer network.
(4) "Computer network" means any system that provides communications between one or more computer systems and its input or output devices, including, but not limited to, display terminals and printers that are connected by telecommunication facilities.
(5) "Computer program or computer software" means a set of instructions or statements and related data which, when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.
(6) "Computer services" include, but are not limited to, computer time; data processing or storage functions; or other uses of a computer, computer system, or computer network.
(7) "Computer system" means a device or collection of devices, including support devices, one or more of which contain computer programs, electronic instructions, or input data and output data, and which perform functions, including, but not limited to, logic, arithmetic, data storage, retrieval, communication, or control. The term does not include calculators that are not programmable and that are not capable of being used in conjunction with external files.
(8) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs, or instructions. Data may be in any form, in storage media or stored in the memory of the computer, or in transit or presented on a display device.
(9) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.
(10) "Intellectual property" means data, including programs.
(11) "Property" means anything of value as defined in [Footnote 1] s. 812.011 and includes, but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in either machine-readable or human-readable form, and any other tangible or intangible item of value.
(History: s. 1, ch. 78-92; s. 9, ch. 2001-54.) ([Footnote 1] Note: Repealed by s. 16, ch. 77-342.)

815.04 Offenses against intellectual property; public records exemption.
(1) Whoever willfully, knowingly, and without authorization modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.
(2) Whoever willfully, knowingly, and without authorization destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.
(3) (a) Data, programs, or supporting documentation which is a trade secret as defined in s. 812.081 which resides or exists internal or external to a computer, computer system, or computer network which is held by an agency as defined in chapter 119 is confidential and exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution. (b) Whoever willfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation which is a trade secret as defined in s. 812.081 or is confidential as provided by law residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.
(4) (a) Except as otherwise provided in this subsection, an offense against intellectual property is a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084. (b) If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.
(History: s. 1, ch. 78-92; s. 1, ch. 94-100; s. 431, ch. 96-406.)

815.045 Trade secret information. The Legislature finds that it is a public necessity that trade secret information as defined in s. 812.081, and as provided for in s. 815.04(3), be expressly made confidential and exempt from the public records law because it is a felony to disclose such records. Due to the legal uncertainty as to whether a public employee would be protected from a felony conviction if otherwise complying with chapter 119, and with s. 24(a), Art. I of the State Constitution, it is imperative that a public records exemption be created. The Legislature in making disclosure of trade secrets a crime has clearly established the importance attached to trade secret protection. Disclosing trade secrets in an agency's possession would negatively impact the business interests of those providing an agency such trade secrets by damaging them in the marketplace, and those entities and individuals disclosing such trade secrets would hesitate to cooperate with that agency, which would impair the effective and efficient administration of governmental functions. Thus, the public and private harm in disclosing trade secrets significantly outweighs any public benefit derived from disclosure, and the public's ability to scrutinize and monitor agency action is not diminished by nondisclosure of trade secrets. (History: s. 2, ch. 94-100.) (Note. Former s. 119.165)

815.06 Offenses against computer users.
(1) Whoever willfully, knowingly, and without authorization: (a) Accesses or causes to be accessed any computer, computer system, or computer network; (b) Disrupts or denies or causes the denial of computer system services to an authorized user of such computer system

services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another; (c) Destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; (d) Destroys, injures, or damages any computer, computer system, or computer network; or (e) Introduces any computer contaminant into any computer, computer system, or computer network, commits an offense against computer users.

(2) (a) Except as provided in paragraphs (b) and (c), whoever violates subsection (1) commits a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084. (b) Whoever violates subsection (1) and: 1. Damages a computer, computer equipment, computer supplies, a computer system, or a computer network, and the monetary damage or loss incurred as a result of the violation is $5,000 or greater; 2. Commits the offense for the purpose of devising or executing any scheme or artifice to defraud or obtain property; or 3. Interrupts or impairs a governmental operation or public communication, transportation, or supply of water, gas, or other public service, commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084. (c) Whoever violates subsection (1) and the violation endangers human life commits a felony of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(3) Whoever willingly, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network commits a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.

(4) (a) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, computer equipment, computer supplies, or computer data may bring a civil action against any person convicted under this section for compensatory damages. (b) In any action brought under this subsection, the court may award reasonable attorney fees to the prevailing party.

(5) Any computer, computer system, computer network, computer software, or computer data owned by a defendant which is used during the commission of any violation of this section or any computer owned by the defendant which is used as a repository for the storage of software or data obtained in violation of this section is subject to forfeiture as provided under ss. 932.701 – 932.704.

(6) This section does not apply to any person who accesses his or her employer's computer system, computer network, computer program, or computer data when acting within the scope of his or her lawful employment.

(7) For purposes of bringing a civil or criminal action under this section, a person who causes, by any means, the access to a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in both jurisdictions.

(History: s. 1, ch. 78-92; s. 11, ch. 2001-54.)

815.07 This chapter not exclusive. The provisions of this chapter shall not be construed to preclude the applicability of any other provision of the criminal law of this state which presently applies or may in the future apply to any transaction which violates this chapter, unless such provision is inconsistent with the terms of this chapter. (History: s. 1, ch. 78-92.)

SECTION 7213 – UNAUTHORIZED DISCLOSURE OF INFORMATION

(a) RETURNS AND RETURN INFORMATION -

(1) FEDERAL EMPLOYEES AND OTHER PERSONS – It shall be unlawful for any officer or employee of the United States or any person described in section 6103(n)(or an officer or employee of any such person),or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)]. Any violation of this paragraph shall be a felony punishable upon conviction by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.

(2) STATE AND OTHER EMPLOYEES – It shall be unlawful for any person [not described in paragraph (1)] willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)] acquired by him or another person under subsection (d),(i)(3)(B)(i),(1)(6),(7),(8),(9),(10),(12),(15) or (16) or (m)(2),(4),(5),(6), or (7) of section 6103. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(3) OTHER PERSONS – It shall be unlawful for any person to whom any return or return information [as defined in section 6103(b)] is disclosed in an manner unauthorized by this title thereafter willfully to print or publish in any manner not provided by law any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(4) SOLICITATION – It shall be unlawful for any person willfully to offer any item of material value in exchange for any return or return information [as defined in 6103(b)] and to receive as a result of such solicitation any such return or return information. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(5) SHAREHOLDERS – It shall be unlawful for any person to whom return or return information [as defined in 6103(b)] is disclosed pursuant to the provisions of 6103((e)(1)(D)(iii) willfully to disclose such return or return information in any manner not provided by law. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

SECTION 7213A – UNAUTHORIZED INSPECTION OF RETURNS OR RETURN INFORMATION

(a) PROHIBITIONS –

(1) FEDERAL EMPLOYEES AND OTHER PERSONS – It shall be unlawful for-

(A) any officer or employee of the United States, or

(B) any person described in section 6103(n) or an officer willfully to inspect, except as authorized in this title, any return or return information.

(2) STATE AND OTHER EMPLOYEES – It shall be unlawful for any person [not described in paragraph(l)] willfully to inspect, except as authorized by this title, any return information acquired by such person or another person under a provision of section 6103 referred to in section 7213(a)(2).

(b) PENALTY –

(1) IN GENERAL – Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding $1000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.

(2) FEDERAL OFFICERS OR EMPLOYEES – An officer or employee of the United States who is convicted of any violation of subsection (a) shall, in addition to any other punishment, be dismissed from office or discharged from employment.

(c) DEFINITIONS – For purposes of this section, the terms "inspect", "return", and "return information" have respective meanings given such terms by section 6103(b).

SECTION 7431 – CIVIL DAMAGES FOR UNAUTHORIZED DISCLOSURE OF RETURNS AND RETURN INFORMATION

(a) IN GENERAL –

(1) INSPECTION OR DISCLOSURE BY EMPLOYEE OF UNITED STATES – If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United States in a district court of the United States.

(2) INSPECTION OR DISCLOSURE BY A PERSON WHO IS NOT AN EMPLOYEE OF THE UNITED STATES – If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against such person in a district court of the United States.

(b) EXCEPTIONS – No liability shall arise under this section with respect to any inspection or disclosure -

(1) which results from good faith, but erroneous, interpretation of section 6103, or

(2) which is requested by the taxpayer.

(c) DAMAGES – In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of-

(1) the greater of –

(A) $1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or

(B) the sum of:

(i) the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus

(ii) in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus

(2) the cost of the action.

(d) PERIOD FOR BRINGING ACTION – Notwithstanding any other provision of law, an action to enforce any liability created under this section may be brought, without regard to the amount in controversy, at any time within 2 years after the date of discovery by the plaintiff of the unauthorized inspection or disclosure.

SECTION 6103 – CONFIDENTIALITY AND DISCLOSURE OF RETURNS AND RETURN INFORMATION

(l) DISCLOSURE OF RETURNS AND RETURN INFORMATION FOR PURPOSES OTHER THAN TAX ADMINISTRATION

(7) Disclosure of return information to Federal, State, and local agencies administering certain programs under the Social Security Act, the Food Stamp Act of 1977, or title 38, United States Code, or certain housing assistance programs

(A) Return information from Social Security Administration – The Commissioner of Social Security shall, upon written request, disclose return information from returns with respect to net earnings from self-employment (as defined in section 1402), wages (as defined in section 3121 (a) or 3401 (a)), and payments of retirement income, which have been disclosed to the Social Security Administration as provided by paragraph (1) or (5) of this subsection, to any Federal, State, or local agency administering a program listed in subparagraph (D).

(B) Return information from Internal Revenue Service – The Secretary shall, upon written request, disclose current return information from returns with respect to unearned income from the Internal Revenue Service files to any Federal, State, or local agency administering a program listed in subparagraph (D).

(C) Restriction on disclosure – The Commissioner of Social Security and the Secretary shall disclose return information under subparagraphs (A) and (B) only for purposes of, and to the extent necessary in, determining eligibility for, or the correct amount of, benefits under a program listed in subparagraph (D).

(D) Programs to which rule applies – The programs to which this paragraph applies are:

(i) a State program funded under part A of title IV of the Social Security Act;

(ii) medical assistance provided under a State plan approved under title XIX of the Social Security Act or subsidies provided under section 1860D–14 of such Act;

(iii) supplemental security income benefits provided under title XVI of the Social Security Act, and federally administered supplementary payments of the type described in section 1616(a) of such Act (including payments pursuant to an agreement entered into under section 212(a) of Public Law 93–66);

(iv) any benefits provided under a State plan approved under title I, X, XIV, or XVI of the Social Security Act (as those titles apply to Puerto Rico, Guam, and the Virgin islands);

(v) unemployment compensation provided under a State law described in section 3304 of this title;

(vi) assistance provided under the Food Stamp Act of 1977;

(vii) State-administered supplementary payments of the type described in section 1616(a) of the Social Security Act (including payments pursuant to an agreement entered into under section 212(a) of Public Law 93–66);

(viii)

(I) any needs-based pension provided under chapter 15 of title 38, United States Code, or under any other law administered by the Secretary of Veterans Affairs;

(II) parents' dependency and indemnity compensation provided under section 1315 of title 38, United States Code;

(III) health-care services furnished under section 1710(a)(1)(I), 1710(a)(2), 1710(b), and 1712(a)(2)(B) of such title; and

(IV) compensation paid under chapter 11 of title 38, United States Code, at the 100 percent rate based solely on unemployability and without regard to the fact that the disability or disabilities are not rated as 100 percent disabling under the rating schedule; and

(ix) any housing assistance program administered by the Department of Housing and Urban Development that involves initial and periodic review of an applicant's or participant's income, except that return information may be disclosed under this clause only on written request by the Secretary of Housing and Urban Development and only for use by officers and employees of the Department of Housing and Urban Development with respect to applicants for and participants in such programs.

Only return information from returns with respect to net earnings from self-employment and wages may be disclosed under this paragraph for use with respect to any program described in clause (viii)(IV). Clause (viii) shall not apply after September 30, 2008.

DRIVER PRIVACY PROTECTION ACT (DPPA)

Under state law, motor vehicle, driver license, and vehicular crash records are subject to public disclosure. The Driver Privacy Protection Act (DPPA) keeps your personal information private by limiting who has access to the information. (http://www.flhsmv.gov/ddl/DPPAInfo.html)

119.0712 Executive branch agency-specific exemptions from inspection or copying of public records.
(2) DEPARTMENT OF HIGHWAY SAFETY AND MOTOR VEHICLES.

(a) Personal information contained in a motor vehicle record that identifies an individual is confidential and exempt from s. 119.07(1) and s. 24(a), Art. I of the State Constitution except as provided in this subsection. Personal information includes, but is not limited to, an individual's social security number, driver identification number or identification card number, name, address, telephone number, medical or disability information, and emergency contact information. For purposes of this subsection, personal information does not include information relating to vehicular crashes, driving violations, and driver's status. For purposes of this subsection, the term "motor vehicle record" means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by the Department of Highway Safety and Motor Vehicles.

(b) Personal information contained in motor vehicle records made confidential and exempt by this subsection may be released by the department for any of the following uses:

1. For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles and dealers by motor vehicle manufacturers; and removal of nonowner records from the original owner records of motor vehicle manufacturers, to carry out the purposes of Titles I and IV of the Anti Car Theft Act of 1992, the Automobile Information Disclosure Act (15 U.S.C. ss. 1231 et seq.), the Clean Air Act (42 U.S.C. ss. 7401 et seq.), and chapters 301, 305, and 321-331 of Title 49, United States Code.
2. For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a federal, state, or local agency in carrying out its functions.
3. For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts, and dealers; motor vehicle market research activities, including survey research; and removal of nonowner records from the original owner records of motor vehicle manufacturers.
4. For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only:
   a. To verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and
   b. If such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.
5. For use in connection with any civil, criminal, administrative, or arbitral proceeding in any court or agency or before any self-regulatory body for:
   a. Service of process by any certified process server, special process server, or other person authorized to serve process in this state.
   b. Investigation in anticipation of litigation by an attorney licensed to practice law in this state or the agent of the attorney; however, the information may not be used for mass commercial solicitation of clients for litigation against motor vehicle dealers.
   c. Investigation by any person in connection with any filed proceeding; however, the information may not be used for mass commercial solicitation of clients for litigation against motor vehicle dealers.
   d. Execution or enforcement of judgments and orders.
   e. Compliance with an order of any court.
6. For use in research activities and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals.
7. For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, anti-fraud activities, rating, or underwriting.
8. For use in providing notice to the owners of towed or impounded vehicles.
9. For use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection. Personal information obtained based on an exempt driver's record may not be provided to a client who cannot demonstrate a need based on a police report, court order, or business or personal relationship with the subject of the investigation.
10. For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under 49 U.S.C. ss. 31301 et seq.
11. For use in connection with the operation of private toll transportation facilities.
12. For bulk distribution for surveys, marketing, or solicitations when the department has obtained the express consent of the person to whom such personal information pertains.
13. For any use if the requesting person demonstrates that he or she has obtained the written consent of the person who is the subject of the motor vehicle record.
14. For any other use specifically authorized by state law, if such use is related to the operation of a motor vehicle or public safety.
15. For any other use if the person to whom the information pertains has given express consent in a format prescribed by the department. Such consent shall remain in effect until it is revoked by the person on a form prescribed by the department.

(c) Notwithstanding paragraph (b), without the express consent of the person to whom such information applies, the following information contained in motor vehicle records may only be released as specified in this paragraph:

1. Social security numbers may be released only as provided in subparagraphs (b)2., 5., 7., and 10.
2. An individual's photograph or image may be released only as provided in s. 322.142.
3. Medical disability information may be released only as provided in ss. 322.125 and 322.126.
4. Emergency contact information may be released only to law enforcement agencies for purposes of contacting those listed in the event of an emergency.

(d) The restrictions on disclosure of personal information provided by this subsection shall not in any way affect the use of organ donation information on individual driver licenses or affect the administration of organ donation initiatives in this state.

(e)1. Personal information made confidential and exempt may be disclosed by the Department of Highway Safety and Motor Vehicles to an individual, firm, corporation, or similar business entity whose primary business interest is to resell or redisclose the personal information to persons who are authorized to receive such information. Prior to the department's disclosure of personal information, such individual, firm, corporation, or similar business entity must first enter into a contract with the department regarding the care, custody, and control of the personal information to ensure compliance with the federal Driver's Privacy Protection Act of 1994 and applicable state laws.

2. An authorized recipient of personal information contained in a motor vehicle record, except a recipient under subparagraph (b)12., may contract with the Department of Highway Safety and Motor Vehicles to resell or redisclose the information for any use permitted under this section. However, only authorized recipients of personal information under subparagraph (b)12. may resell or redisclose personal information pursuant to subparagraph (b)12.

3. Any authorized recipient who resells or rediscloses personal information shall maintain, for a period of 5 years, records identifying each person or entity that receives the personal information and the permitted purpose for which it will be used. Such records shall be made available for inspection upon request by the department.

(f) The department may adopt rules to carry out the purposes of this subsection and the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. ss. 2721 et seq. Rules adopted by the department may provide for the payment of applicable fees and, prior to the disclosure of personal information pursuant to this subsection, may require the meeting of conditions by the requesting person for the purposes of obtaining reasonable assurance concerning the identity of such requesting person, and, to the extent required, assurance that the use will be only as authorized or that the consent of the person who is the subject of the personal information has been obtained. Such conditions may include, but need not be limited to, the making and filing of a written application in such form and containing such information and certification requirements as the department requires.

(g) This subsection is subject to the Open Government Sunset Review Act in accordance with s. 119.15 and shall stand repealed October 2, 2012, unless reviewed and saved from repeal through reenactment by the Legislature

CF OPERATING PROCEDURE
NO. 50-2

STATE OF FLORIDA
DEPARTMENT OF CHILDREN AND FAMILIES
TALLAHASSEE, November 3, 2023

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 2-1(b) and 2-1(c) established the timeframe to deactivate system user's account when access is no longer appropriate and added Chapter 5, Patching and Reboot of Information Technology Resources to describe the Department's current policy and procedures.

This operating procedure supersedes CFOP 50-2, dated June 22, 2023.
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. 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 by typing **encrypt** in the email 'Subject' line. 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.

2-4. 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.