State of Florida

People First System
Security Guidelines Manual

Updated: March 2024

Section 1 **Overview**	This document is consistent with industry best practices and provides guidelines for state agencies to maintain the security and confidentiality of data within the People First system. It includes data security procedures, background reviews and privacy disclosure statements. Use this manual in conjunction with the standards established in Rule Chapter 60GG-2 (Information Technology Standards), Florida Administrative Code (F.A.C.) and Florida Statute (F.S.) 501.171 (Florida Information Protection Act of 2014). Employee data is a valuable asset that must be protected from unauthorized access, modification, destruction, or disclosure, whether accidental or intentional. Take prudent business measures when managing data in the People First system to protect it. Consistent with industry security standards, limit access to People First users as outlined in the Security Role Code Definitions and Assignments guideline described in Section 6 and Exhibit 3. Violations of these guidelines may result in disciplinary action including dismissal and/or possible legal action.

Section 2 **Key Definitions**	**Covered Entity:** The Health Insurance Portability and Accountability Act of 1996 (HIPAA), defines a covered entity as all health plans (e.g., health insurance companies, HMOs, Medicare and Medicaid), all health care clearinghouses (e.g., entities who translate and interpret billing information) and health care providers electronically transmitting certain health transactions (e.g., claims, eligibility, referrals, claims status). The entities must comply with its administrative rules and regulations. **Custodian of an Information Resource**: Guardian or caretaker; the holder of data; the agent charged with the resource owner's requirements for processing, communications, protection controls, access controls, and output distribution for the resource; a person responsible for implementing owner-defined controls and access to an information source. The custodian is normally a provider of services. **Data**: A representation of facts or concepts in an organized manner that may be stored, communicated, interpreted, or processed by people or automated means. **Florida Criminal Information Center (FCIC) background check:** An inquiry to identify violation(s) of law resulting from arrests and charges by law enforcement officers in the State of Florida. Referred to as a Level I Background Check in this document. **Guideline**: A recommended process intended to provide uniformity to the implementation of policies, procedures and standards. **National Criminal Information Center (NCIC) background check:** An inquiry using fingerprints to check national criminal records of the Federal Bureau of Investigation to identify violation(s) of law resulting from arrests

	and charges made by law enforcement officials in the United States. Referred to as a Level II Background Check in this document. **People First System:** The State of Florida's self-service, secure, Web-based application and enterprise-wide suite of human resource services. People First system services include those accessed through the Interactive Voice Response (IVR) system and the service center in Tallahassee, Florida. **Security Role Code:** A defined code used to determine the level of access a user has to the People First system. Throughout this document, the Security Role Code will also be referred to as Role Code and is considered to have the same meaning as security role code. **Security Standard**: A set of practices and rules that specify or regulate how a system or organization provides security services. **Special Trust or Position of Trust:** A position or physical location in which an individual can view or alter confidential information or is depended upon for continuity of information resources imperative to the operations of the agency and its mission. **Vendor:** A non-State of Florida employee contracted by an agency to perform certain HR duties in the People First system. They are usually hired to enter and update certain miscellaneous deduction codes on agency employees.

Section 3 **Department of Management Services Responsibilities**	The Department of Management Services (DMS) manages the People First system. Keeping data secure is a collaborative effort. The goal is to help agencies protect and safeguard information about their employees. The DMS People First Division is committed to system security through the following tasks: • Provide direction on how People First role codes will be assigned. • Provide direction on employee responsibilities to access and protect People First employee and work data. • Provide direction on when to conduct employee background checks. • Work with the Service Provider to maintain the People First Security Plan. • Perform random audits of state employees who have accessed People First data. • Perform random audits of NorthgateArinso (NGA) employees who have accessed People First data. • Assist agencies in performing audits and investigations of suspected People First security violations.

Section 4	This section identifies agency responsibilities with regard to People First system security:
Agency Responsibilities	**Agency Human Resource Offices** • Implement and administer the role code assignment guideline. • Implement and administer the employee security guideline. • Implement and administer the employee background check guideline. • Assist the People First Division with performing system security audits. • Provide information security awareness training to employees. • Provide specialized training for employees who view or manage confidential information. • Maintain records of individuals who have completed security awareness training. **General System Access** This guideline is used to make agencies aware of their responsibility to protect data. Agencies existing data security policies and data security acknowledgement forms should reference and cover the People First system and its data. The 'Sample Policy Letter to Applicable Employees' (Exhibit 1) and the 'Sample Acknowledgement of Policy Concerning Employee Responsibilities when Accessing and Protecting People First Data' (Exhibit 2) should be incorporated into agencies existing data security policies and data security acknowledgement forms. Agency employees who have access to view or update other employees' data within the People First system should be required to read agency data security policies and sign agency data security acknowledgment forms. Agency data security acknowledgement forms should be kept in the employee's personnel file. **Passwords** A People First password is personal; keep it private. Never write passwords down or share with other individuals. Do not store passwords in a personal computer or laptop. Log out or use a password-locked screensaver to block the normal display of an employee's monitor. Passwords must be changed every 90 days. Users should report any suspected password breaches. **Confidential Data** Keep confidential data accessible only to authorized individuals. Use due diligence to protect confidential data. Confidential data should not be sent through email. **Benefits Access** Although a particular agency may not meet the definition of a Covered Entity, it has access to protected health information (PHI) that is covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Agencies should train employees on HIPAA to ensure employees understand their responsibilities when accessing PHI, producing reports or creating data files. **Data Warehouse Access** Agencies should be aware that employees with access to the People First Data Warehouse can extract agency-wide data, including data that may be considered sensitive and/or confidential (e.g., Social Security numbers, home

addresses). Agencies should train employees on public record laws, including Chapter 119, Florida Statutes (F.S.). Agencies should ensure employees with access to the People First Data Warehouse are in a Position of Trust. The DMS recommends that the agency process a Level II Background Check on these individuals every five years. It is recommended that the following statement be used on all reports: *"This report may contain information that is confidential under state or federal law. Improper access or release of such information may be a violation of these laws."*

Process for requesting People First Data Warehouse access:

- The agency will download the People First Data Warehouse Authorization Form from the following link: https://www.dms.myflorida.com/content/download/115340/636849
- Complete the form and email it to PeopleFirstDataWarehouse@dms.fl.gov.
- Once the update is completed, the People First Data Warehouse team will notify the requesting agency via email.

  Note: Forms must be submitted for updating and deleting access to the People First Data Warehouse when the employee's role changes within an agency. For a separation from the agency, the employee's access is systematically revoked once the separation action is completed in the People First system and no "delete access" request needs to be submitted.

Learning Management System (LMS) Access
Agencies should be aware that system Administrator and Trainer access must be granted and removed by the People First Division. Access to agency specific information will remain with an employee, should they move to another position or agency, as it is not tied to their position.

Process for requesting People First LMS access:

- The agency delegated authority will download the People First Learning Management Authorization Form from the following link: https://www.dms.myflorida.com/content/download/146986/979626
- Complete the form and email it to PeopleFirstTalentManagement@dms.fl.gov.
- Once the update is completed, the People First Talent Management team will notify the requesting agency via email.

Security Violations
To report any security violation, suspected security violation, or to request audits of employees and their access, contact the DMS People First Data Integrity & Security Lead at (850) 487-3443.

Section 5	This section identifies agency employees' responsibilities with regard to People First system security:
Employee Responsibilities	**General System Access** This guideline is used to make employees aware of their responsibility to protect data. **Passwords** A People First password is personal; keep it private. Never write passwords down or share with other individuals. Do not store passwords in a personal computer or laptop. Log out or use a password-locked screensaver to block the normal display of an employee's monitor. Passwords must be changed every 90 days. Users should report any suspected password breaches. **Confidential Data** Keep confidential data accessible only to authorized individuals. Use due diligence to protect confidential information. Confidential data should not be sent through email. **Benefits Access** Although a particular agency may not meet the definition of a Covered Entity, it has access to protected health information (PHI) data that is covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Employees should understand their responsibilities when accessing PHI data, producing reports or creating data files. **Data Warehouse Access** Employees with access to the People First Data Warehouse can extract agency-wide data, including data that may be considered sensitive and/or confidential (e.g., Social Security numbers, home addresses). It is recommended that the following statement be used on reports: "This report may contain information that is confidential under state or federal law. Improper access or release of such information may be a violation of these laws."

Section 6	All agencies and entities using the People First system should use the following procedures and guidelines when assigning People First security role codes.
People First Security Role Code Assignment	**Design of Security Role Codes** The security role codes within the People First system are designed to limit access to data based on the employee's work responsibilities. The current security role codes are defined in Security Role Code Definitions and Assignments (Exhibit 3). **Policy for the Assignment of Security Role Codes** The proper assignment of People First security role codes is critical in maintaining data security and segregation of duties. When assigning role codes, agencies should review the employee's position description and assign the role codes based on the stated job responsibilities.

	Agencies should record the assigned role code on the employee's position description. In addition to the employee's job responsibilities, use the guidelines and descriptions in Security Role Code Definitions and Assignments (Exhibit 3) when assigning People First role codes.

Section 7 **Employee Background Checks**	The Employee Background Check Guideline (Exhibit 4) describes the agencies' responsibilities to conduct employee background checks for employees who access the People First system. All agencies should follow this guideline.

Section 8 **People First Auditing**	This section defines the types of audits that the DMS People First Division will conduct with regard to People First system security: **Audit of People First Service Center Employee's Access to People First Data** The following policy addresses audits of People First Service Center employees who access State of Florida employee data within the People First system. **Policy** On a monthly basis, the DMS People First Division reviews access audit reports generated from the People First system. The audit reports identify the People First system information types (info types) accessed. These reports are reviewed to determine if the data viewed was consistent with the service center employee's job duties and the People First Next Generation contract, with special attention being paid to accessing an employee's personal or address information. If unusual access patterns are discovered, the DMS People First Division consults with NGA Management. **Audit of Authorized Agency Users' Access to People First Data** The following policy addresses audits of agency employees who access other employee data within the People First system. **Policy** On a monthly basis, the DMS People First Division reviews access audit reports generated from the People First system. The audit reports identify the People First system information types (info types) accessed. These reports are reviewed to determine if the data viewed was consistent with the People First System Security Guidelines Manual. If unusual access patterns are discovered, the DMS People First Division consults with the appropriate agency human resource officer.

Exhibit 1

Sample Policy Letter to Applicable Employees

Employee Responsibilities when Accessing and Protecting People First Data

The People First system enables employees to record time, request leave, make insurance benefit elections, maintain their contact information and other employee related information for most employees. All personnel who have access to this information are responsible for ensuring that they only access employee data for a legitimate business purpose, and that they maintain the integrity of any confidential information accessed. For purposes of this policy, confidential information, records or data means that information exempted from disclosure as a public record as provided in Chapter 119, F.S. or other state or federal law. Examples of confidential information include personal addresses, bank information (which is only accessible by the employee), SSNs, medical information.

Employees should only view information or data they have a legitimate business reason for accessing in the performance of their duties. The "casual viewing" of employee data constitutes misuse of access and is not tolerated. Database queries are performed on a regular basis to identify misuse of the People First system. Any violations of this policy are subject to disciplinary action (e.g., suspension, termination or possible legal action).

Properly destroy any documents or records no longer needed. Consult the State of Florida retention guidelines, as published in Department of State Schedule GS1-SL and Rule Chapter 60GG-2, F.A.C., before disposing of any document, hardware, or electronic media or device.

Exhibit 2

To assist agencies in ensuring that all employees and Other Personal Services (OPS) personnel are familiar with this policy, attached is a sample acknowledgement form to be signed and returned to agency managers. Each manager is responsible for including a copy of this signed form in the employee's personnel file.

Sample Acknowledgement of Policy Concerning Employee Responsibilities when Accessing and Protecting People First Data

I have received, read and understand the letter that addresses "**Employee Responsibilities when Accessing and Protecting People First Data**"

Employee Signature: _____

Date: _____

Supervisor's Signature: _____

Date: _____

Note: You must include a completed and signed copy of this form in the employee's personnel file.

Exhibit 3

Security Role Code Definitions and Assignments

For detailed information on all role codes and their use in the People First system, click here to review the People First Security Role Code Definitions. The document is also available at https://www.dms.myflorida.com/workforce_operations/people_first/for_state_hr_practitioners/hr_professional_user_guide, located under Section I: General System.

Important Information for Security Role Code assignments:

- Any employee receiving any role code other than 'E' must have a defined business need to receive the higher role code (code other than 'E').
- Only employees can access their Direct Deposit information. None of the higher role codes have access to view Direct Deposit information for anyone other than themselves.
- All higher role codes allow Manager Self Service functions for their Direct Reports, including the ability to create and view Personnel Action Requests.

Process for requesting Security Role Code assignments to allow statewide inquiry access for FTE employees (This applies only to Role Codes 'A', 'X', 'Y' and 'Z'):

- The agency human resource officer (or designee) will send an email to the DMS People First Project Administrator and copy the DMS People First Data Integrity & Security Lead, requesting the desired statewide role code to be assigned. The email will identify the employee's name, appointment ID, position number and the reason for the level of access being requested.

- If the request is approved, the DMS People First Project Administrator will email the agency human resource officer (or designee) notifying them of the approval. The DMS People First Data Integrity & Security Lead will be copied on the email to make the requested change.

- The DMS People First Data Integrity & Security Lead will make the requested role code change in the system and email the agency human resource officer (or designee) when the update is complete. The DMS People First Project Administrator will also be copied on this email.

- The following standard language will be included in the notification email to the requesting agency and will serve as a reminder to the agency to conduct the required background check for the requested role code assignment: *"As this role code allows an employee to cross agency boundaries, DMS requires that the employee complete a Level II Background Check. Periodic random audits are performed on role codes with statewide access to ensure compliance with the People First System Security Guidelines Manual."*

Exhibit 4

Employee Background Check Guideline

Purpose

To provide a guideline for required employee background investigations for employees assigned specific People First security role codes. It does not supersede the provisions established in Sections 110.1127 F.S., 282.318 F.S., and 435.04(1) F.S., and rule 60GG-2 (Information Technology Standards), F.A.C.

Scope

Certain positions are designated as Positions of Special Trust, due to their access capability to the state's human resource system. As a result of this designation, these employees are subject to a Level II Background Check as a condition of employment. Additionally, designated contract employees, volunteers and interns in positions or job functions designated as Positions of Special Trust are subject to security background checks in accordance with law.

The DMS People First Division requires that FTE employees who are assigned security role codes that allow access to employee information outside of their respective agencies have a Level II Background Check performed on them at least every five years. This includes the following role codes; 'A', 'F', 'G', 'N', 'S', 'X', 'Y', and 'Z'.

Additionally, the DMS People First Division recommends that agency employees (FTE and OPS) with any HR ('H' and 'U') and HR equivalent ('B', 'C', 'I', 'K', 'R', 'T', 'V') role code allowing access to employee information inside the agency have a Level II Background Check performed on them at least every five years, as well as all agency employees who are granted access to the People First Data Warehouse.

Authority

1. Section 110.1127, F.S., Employee background screening and investigations.
2. Section 282.318, F.S., Security of data and information technology.
3. Section 435.04(1), F.S., Level 2 screening standards.
4. Chapter 60GG-2.002, F.A.C., Identify.
5. Chapter 60GG-2.003, F.A.C., Protect.

Definitions

1. Employee: Any person who has been hired, works for the state and receives a warrant (electronic or paper) from the state for services rendered.
2. Contractor Employee: An individual or entity that contracts directly or indirectly through another contracting entity, with the state to perform a service for a fee.
3. Intern: A student or a graduate of an educational institution with a cooperative agreement with an agency that allows students or graduates to perform duties and receive training.
4. Volunteer: Any person who, of his or her own free will, provides goods or services, or conveys an interest in or otherwise consents to the use of real property to DMS with no monetary or material compensation.
5. Vendor: A person or organization that provides a service or a product to the state including a person or organization that provides software or firmware or documentation to a user for a fee or in exchange for services.

6. Position of Trust or Special Trust: A position or physical location in which an individual can view or alter confidential information or is depended upon for continuity of information resources imperative to the operations of the agency and its mission.
7. Florida Criminal Information Center (FCIC) background check: An inquiry to identify violation(s) of law resulting from arrests and charges by law enforcement officers in the State of Florida.
8. National Criminal Information Center (NCIC) background check: An inquiry using fingerprints to check national criminal records of the Federal Bureau of Investigation to identify violation(s) of law resulting from arrests and charges made by law enforcement officials in the United States.
9. Convicted/Conviction: An adjudication of guilt by a court of competent jurisdiction; a plea of guilty or nolo contendere; a verdict of guilty when adjudication is withheld; or entering into a pretrial intervention program.
10. Provider: Third party such as contractor, vendor, or private organization providing products, services, or support.

Procedures

1. The Secretary (or designee) of an agency may designate positions of special trust regarding access to the People First system subject to a security background check, including fingerprinting, as a condition of employment or contract award.
2. The appropriate agency office will assign in People First all special trust positions either a security check Level I (State of Florida FDLE Background) or Level II (National FBI Background) and maintain a listing of all special trust positions in the Department.
3. All job announcements for positions of special trust will advise job seekers that a background investigation and fingerprinting are conditions of employment. Solicitations for services that involve positions of special trust will advise vendors that a background investigation and fingerprinting will be required for contractor employees.
4. As prescribed by the agency, supervisors review the Candidate Profile prior to an offer of employment to determine whether any potential criminal conviction may disqualify an applicant from employment in a position of special trust. If any criminal convictions are disclosed on the application, the supervisor shall consult with the appropriate office.
5. Upon employment or award of a contract that involves positions of special trust, the supervisor or contract manager shall ensure that, within 30 working days new employees or contractor employees are scheduled for an appointment with the appropriate office to complete necessary forms to initiate the appropriate background check based upon the level of screening established for the position of special trust.
6. As prescribed by the agency, supervisors of employees or contractor employees in positions of special trust shall coordinate, with the appropriate office in their agency the background screening process of current employees, contractor employees and all new hires.
7. Any person who is required to undergo a security background investigation and who refuses to cooperate in such investigation, or refuses to submit fingerprints, shall be disqualified from working in a position of special trust or, if employed, shall be dismissed.

Office of Inspector General (Or Appropriate Office)

1. It is the responsibility of each agency to identify a custodian who will be responsible for maintaining employee background checks.

2. Background investigations or fingerprinting of employees in positions of special trust shall be in accordance with established procedures of the agency and Sections 110.1127 and 435.04, F.S.
3. Background investigations or fingerprinting of state employees shall be conducted at the expense of the agency. The background investigations or fingerprinting of contractor employees shall be paid by the vendor.
4. Background screening records are confidential and not part of an employee's personnel file. Section 110.1127 (2)(d), F.S., does not allow the release of background records for purposes other than screening for employment.
5. The appropriate agency office will conduct reviews of employees identified as having a criminal record. Information will be shared with the applicable senior manager, agency Human Resource Office, and the Office of the General Counsel for consideration of appropriate action.

Disqualifying Information and Granting of Exemptions

1. When background screening indicates criminal history, the agency designee or contract manager in consultation with the appropriate office shall determine whether the convictions would prohibit the employee from working in a position of special trust.
2. Exemptions may be granted by the agency in accordance with the provisions of Chapter 435, F.S.
3. Employees or contractor employees with disqualifying criminal records not granted an exemption shall be removed from a position of special trust in accordance with Statute or the personnel rules.
4. Challenges to disqualification or requests for exemption from disqualification shall be conducted in accordance with the requirements of Chapter 435, F.S.