



State of Florida

People First System Security Guidelines Manual

Updated: September 2009

**State of Florida
People First System Security Guidelines Manual
September 2009**

Section	Topic	Page
1	Overview	3
2	Key Definitions	4
3	Department of Management Services Responsibilities	6
4	Agency Responsibilities	7
5	Employee Responsibilities	9
6	People First Security Role Code Assignment	10
7	Employee Background Checks	11
8	People First Auditing	12
Exhibit 1	Sample Policy Letter and Acknowledgment Form	14
Exhibit 2	Security Role Code Matrix	16
Exhibit 3	Employee Background Check Guideline	21

**State of Florida
People First System Security Guidelines Manual
September 2009**

<p>Section 1</p> <p>Overview</p>	<p>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 60DD-2, Florida Administrative Code (F.A.C.) the Florida Information Resource Security Policies and Standards.</p> <p>Employee data is a valuable asset to protect 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 assignment guideline (see Section 6 and Exhibit 2).</p> <p>Violations of these guidelines may result in disciplinary action including dismissal and/or possible legal action.</p>
--	---

**State of Florida
People First System Security Guidelines Manual
September 2009**

<p align="center">Section 2</p>	<p>Covered Entity: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires 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) to comply with its administrative rules and regulations.</p> <p>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.</p> <p>Data: A representation of facts or concepts in an organized manner that may be stored, communicated, interpreted, or processed by people or automated means.</p> <p>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.</p> <p>Guideline: A recommended process intended to provide uniformity to the implementation of policies, procedures and standards.</p> <p>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.</p> <p>People First System: The State of Florida's self service, secure, Web-based application and enterprise-wide suite of human resource services. The People First system services include those accessed through the Interactive Voice Response (IVR) system and the service centers in Tallahassee, Florida, and Jacksonville, Florida.</p> <p>Security Role Code: A defined code used to determine the type of access a user has to the People First system. Throughout this document, the Security Role Code may also be referred to as Role Code and is considered to have the same meaning as security role code.</p>
<p>Key Definitions</p>	

**State of Florida
People First System Security Guidelines Manual
September 2009**

	<p>Security Standard: A set of practices and rules that specify or regulate how a system or organization provides security services.</p> <p>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.</p>
--	--

**State of Florida
People First System Security Guidelines Manual
September 2009**

<p>Section 3</p> <p>Department of Management Services Responsibilities</p>	<p>Our agency, the Department of Management Services (DMS) manages the People First system. Keeping data secure is a collaborative effort. It's our goal to help you protect and safeguard information about your employees.</p> <p>The People First team is committed to system security through the following tasks:</p> <ul style="list-style-type: none"> • Provide direction on how People First role codes will be assigned. • Provide direction on employee responsibilities to access and protect People First employee 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 Convergys employees who have accessed People First data. • Assist agencies in performing audits and investigations of suspected People First security violations.
--	---

**State of Florida
People First System Security Guidelines Manual
September 2009**

<p>Section 4</p>	<p>This section identifies agency responsibilities with regard to People First system security:</p>
<p>Agency Responsibilities</p>	<p>Agency Personnel Offices</p> <ul style="list-style-type: none"> • 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 team 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. <p>General System Access</p> <p>This guideline is used to make agencies aware of their responsibility to protect data. People First users who view other employees' data within the People First system should receive the policy and sign an acknowledgement form (see Exhibit 1 for sample policy letter and acknowledgment form). Agencies' existing data security policies and acknowledgement forms should reference and cover the People First system and its data. Agencies should maintain the system security acknowledgement form in the employee's personnel file.</p> <p>Passwords</p> <p>Your People First password is personal; keep it private. Never write passwords down or share with other individuals. Do not store your password in your personal computer or laptop. Log out or use a password-locked screensaver to block the normal display of your monitor.</p> <p>Confidential Data</p> <p>Keep confidential data accessible only to authorized individuals. Use due diligence to protect confidential data. Confidential data should be encrypted when sent through e-mail.</p> <p>Benefits Access</p> <p>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 they understand their responsibilities when accessing PHI, producing reports or creating data files.</p> <p>Data Warehouse Access</p> <p>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</p>

**State of Florida
People First System Security Guidelines Manual
September 2009**

	<p>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 three years. 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."</p> <p>Security Violations To report any security violation, suspected security violation, or to request audits of employees and their access, contact the People First Security Officer at (850) 487-3443.</p>
--	--

**State of Florida
People First System Security Guidelines Manual
September 2009**

Section 5	<p>This section identifies agency employees' responsibilities with regard to People First system security:</p>
Employee Responsibilities	<p>General System Access This guideline is used to make employees aware of their responsibility to protect data.</p> <p>Passwords Your People First password is personal; keep it private. Never write passwords down or share with other individuals. Do not store your password in your personal computer or laptop. Log out or use a password-locked screensaver to block the normal display of your monitor.</p> <p>Confidential Data Keep confidential data accessible only to authorized individuals. Use due diligence to protect confidential information. Confidential data should be encrypted when sent through e-mail.</p> <p>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.</p> <p>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."</p>

**State of Florida
People First System Security Guidelines Manual
September 2009**

<p align="center">Section 6</p>	<p>All agencies and entities using the People First system should use the following procedures and guidelines when assigning People First security role codes.</p>
<p align="center">People First Security Role Code Assignment</p>	<p>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 listed in Exhibit 2.</p> <p>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.</p> <p>In addition to the employee's job responsibilities, use the guidelines and descriptions in Exhibit 2 when assigning People First role codes.</p>



**State of Florida
People First System Security Guidelines Manual
September 2009**

Section 7	The Employee Background Check Guideline in Exhibit 3 of this document describes the agencies' responsibilities to conduct employee background checks for employees who access the People First system. All agencies should follow this guideline.
Employee Background Checks	

**State of Florida
People First System Security Guidelines Manual
September 2009**

<p align="center">Section 8</p>	<p>This section defines the types of audits that the People First team will conduct with regard to People First system security:</p>
<p align="center">People First Auditing</p>	<p>Audit of People First Security Role Code Assignments The DMS developed the following policies to audit the assignment of People First role codes to employees. When necessary, agency human resource offices assist with audits.</p> <p>Policy The DMS People First team conducts quarterly reviews of how the People First role codes are assigned. The reviews include a sample of State of Florida employees who have been assigned an A, B, C, D, F, G, H, L, M, R, S, T, V, W, or Z role code.</p> <p>The review ensures role codes were assigned according to guidelines.</p> <p>Audit of Authorized Users' Access to People First Data The following policy addresses audits of employees who access other employee data within the People First system. When necessary, agency human resource offices assist with audits.</p> <p>Policy On a quarterly basis, the DMS People First team reviews access audit reports generated from the People First system. These audit reports describe the People First system information types (info types) accessed.</p> <p>Report 1: This report lists employees who accessed data on a sample of People First users. These reports are reviewed to determine if the data viewed was consistent with the People First Security Guidelines Manual. If unusual access patterns are discovered, the People First team consults with the appropriate agency office.</p> <p>Report 2: This report lists employees who accessed data on select senior management staff. These reports are reviewed to determine if the data viewed was consistent with the People First Security Guidelines Manual. If unusual access patterns are discovered, the People First team consults with the appropriate agency office.</p> <p>Report 3: This report lists employees who accessed data on select key State of Florida employees such as governor, lieutenant governor, chief financial officer, attorney general, and agriculture commissioner and others. These reports are reviewed to determine if the data viewed was consistent with the People First Security</p>

**State of Florida
People First System Security Guidelines Manual
September 2009**

	<p>Guidelines Manual. If unusual access patterns are discovered, the People First team consults with the appropriate agency office.</p> <p>Report 4: This report lists Convergys employees who have accessed data on state employees. These reports are reviewed to determine if the data viewed was consistent with the People First Security Guidelines Manual. If unusual access patterns are discovered, the People First team consults with the appropriate agency office.</p> <p>Report 5: This report lists employees accessed by state employees assigned an A, G, H, or S role code. These reports are reviewed to determine if the data viewed was consistent with the People First Security Guidelines Manual. If unusual access patterns are discovered, the People First team consults with the appropriate agency office.</p>
--	---

**State of Florida
People First System Security Guidelines Manual
September 2009**

Exhibit 1

Sample Policy Letter to Applicable Employees

Employee Responsibilities when Accessing and Protecting People First Employee Data

The People First system enables you to record time worked, leave and other historical information for most employees. Agency 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. Examples of confidential information include personal addresses, bank information, SSN's, medical information, etc.

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 GSI-S and Rule Chapter 60-DD-2, before disposing of any document, hardware, or electronic media or device.



**State of Florida
People First System Security Guidelines Manual
September 2009**

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

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

Employee Signature: _____

Date: _____

Supervisor's Signature: _____

Date: _____

**State of Florida
People First System Security Guidelines Manual
September 2009**

Exhibit 2

SECURITY ROLE CODE MATRIX	
<p>Important Information for Security Role Codes:</p> <ul style="list-style-type: none"> For all role codes (except 'E') the employee receiving the code must have a defined business requirement to receive the code. 	
Security Role Code	Description
A - Agency HR w/ Profiler Access	<p>Assigned only to professional human resources staff. Employees requesting an 'A' role code make a formal request through their personnel officer to the DMS People First Director. When making the request, agencies should include the job functions of the employee(s), the decentralized nature of the human resource office, the organizational unit of the employee(s) for the exception and any other information that may be relevant to the request.</p> <ul style="list-style-type: none"> Maintenance access for all employees in their agency Perform all employee actions for the agency. Maintain organizational and position structures for agency. Perform maintenance functions for Organizational Units, Classes, Broadband and Positions that affect their agency. Access to the staffing module. Maintain Position Security information. No access to employee Direct Deposit data. View-only access to all other agencies' employees. Excludes exempt data (F.S. 119) for other agencies. Limited view of employee data such as pay and benefits statewide.
B - Both Time Administrator and Requisition Manager	<p>Assigned to a "human resources liaison." Generally speaking, a "human resources liaison" assists with filling job requisitions and approving time sheets. There is no limit on the number of assigned 'B' role codes. See descriptions of role codes 'R' and 'T'.</p>
C - Agency Compliance Access & Applicant Profiler	<p>Assigned to staff in the compliance and inspector general offices. There is no limit on the number of assigned 'C' role codes; however, the employee receiving this code must have a defined business requirement that requires the assignment of this code.</p> <ul style="list-style-type: none"> View all employees in their agencies. No access to employee Direct Deposit data. View-only access to the Training, Performance Management, Organizational Management and Time and Payroll modules. View all employee data for the agency except Social Security number (SSN), home address, telephone and dependent data. Access to the staffing module. This security profile can be used for employees with statewide

**State of Florida
People First System Security Guidelines Manual
September 2009**

	<p>access but no direct reports.</p> <ul style="list-style-type: none"> • Manager access for their direct reports' structure. • Perform Personnel Action Requests for their direct reports.
D - Accounting/Payroll	<p>Assigned to staff in the agency budget or accounting office. There is no limit on the number of assigned 'D' role codes.</p> <ul style="list-style-type: none"> • Perform Personnel Action Requests for their direct reports. • Access to Organizational Management.
E - Employee Self Service Only	<p>Default employee role code. It provides access to all employee self service functions.</p> <ul style="list-style-type: none"> • Perform employee self-service functions. • Maintain personal data (e.g., addresses, EEO, W-4, Direct Deposit). • View pay and work details (e.g., work schedule, deductions). • Request leave, view leave balances. • Enter time worked and leave used, and request schedule changes. • Maintain some voluntary deductions. • Search for and apply for jobs. • Maintain dependent information, and enroll in and maintain benefits.
F - BOSP	<p>Assigned only to staff in the Bureau of State Payrolls or the People First team.</p> <ul style="list-style-type: none"> • Statewide view access to most employee data. • Access to pay related data for all state employees (e.g., salary, hourly rate, additives, deductions). • View all employees W-4 and W-5 information. • View position information for payroll purposes (e.g., Overtime indicators, funding). • Perform Personnel Action Requests for their direct reports.
G - Inspector General (Compliance + Applicant Profiler + Chapter 119 Information)	<p>Assigned to staff in the auditor general, inspector general and general counsel offices. There is no limit on the number of assigned 'G' role codes.</p> <ul style="list-style-type: none"> • View all employees in all agencies. • No access to employee Direct Deposit data. • Access to employee exempt data (F.S. 119). • View-only access to the Training, Performance Management, Organizational Management, Staffing and Time and Payroll modules. • View all employee data for the agency including SSN, home address and telephone, and dependent data. • Perform Manager functions for their direct reports. • Perform Personnel Action Requests for their direct reports.
H - Agency HR w/o Profile Access	<p>Assigned to professional human resources staff and liaisons.</p> <ul style="list-style-type: none"> • Maintenance access for all employees in their agency. • Perform all employee actions for agency. • Maintain organizational structure for agency. • Perform maintenance functions for Organizational Units, Classes, Broadband and Positions that affect their agency.

**State of Florida
People First System Security Guidelines Manual
September 2009**

	<ul style="list-style-type: none"> • Access to the staffing module. • Maintain Position Security information. • No access to employee Direct Deposit data. • Cannot view employee's data from other agencies. <p>Note: Department of Health can only view/maintain information for employees within their sub-agency.</p>
L - Supervisor	<p>Assigned to lower level managers with direct reports; however, they do not have a need to create Personnel Action Requests. There is no limit on the number of assigned 'L' role codes.</p> <ul style="list-style-type: none"> • Limited access to all employees that report to them. • No access to employee Direct Deposit data. • No access to employee's pay, deductions or additives. • Access to the Training, Performance Management, Organizational Management and Staffing modules. • Maintain and approve time worked, leave used, leave requests and flex schedule request. • Cannot perform Personnel Action Requests.
M - Manager	<p>Assigned to managers with direct reports and responsible for processing Personnel Action Requests. There is no limit on the number of assigned 'M' role codes.</p> <ul style="list-style-type: none"> • Access to all employees that report to them based on the organizational structure. • No access to employee Direct Deposit data. • Access to the Training, Performance Management, Organizational Management and Staffing modules. • Can perform employee Actions (Appointment, Separation, etc.). • Access to Staffing for their specific requisitions. • Maintain employee data if an employee is unable to. • Maintain and approve time worked, leave used, leave requests and flex schedule request. • Open and close requisitions, and perform all staffing functions. • Perform Personnel Action Requests for their direct reports.
O - Bureau of Accounting	<ul style="list-style-type: none"> • This code is eliminated with the July 2010 system release.
P - Profiler Access	<ul style="list-style-type: none"> • This code is eliminated with the July 2010 system release.
R - Requisition Manager	<p>Assigned to employees who are responsible for the management of advertised positions. There is no limit on the number of assigned 'R' role codes.</p> <ul style="list-style-type: none"> • View the Organization Management module. • No access to employee Direct Deposit data. • Access to all positions in a defined set of organizational units. • Perform all staffing functions; open and close requisitions, search for

**State of Florida
People First System Security Guidelines Manual
September 2009**

	<p>applicants, maintain vacancy status of positions, etc.</p> <ul style="list-style-type: none"> • Perform Personnel Action Requests for their direct reports.
S - Statewide Access	<p>Only assigned by the DMS People First team and in general is reserved for use by the People First team in testing and maintaining the People First system.</p> <ul style="list-style-type: none"> • View all employees regardless of the agency. • No access to employee Direct Deposit data or benefits information. • Access to employee exempt data (F.S. 119). • Access to the Training module. • Access to the Performance Management module. • Access to the Organizational Management module. • Manager access (as described above) for employees that report to them. • View all employee data for all agencies including SSN, home address and telephone, etc. • View and maintain Organizational Units, Classes, Broadband, and Position data. • Access to monitor staffing functions. • Used for employees with statewide access. • Perform Personnel Action Requests for their direct reports.
T - Time Administrator	<p>Assigned to employees who assist other employees with their time sheets. It is generally used by business units with large numbers of employees with limited computer access. There is no limit on the number of assigned 'T' role codes.</p> <ul style="list-style-type: none"> • Access to all employees in a defined set of organizational units. • Access to all time entry, leave requests and time approval functions. • No access to employee Direct Deposit data. • No access to most employee pay and personal information. • Cannot perform employee actions (appointment, etc.). • Can enter and approve time worked and leave used, leave request and flex schedule requests. • Can perform Personnel Action Requests for their direct reports.
V - Third Party Vendor (Provider)	<p>Assigned to contractors responsible to assist with processing miscellaneous deductions.</p> <ul style="list-style-type: none"> • Access to employee deduction data (one-time and recurring deductions).
W - Risk Management/Worker's Compensation	<p>Assigned to staff in the Division of Risk Management and can be assigned only by the DMS People First team.</p> <ul style="list-style-type: none"> • Access to all employees for purposes of managing Worker's Compensation and Risk Management. • Perform Personnel Action Requests for their direct reports.
Z - Retirement	<p>Assigned to staff in the Division of Retirement and can be assigned only by the DMS People First team.</p>

**State of Florida
People First System Security Guidelines Manual
September 2009**

	<ul style="list-style-type: none">• Access to all employees for purposes of managing Division of Retirement functions.• Perform Personnel Action Requests for their direct reports.
--	--

**State of Florida
People First System Security Guidelines Manual
September 2009**

Exhibit 3

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 60DD-2.008, F.A.C. (Personnel Security and Security Awareness).

Scope

The DMS recommends that employees (state and OPS) who are assigned an A, C, D, F, G, H, S, V, W, or Z role code in People First and/or who have access to the People First data warehouse have a Level II background check performed on them.

Certain positions in the Career Service, OPS, Selected Exempt Service and Senior Management Service 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.

Authority

1. Section 110.1127, F.S., Employee Security Checks.
2. Section 282.318, F.S., Security of Data and Information Technology Resources.
3. Section 435.04(1), F.S., Employment Screening.

Definitions

1. Employee: Any person who has been hired, works for the state and receives a warrant 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.

**State of Florida
People First System Security Guidelines Manual
September 2009**

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-wide background) or Level II (national background including fingerprint investigation) and maintain a listing of all special trust positions in the Department.
3. 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. 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 State of Florida employment application 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 background investigation or fingerprinting process based upon the level of screening established for the position of special trust.
6. 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.

**State of Florida
People First System Security Guidelines Manual
September 2009**

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.