

People First Division

Procedures for Handling Confidential or Exempt Records and Information

❖ **Authorities**

Florida Statutes

Chapter 119 – Public Records

Chapter 257 – Public Libraries and State Archives

Florida Administrative Code

Rule 1B-24.003 – Records Retention Scheduling and Disposition

Rule 1B-26.003 – Electronic Recordkeeping

Department Policies

Administration – 98-106 – Records Management

Administration – 94-102 – Public Records Requests/Public Meetings

Human Resources – 06-110 – Misuse of Information and Data

Human Resources – 05-107 – Background Investigations & Fingerprinting Requirements

❖ **Definitions**

1. “Confidential” means public records or information that are protected from disclosure under Florida or federal law under all circumstances, absent an express statutory exception or court order.
2. “Exempt” means public records or information that are designated as protected from disclosure under Florida or federal law, but may be disclosed within the discretion of the custodian.
3. “Commercial Entity” under section 119.071(5), F.S., means any corporation, partnership, limited partnership, proprietorship, sole proprietorship, firm, enterprise, franchise, or association that performs a commercial activity in this state.

❖ **Requirements for Maintaining and Providing Access to Public Records**

1. Section 257.36(5), F.S., requires agencies to establish and maintain an active and continuing program for the economical and efficient management of records.
2. Section 119.07(1), F.S., requires records custodians to allow inspection and copying of public records, except for records statutorily designated as confidential or exempt from disclosure.

❖ **Collection, Use and Release of Social Security Numbers**

Social security numbers (SSN's) that are stored in the People First system are confidential and exempt from public disclosure, with specified exceptions. In accordance with section 119.071(5), F.S., and Department Policy Administration 94-102, the People First Division (Division):

1. will not use social security numbers (SSN's) unless it is authorized by law to do so, or use is imperative for the performance of the Division's duties and responsibilities;
2. will ensure that the use or release of SSN's complies with Florida and federal laws;
3. will disclose SSN's only in accordance with section 119.071(5), F.S.;
4. will not deny a commercial entity access to SSN's for commercial activities upon receipt of a written request meeting the following requirements:
 - verified (sworn to) as provided under section 92.525, F.S.;
 - legibly signed by an authorized officer, employee, or agent of the commercial entity;
 - containing the commercial entity's name, business mailing and location addresses, and business telephone number; and
 - stating the purposes for which SSN's are needed, and how the SSN's will be used in the performance of a commercial activity, with citation to the Florida or federal laws permitting such use; and
5. will disclose SSN's only upon authorization of the People First Director.

❖ **Other Confidential or Exempt Records and Information**

The following are examples of confidential or exempt records and information maintained by the Division in performance of assigned duties and responsibilities:

1. All social security numbers held by an agency are confidential and exempt. Section 119.071(5), F.S.
2. Medical information pertaining to a prospective, current, or former officer or employee of an agency which, if disclosed, would identify that officer or employee is exempt. Section 119.071(4)(b)(1), F.S.
3. Patient medical records and medical claims records of state employees, former state employees, and their eligible covered dependents in the custody or control of the state group insurance program are confidential and exempt. Section 110.123(9), F.S.

4. Personal identifying information of a dependent child of a current or former officer or employee of an agency, whose dependent child is insured by the agency's group insurance plan is exempt. Section 119.071(4)(b)(2), F.S.
5. Personal identifying information, which may include home addresses, telephone numbers, social security numbers, dates of birth and photographs, for specified agency personnel, and their spouses and children, is exempt. Section 119.071(4)(d), F.S.
6. The names and addresses of retirees are confidential and exempt to the extent that no state agency may provide the names or addresses of such persons in aggregate, compiled, or list form to any person except to a public agency engaged in official business. However, a state agency may provide the names and addresses of retirees from that agency to a bargaining agent as defined in s. 447.203(12) or to a retiree organization for official business use. Lists of names or addresses of retirees may be exchanged by public agencies, but such lists shall not be provided to, or open for inspection by, the public. Any person may view or copy any individual's retirement records at the Department of Management Services, one record at a time, or may obtain information by a separate written request for a named individual for which information is desired. Section 121.031(5), F.S.
7. Personal identifying information of a member in the investment plan contained in Florida Retirement System records held by the state board or the department is exempt. Section 121.4501(19), F.S.
8. Bank account numbers held by an agency are exempt. Section 119.071(5)(b), F.S.
9. Records or information contained in a response to a competitive solicitation or contract-related records or information designated by a vendor as trade secret are confidential and exempt. Section 815.045, F.S. If a document is marked trade secret, confidential or proprietary, the document will be reviewed by the Office of the General Counsel (OGC).

❖ **Responding to Public Records Requests**

The Division's contact person for public records requests is the Security Lead. All requests are reviewed by the Security Lead, and where applicable, the Director and OGC.

❖ **Communication of Division Procedures**

Division members are made aware of the procedures and applicable state and federal laws, rules and policies regarding the protection of confidential and/or exempt information through e-mail and scheduled staff meetings.

❖ **Standard Documents**

1. In accordance with Department Policy 09-110, the Division regularly reviews and updates procedures and standard documents for changes in laws, management objectives, and advances in technology.
2. The Division reviews on a regular basis its procedures and standard documents to ensure that confidential and or exempt information is used only to the extent necessary for the performance of the Division's duties and responsibilities.

❖ **Physical and Electronic Security**

In order to prevent unauthorized access to records containing confidential and/or exempt information, the Division ensures that such information is secured behind locked doors or safe filing cabinets when such documents are not in use. This procedure is in compliance with Department Administration Policy 94-102 and Human Resource Policy 06-110.

The Division procedures include the following:

1. Rooms 220 and 235 are designated as secured areas.
2. Sensitive data is kept within the secured area for storage when such documents are not in use.
3. Employees comply with established protection and control procedures and protect information and data being used.
4. Employees are required to secure the confidential and/or exempt documents behind locked doors or in locked cabinets after work hours or when not in use for extended periods of time during the work day.
5. All sensitive documents are placed in the secure shred bin.
6. Computers are locked when employees are not at their desks.

❖ **Access Controls**

1. The objective of security controls is to protect the integrity, confidentiality, and availability of information systems data and resources. Effective security controls include access controls that ensure users have only access privileges needed to perform their duties, access to sensitive resources is limited to authorized users, and users are restricted from performing incompatible functions.

2. The Division has written procedures for requesting, approving, assigning, monitoring, and removing user access privileges.

❖ **Positions of Special Trust**

1. The Division complies with Department Policy Human Resources 05-107 for designating positions that, because of special trust, responsibility, or location require persons occupying the positions to be subject to a level 2 screening as a condition of employment. Employees occupying positions of special trust are required to sign an acknowledgement stating that they are aware of, and agree to, the requirements of Department Policy Human Resources 05-107.
2. The Division has designated all Division positions as positions of special trust.
3. The contract for the People First system states that "the Service Provider shall conduct a criminal background screening of, or ensure that such a screening is conducted for, each of its employees, Subcontractor personnel, Independent Contractors, leased employees, volunteers, licensees or other person". The contract stipulates the following minimum screening requirements: "The minimum background screening process shall include a check of the following databases through a law enforcement agency or a Professional Background Screener accredited by the National Association of Professional Background Screeners or a comparable standard: (i) Social Security Number Trace; and (ii) Criminal Records (Federal, State and County criminal felony and misdemeanor, national criminal database for all states which make such data available)".