



## ADMINISTRATIVE POLICY

POLICY NUMBER  
1.11

<b>TITLE:</b>	Protocols for Protecting Personal Information
<b>RESPONSIBLE OFFICE:</b>	Director's Office/Division of Workforce Services
<b>EFFECTIVE:</b>	March 11, 2015

### I. PURPOSE/SCOPE

This Policy establishes requirements and formalizes existing safeguards for protecting the Personal Information possessed by the Department of Economic Opportunity. This Policy will be amended over time as the Department continues to implement measures to protect Personal Information and prevent identity theft and benefits fraud.

### II. REVISION INFORMATION

Revised March 2015

### III. AUTHORITY

- A. Rules 71A-1.006, 1.007, 1.019, Florida Administrative Code
- B. Rule 60L-36.005, Florida Administrative Code
- C. Department Policy 5.10

### IV. DEFINITIONS

- A. Covered Employee — This definition includes any Department employee, including intern, volunteer, contract employee, independent contractor or its employee, or vendor, that is working in, performing duties pertaining to, or being paid by the Department for work done within the Division of Reemployment Assistance. For the purposes of this Policy, Reemployment Assistance includes only the Bureau of Reemployment Assistance Program (a bureau of the Division of Workforce Services) and Reemployment Assistance Appeals. For Information Technology (IT) positions that support the above-identified areas the following sections of this Policy shall apply: V.E. and V.F.
- B. Department — Department of Economic Opportunity.
- C. Mobile Device — Any smartphone, cellular telephone, camera, tablet computer, E-reader, USB storage device, hand-held computer device, mobile computing device,

mobile storage device, CD or DVD, external hard drive, or any other portable electronic device capable of accessing the Internet and/or sending and receiving email and/or capturing images.

D. Personal Information — An individual's social security number, driver's license number, bank account number, credit card number, or bank routing number, regardless of whether such information is also used in combination with the individual's name. This definition also includes any information related to a reemployment assistance claim. Personal Information may also include information that has been declared confidential by Florida or federal law. As used in this Policy, this term refers to entire record systems, specific records, or individually identifiable data that by law are not subject to public disclosure under Article I, Section 24 of the Florida Constitution and s. 119.07, Florida Statutes. When applicable, this term covers all documents, papers, computer files, letters, and all other notations of records or data that are designated by law as confidential. Further, the term also covers the verbal conveyance of data or information that is confidential. This definition does not in any way expand the Department's responsibilities under s. 501.171, Florida Statutes.

## V. PROCEDURES/POLICY

### A. Identification of Covered Employees and Exemptions

1. This Policy applies to all Covered Employees.
2. The Director of the Division of Workforce Services may identify and prepare a list of Covered Employees who, based on job duties, should be exempt from some or all of the requirements of this Policy.
3. Any such list of exempt employees shall include (1) a statement of the specific portions of this Policy from which each employee is exempt, and (2) a written justification for each employee specifically describing why he or she should be exempt from each listed requirement.
4. Before becoming effective, any exemption shall be reviewed and approved by the Department's Chief Information Officer, General Counsel, and Chief of Staff.
5. The Director of the Division of Workforce Services shall immediately remove an exemption from the list if he or she determines that placement on the list is no longer appropriate.
6. The Director of the Division of Workforce Services shall provide any list of exempt employees to the Bureau of Human Resource Management, which shall maintain a database of exemptions.
7. Any list of exemptions must be approved once every quarter of the calendar year consistent with the above requirements. Upon any change in a Covered Employee's job duties, that Covered Employee's exemption status, if any, shall be reviewed and re-approved consistent with the above requirements.

### B. Access to Systems and Databases Containing Personal Information

In collaboration with the Chief Information Officer, the Director of the Division of Workforce Services shall conduct regular reviews of system and database access and permission levels to ensure that access to Personal Information is appropriately

limited. Such reviews shall at a minimum consist of compiling: (1) a "System and Database Access List" that contains each system and database accessible to or maintained by the Department; (2) a list of Covered Employees with the ability to grant access to any such system or database; and (3) a list of Covered Employees with access to any such system or database. The "System and Database Access List" must be routinely updated. In the last week of each quarter of the calendar year, the Director of the Division of Workforce Services and the Chief Information Officer must certify to the Executive Director that a review consistent with this section has occurred.

C. Printing and Storing Documents Containing Personal Information

1. The Division of Workforce Services shall determine and identify which Covered Employees require the ability to print documents due to business needs. Only the work stations of Covered Employees identified as requiring the ability to print documents shall be connected to network printers.
2. The use of non-networked printers is forbidden.
3. Covered Employees with an identified business need to print documents shall not print any Personal Information without documented approval from his or her supervisor. Such approval must be narrowly tailored to include only the permission necessary for the performance of specifically documented job duties.
4. Documents containing Personal Information must at all times be adequately secured to ensure that unauthorized viewing is not possible. For example, Personal Information must not be left unattended and exposed in a cubicle, on a desk, or in an unlocked office.
5. Supervisors must review printing activity on a weekly basis to ensure Personal Information is being protected.
6. Supervisors must ensure that once a printed document is no longer needed it is properly disposed of in accordance with Department [Policy 4.09](#), Records Management Policy.
7. The Division of Information Technology shall facilitate the routine monitoring of print jobs to individual work stations, including but limited to the electronic recording and storage of the date, time, content if feasible, and responsible party for each print job.

D. Data Storage, Duplication, and Distribution

1. No Covered Employee shall insert or connect a Mobile Device into a Department computer.
2. Covered Employees shall not duplicate or copy Personal Information by any means without prior documented approval from his or her supervisor. For example, a Covered Employee may not use image capturing software to create an image of Personal Information or take any written notes containing Personal Information.

3. Covered Employees shall not take documents containing Personal Information outside of a Department building and may only transport those documents within a Department building for a legitimate business purpose.
4. Covered Employees shall not electronically or otherwise distribute Personal Information using any unapproved means or for any unapproved purpose.

E. Prohibition on Use of Certain Mobile Devices

1. Covered Employees may not use Mobile Devices at any work station where access to Personal Information is possible.
2. Mobile Devices shall not be visible at work stations at any time. For example, Mobile Devices shall not be placed on desktops.
3. Covered Employees must step away from all work stations where access to Personal Information is possible before using a Mobile Device. Such use should be limited to breaks or urgent situations and shall only be used in designated break areas.
4. If a Covered Employee chooses to bring his or her Mobile Device into a Department building, and when a Covered Employee is at or near a work station, such devices may be kept inside the employee's pocket, purse, brief case, or other similar area. A Covered Employee shall not answer a ringing Mobile Device or otherwise interact with a Mobile Device while at or near a work station where access to Personal Information is possible. If any part of a Mobile Device is visible at or near at work station where access to Personal Information is possible, it will be assumed that the Covered Employee is in violation of this Policy.

F. Active Supervision and Monitoring of Covered Employees

1. Supervisors of Covered Employees must physically monitor all Covered Employee's computer activity on a routine basis by walking through applicable work station areas. Such monitoring shall be accomplished multiple times each day and should occur at both routine and random times. Employees must structure their work stations in a manner that facilitates this requirement and must allow their supervisors to view their computer activity at any time.
2. The Division of Information Technology may collect logs of any Employees' computer activity and provide them to supervisors, the Department's Office of Inspector General, or any other appropriate authority. In conjunction with the Division of Information Technology, supervisors, and/or the Office of Inspector General shall evaluate the data for unauthorized or inappropriate use and may interview Employees if necessary.

G. Disciplinary Action

Failure to comply with any of the requirements of this Policy may result in disciplinary action, up to and including termination. Any suspected violations of Florida or federal law will be taken seriously and may result in the referral to the appropriate local, state and/or federal authorities for criminal prosecution.

H. Training and Affidavit of Understanding

Every Covered Employee must receive annual training on the requirements of this Policy and after each annual training must acknowledge that they understand and will follow the requirements of this Policy. The training must detail the state and federal crimes dealing with identity theft, benefits fraud, and unauthorized access to and/or misuse of Personal Information. Although the training is mandatory, if a Covered Employee is unable to attend training for any reason, all terms and conditions of this Policy still apply to that Covered Employee.

**VI. FORMS/ATTACHMENTS**

None