STATE OF FLORIDA
DEPARTMENT OF
CHILDREN AND FAMILIES
TALLAHASSEE, December 11, 2008

CF OPERATING PROCEDURE
NO. 55-18

Financial Management

DATA SECURITY ON GRANTS SYSTEM

1. Purpose. This operating procedure serves as a guide and reference for data security for the GRANTS System.

2. Authority. The basis for this operating procedure is Information Systems' requirements for security of all the Department's automated systems.

3. Definitions.

a. Access. To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of information resources.

b. Access Level. A security level based on a user's authorized actions within the GRANTS System.

c. Authorization. The granting of access rights to a user, program or process by the system owner(s).

d. Data. A collection of organized facts or concepts, especially information organized for analysis or used to make decisions ("statistical data").

e. Data Security. The process of protecting information from unauthorized use (accidental or intentional) by restricting database access for viewing, organizing and updating data files.

f. GRANTS (Grants and other Related Allocation aNd Tracking System). A system that tracks grant related expenditures, earnings, cash and draws associated with each grant.

g. GRANTS Security Coordinator. Person who maintains data security on the GRANT System.

h. Password. A protected/private character string used to verify an identity.

i. Position Description. Description of a user's job duties/responsibilities.

j. System Owner. The individual/office having the primary responsibility for granting access, defining requirements and establishing the rules for appropriate use and protection of the data/information within a system.

k. User. An individual who is authorized access to a system/application by the owner, in accordance with the owner's procedures and rules.

l. User Code. Identifies a specific user by the use of a unique symbol or character string.

This operating procedure supersedes CFOP 55-18 dated July 18, 2007.
OPR: ASFMS
DISTRIBUTION: X: OSES; OSLS; ASGO; ASFM; ASB; ITS; Regional Directors; Region IT Managers.

m. User Request Form. Form CF 106 (available in DCF Forms), used to request staff additions, deletions, and modifications on the GRANTS System.

4. Importance of Security for GRANTS.

a. The Department is dependent on GRANTS to accomplish its mission since it is the management tool to monitor federal funding.

b. The data within this system is used to make decisions on federal draws and federal reporting as required by law.

c. This data must be available, accurate and protected from unauthorized use.

5. Objectives. The objectives of security for GRANTS are to:

a. Minimize the chance of unauthorized access to information;

b. Minimize the chance of unauthorized changes to data;

c. Hold each user accountable for their activities on the system; and,

d. Limit access to only those transactions necessary to accomplish position responsibilities.

6. Assumptions for GRANTS Security.

a. Each user office knows the requirements of their data.

b. Each user is held accountable for their activities on the system.

7. Access Authorization.

a. To be granted authorized access, an individual must have a need and right to know the information.

b. The system owner is the Office of Revenue Management Staff Director, who will determine which individuals, as part of their job responsibilities, should have access to the system. The system owner may delegate, to appropriate supervisory staff, the responsibility to review and approve user request forms within Revenue Management. The system owner must approve GRANTS User Access Requests submitted by non-Revenue Management individuals and will restrict system override capabilities to essential personnel.

c. For access to GRANTS, an individual must complete and submit a copy of form CF 106, GRANTS User Access Request, to the GRANTS Security Coordinator. This form is available in DCF Forms on both the Intranet and Internet. A copy of the individual's State of Florida Position Description must accompany the GRANTS User Access Request form.

d. The first activity of an authorized user will be to change the initial password to a personal password. See paragraph 9 of this operating procedure for guidelines on creating and safeguarding a personal password.

e. The proper User Code and password will be required each time the user accesses the system.

f. If a user's access authorization requires a change, the user must complete and submit another GRANTS User Access Request form.

g. When a user transfers to another unit within the Department or leaves the Department, the user's supervisor must notify the Security Coordinator by submitting a GRANTS User Access Request form to delete user access. This request must be submitted within five (5) business days of the user's transfer or termination.

8. Responsibilities of the Central Office GRANTS Security Coordinator. This coordinator will:

a. Notify Data Security at Northwood Data Center of a new user access request and obtain User Code and initial password.

b. Provide the user with a User Code that identifies the individual to the system and is a unique identifier.

c. Provide the user with an initial password that verifies that the individual attempting initial access is the individual authorized by the GRANTS Security Coordinator for the user code assigned. This initial password should prompt the user to change from this first time password to a personal password.

d. Maintain a list of all authorized users that includes User Code, name and employee number.

e. Maintain security reports that list user access levels.

f. Provide security reports to Office of Revenue Management supervisors for review on a quarterly basis for required changes or updates.

9. Creating and Safeguarding a Personal Password.

a. A personal password for GRANTS:

(1) Is between six (6) and eight (8) alpha/numeric characters (required).

(2) Must not contain spaces between characters (required).

(3) Does not reflect personal information, such as identity, history or environment (e.g., name, initials, date of birth, school, office, job, etc.).

(4) Is not any word found in a dictionary.

(5) Is not easily guessed (e.g., days of the week, seasons, months).

(6) Must be created and changed only by the individual identified as the authorized user.

(7) Must not be written down.

(8) Must not be shared.

(9) Must be changed every 45 days, in accordance with Department standards.

(10) Must be changed any time the password is compromised.

(11) Must be different from the previous password, when changed.

b. Personal passwords used to verify identity shall be known only by the user having that identity.

c. Each user shall be responsible for providing protection against loss or disclosure of passwords in their possession.

d. The password must be entered by the owner in a manner that protects the password from disclosure to anyone observing the entry process.

e. Passwords may not be displayed on the terminal during the entry process.

f. Passwords may not be printed on any output media.

g. Passwords will be locked after three (3) incorrect attempts.

h. For password resets, the user must contact the Help Desk at 487-9400 or via the Department's Intranet. For verification requirements, the user must provide User Code and last four digits of the user's Social Security Number.

BY DIRECTION OF THE SECRETARY:

(Signed original copy on file)

MELISSA P. JAACKS
Assistant Secretary for
Administration

SUMMARY OF REVISED, ADDED, OR DELETED MATERIAL

This operating procedure has been revised to conform to the requirements of the plain language initiative.