

Series: Operating Procedures **COA:** RPM 8.01
CFOP:
Procedure Name: Systems Management Security
Procedure Number: OP-1100
Revision #/Date: (2)1/6/09
Effective Date: 1/20/06

Applicable to: All CBCB Staff and Contract Providers

SUBJECT: Systems Management Security

PURPOSE: To outline minimum security responsibilities regarding employee and contract provider employee access to data. Adherence to this policy will ensure the ability to provide personal accountability pertaining to the security of CBC of Brevard and contract provider employee access to data through the use of computer-related media

PROCEDURE:

References

Florida Statutes: Section 282.318 and Chapter 815
Florida Administrative Code 60DD-2, "Florida Information Resource Security Policies and Standards".
CBCB Policies/Procedures: GOV 202, GOV203

Definitions

Confidential and Sensitive Information: Confidential and sensitive information refers to information that has specific statutory exemption from the public records laws. Specific requirements for appropriate levels of data security remain under the purview of each agency.

Overview

- a. Every CBC of Brevard and contract provider employee shall be held responsible for information security, especially involving the access, transport or storing of sensitive and confidential information. Fulfillment of security responsibilities shall be mandatory and violations may be cause for disciplinary action, up to and including dismissal, civil penalties, or criminal penalties under chapters 119, 812, 815, 817, 839, or 877, Florida Statutes, or similar laws.

- b. All employees, including contracted employees with access to data through computer-related media must read and sign the DCF Security Agreement Form (CF 114).

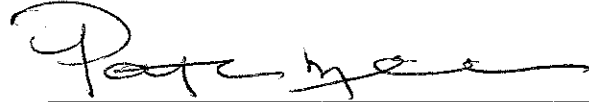
- c. This procedure regulates the assignment and use of computer system user IDs and associated passwords and employee responsibilities when granted system access. Information sharing with selected employees should be handled through other administrative methods rather than sharing passwords. User IDs that have not been utilized for a period of 60 days will be automatically revoked and will require the CBC of Brevard Security Officer and DCF's Region Security Officer intervention to reactivate for the purposes of verifying current or continued employment.
- d. Electronic mail may contain confidential or sensitive information and at those times proper security should be maintained when using this tool. Special e-mail rules and alias assignments should be individually established to permit sharing of electronic mail; and mainframe security features are available to give supervisors appropriate access rights to their employees' cases, if required. Employees should investigate and use these available methods for information and access sharing rather than sharing passwords. However, for special emergency needs to conduct official state business, an e-mail password may be divulged to a trusted individual of the password owner's choosing, but only if it becomes absolutely necessary to conduct such business. At such time and under those certain circumstances that an e-mail password becomes compromised, the password owner shall change the e-mail password as soon as possible to once again assure that security is not compromised.

Process

- a. CBC of Brevard determines who within their organization should have access to the data. CBC of Brevard's designated Data Security Officer will distribute the DCF Security Agreement Form (CF 114) to each provider employee granted access to data through the use of computer-related media (e.g., printed reports, microfiche, system inquiry, on-line update, or any magnetic media). *Note: The provider may not require its employees to disclose their passwords.*
- b. All CBC of Brevard and contracted employees who have access to data will read the DCF Security Agreement Form (CF 114) and, if necessary, obtain clarification from a supervisor or designee. CBC of Brevard will identify an individual to function as its Data Security Officer. This Data Security Officer will act as a liaison to the department's security staff. The provider will obtain signed CF 114 forms from each of its employees who have access to data at least annually. *Note: For multi-year contracts, newly signed forms will be obtained from each provider employee upon the contract's renewal.*
- c. All CBC of Brevard and contracted employees will acknowledge receipt of the minimum security requirements in the "Florida Computer Crimes Act (Chapter 815, Florida Statutes)" and departmental policy and procedures and agree to abide by the requirements by signing the CF 114 form.
- d. CBC of Brevard is responsible for maintaining the signed CF 114 forms for its employees who are granted access to data and will make the forms available to authorized department staff upon request.
- e. All CBC of Brevard and contracted employees will retain a duplicate copy of the form and a copy of the "Florida Computer Crimes Act (Chapter 815)".

- f. Supervisors are responsible for immediately notifying the Data Security Officer, located at the main office of CBC of Brevard, upon the termination, transfer or resignation of any CBC of Brevard or Contract employee for the purpose of system access adjustment or termination.

BY DIRECTION OF THE CHIEF EXECUTIVE OFFICER:



DR. PATRICIA NELLIUS-GUTHRIE
Chief Executive Officer
CBC of Brevard, Inc.

APPROVAL DATE: 3/2/09