



Series: Information Technology

COA: RPM 5, 6.01, 6.03, 8.01, 8.02

CFOP: CFR45, CFR 164.310(b)

Procedure Name: Workstation Security

Procedure Number: IT-803

Revision #/Date:

Effective Date: 12/12/08

**Applicable to:** All CBCB employees, contractor, freelancers, and other agents who utilize computers to access any organization or client-specific data.

---

**SUBJECT:** Workstation Security

**PURPOSE:** The purpose of this procedure is to define standards and restrictions for the computing environment in which CBCB employees, contractors or other associates use workstations to access company and client information.

**PROCEDURE:**

### Reference

CBCB Policies/Procedures: GOV-202, GOV-203, OP-1099, OP-10100, OP-1050-19

### Definition

CBCB computers will be considered workstations.

### Security Protocols

In order to properly and reasonably secure and protect company and client information, the following safeguards will be adhered to:

- Physical:
  - Workstations, wherever possible, will be segregated from the client/visitor/waiting area.
  - Computer monitors, wherever possible, will be turned to such a position that visitors or clients cannot see the contents of the screen while maintaining the working comfort and convenience of the end-user.
  - In exceptional cases in which the above two safeguards cannot be accommodated, the use of a reduced viewing angle computer monitor shield will be employed.

- Logical:
  - Workstations will be locked whenever not currently in use and especially in the presence of visitors/clients when the end-user must leave the workstation. The workstation may be locked as follows:
    - CTRL+ALT+DEL then click Lock Computer
    - 'Windows + L'
    - Logging off from Windows
  - Workstations will be automatically locked by the network after ten (10) minutes of inactivity.
- Agreement:
  - End users will complete Computer Security Requirements as provided for in CBCB procedures OP-1099 and OP-10100.
  - Upon login to Windows, CBCB network users will be presented with a network security agreement encompassing the security issues outlined in CBCB procedures OP-1099 and OP-10100, HIPAA, COA Risk Prevention and Management Guidelines, and Florida Statutes Chapter 668 regarding electronic mail.

The Windows logon network security agreement will read as follows:

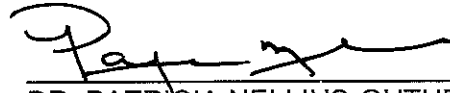
**Community Based Care of Brevard Inc. Network**

You are about to enter a secure network which may avail confidential client information. You are hereby bound by the rules of HIPAA, CBCB procedures OP-1099 and OP-10100, COA RPM Guidelines and Florida Statute Chapter 668. You further agree that your activity may be tracked, recorded and reviewed for compliance with the above rules and regulations. All electronic mail addresses transmitting or receiving mail from CBCB are considered public record. By clicking "**OK**" you agree to be so bound.

**Procedure Noncompliance**

Failure to comply with this procedure should be reported as outlined in CBCB procedure OP-1050-19, Security Incident Reporting and Tracking.

BY DIRECTION OF THE CHIEF EXECUTIVE  
OFFICER:



---

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

APPROVAL DATE: 1/7/09