



**Series:** Operating Procedures COA: RPM 6.01  
CFOP: 50-19  
**Procedure Name:** Security Incident Reporting and Tracking  
**Procedure Number:** OP-1050.19  
**Revision #/Date:**  
**Effective Date:** 10/01/08

**Applicable to:** All CBCB Staff, Contract Providers, External Agencies that using CBCB information resources

---

**SUBJECT:** Security of Information

**PURPOSE:** To outline responsibilities for reporting, tracking, handling, and resolving incidents that result in damage, release of confidential information, and/or electronic denial of data processing services or security violations that could potentially lead to a breach of security.

**PROCEDURE:**

**Reference:**

CBC Risk Management Policy: GOV-203

### Definitions

- a. Security Violation. An intentional violation of one or more of the department's security policies, rules, operating procedures or regulations, or a computer crime as described in Florida Statutes.
- b. Security Incident. An event or unintentional action that results in compromised data confidentiality, a danger to the physical safety of technology resources or personnel, misuse of state technology resources, and/or electronic denial of technology resource services.
- c. System Owner(s). The entity that owns the data and has the primary responsibility for decisions relating to a particular data processing system's specification and usage

### Background

Computer systems are subject to a wide range of mishaps from corrupted data files to viruses to natural disasters. For example, frequently occurring events (e.g., a mistakenly deleted file) can usually be readily repaired (e.g., by restoration from the backup file). More severe mishaps, such as outages caused by natural disasters, are normally addressed in an organization's contingency plan. Other damaging events result from *deliberate malicious technical activity* (e.g., the creation

of viruses or system hacking). A computer security incident or violation can result from a computer virus, other malicious code, or a system intruder, either an insider or an outsider. It can more generally refer to those incidents that, without technically expert response, could result in severe damage. The primary benefits of an incident handling capability are *containing* and *repairing* damage from incidents, and *preventing* future damage.

**Responsibilities for Reporting and Handling Actual or Suspected Security Incidents/  
Violations**

- a. System owners are responsible for ensuring that their application has documented security guidelines and rules included in a user guide or application manual, and that all users of their system(s) have access to this documentation. The user guide must document what is expected of the user, what are security violations, and how the supervisor will handle them.
- b. An employee or contracted employee who knows or suspects that a security incident or violation has occurred is responsible for informing their supervisor immediately of the incident or violation. Failure to do so may result in disciplinary action.
- c. Supervisors are required to immediately notify their manager, CBC of Brevard Security Officer and the Inspector General of any security incidents or violations, whether suspected or confirmed. Through coordination with CBC of Brevard personnel at the direction of the Inspector General, Supervisors will immediately ensure the equipment is secured and placed in a locked location. Information Systems personnel will be allowed to examine the equipment, if necessary, with consent from the Inspector General using the Chain of Custody Form. Failure to do so may result in disciplinary action.
- d. The CBC of Brevard Security Officer is responsible for reporting to the DCF Information Security Manager and Information Systems' Helpdesk (850-487-9400) on any security incidents or violations and following up on these reports until they are closed.
- e. The CBC of Brevard Security Officer is responsible for conducting quarterly audits of FSFN cases to determine if unauthorized viewing activity has occurred within CBC of Brevard and its contractors. The sample reviewed will be that of the quarterly QA sample.
- f. The CBC of Brevard Security Officer is responsible for notifying the affected clients when a compromise of confidential information has been identified.
- g. The CBC of Brevard Security Officer is responsible for determining future training or policy/rule enhancements that may be required to prevent recurrences of particular types of violations/incidents.

BY DIRECTION OF THE CHIEF EXECUTIVE  
OFFICER:



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

APPROVAL DATE: 12/14/08