

## **LEON COUNTY E.M.S.**

### Standard Operating Guideline

---

Title: Security Incident Management  
Effective: June 2006  
Reviewed: December 2012  
Revisions: 1  
Pages: 2

---

#### I. PURPOSE:

To provide guidelines for Security Incident Management

#### II. GUIDELINE:

Incidents that could compromise our electronic information system are serious as critical patient information may be damaged or lost. This policy establishes Leon County EMS Division's general policy on how to report a security incident and the steps that will be taken to investigate and take action when a potential to actual security incident occurs.

#### III. PROCEDURE:

##### Security Incident Defined

A "Security Incident" is an attempted entry, unauthorized entry, or an information breach or attack on our electronic information system. It includes unauthorized probing and browsing of the files, a disruption of service from any cause, and incidents where electronic information has been altered or destroyed.

Security incidents may include such things as a virus or a worm, or unauthorized use of computer accounts and computer systems. It may also include complaints or reports of improper use of our information system.

##### Reporting a Security Incident

All staff members are responsible for immediately reporting a security incident or suspected security incident immediately.

When a suspected security incident occurs, an Incident Report will be completed.

The Privacy/Information Security Officer will be responsible for initiating an immediate investigation to isolate the problem and take whatever action is necessary to protect the

information system and e-PHI and other vital electronic information. All actions will be done in a coordinated manner with Leon County MIS.

The Privacy/Information Security Officer will notify management immediately in the event the incident cannot be immediately corrected, or if any e-PHI or other vital information is altered or destroyed. Management will also be notified of any completed investigation and the outcome of the investigation. In the event of a suspected computer crime, or other unlawful activity via the use of the information system, local, state, or federal law enforcement may need to be notified. That determination will be made by management with recommendation from the Privacy/Information Security Officer.

The Information Security Officer is responsible for coordinating communications with the county departments and divisions and outside organizations.

Whenever a security incident, such as a virus, worm, hoax e-mail, discovery of hacking tools, altered data, or other event that could harm the information system is suspected or confirmed, remedial action will be taken, confirmed that they caused or contributed to the incident.