Section 100 – Management & Administration

General Rules & Administration – 100.00		
S.O.P. # 100.22	**OPSEC**	PAGE: 1 OF 3
EFFECTIVE: 06/01/2004	Authorized: John Filer, Chief	
REVISED: 01/24/2017	Authorized: William Stephens, Director	

100.22.01 Purpose

The purpose of this SOP is to advise all uniformed and non-uniformed personnel, the policies and procedures regarding operational security (OPSEC) for the Department.

100.22.02 Applicability

All uniformed and non-uniformed personnel.

100.22.03 General

OPSEC is an analytical process and strict set of policies that are integrated into our daily routines for the purpose of denying information about our operations, personal employment information or protected healthcare information to those who could use it to do us harm. OPSEC does not replace other security disciplines, it supplements them. Articles of information that are secure, sensitive or confidential in nature may come in all sorts of formats, verbal, written or even web-based; these include but may not be limited to…

- Personnel Files
- Personnel Phone & ID Lists
- Patient Care Reports
- Special Operations SOP's
- Operations Manuals or Protocols
- Training Manuals and Course Syllabi
- Threat Assessments & Capabilities Lists
- "Classified" or "Sensitive" Documents or Information
- Emergency Operations Plans
- Strategy Plans or Analysis'
- Budget Plans & Budget Analysis'
- Federal, State & Local Intelligence Reports

Any one or combination of the above-mentioned information types, if disseminated to the wrong person/s or groups may be used to do harm. Department of Emergency Services personnel should be mindful and cognizant of OPSEC policies when dealing with or handling article of information of any type.

100.22.04 OPSEC Guide

Prior to dissemination of any sort, persons should review an article or document for information containing the following…

1. To your knowledge, is all the information in the article widely known within your professional community?
2. Is the fact that your organization has any efforts in this area publicly known?
3. Does the article contain protected healthcare information?
4. Does the article contain private employment information such as home addresses, dates of birth, phone numbers or names of a spouse or children?
5. Does the article contain personal financial information such as social security numbers, account identification or routing numbers?
6. Does the article contain information or accounts which are part of an active investigation?
7. Does the article contain disciplinary or human resource related information specific to a single or group of employees?
8. Through dissemination, will the article jeopardize the lives or safety of personnel operating in the field?
9. Is this article or piece of information on the *Departments' Critical Information/Document List?*

If one has answered **NO** to all of the above guideline questions then article/s of information may be discussed or disseminated. If an answer of **YES** was answered to any one of the guideline questions then the article/s of information shall be considered "sensitive", "secure" and or "confidential" and strictly adhered to this SOP.

100.22.05 Critical Information/Document List

1. Personnel Files
2. Personnel Phone & ID Lists
3. Patient Care Reports
4. Special Operations SOP's
5. Operations Manuals or Protocols
6. Training Manuals and Course Syllabi
7. Threat Assessments & Capabilities Lists
8. "Classified" or "Sensitive" Documents or Information
9. Emergency Operations Plans
10. Strategy Plans or Analysis'
11. Budget Plans & Budget Analysis'
12. Federal, State & Local Intelligence Reports

100.22.06 Policy

1. Articles of information that meet the OPSEC criteria and are on the *Critical Information/Document List* may not be:

   i. Disseminated to, or discussed with the public without expressed or written permission from the Director of Emergency Services,
   ii. Left or kept in open view of the public;
   iii. Left or kept in unsecured storage utilities when not in active use;
   iv. Left or kept in unsecured storage media when not in active use;
   v. Transported or transferred to personal or home PC's, PDA's, storage utilities, storage media or mass storage/archiving devices to include private servers or the "cloud".
   vi. Emailed or otherwise transferred to a non-governmental email account, servers or "cloud" utilities;
   vii. Shared on social media.

2. Articles of information that meet the OPSEC criteria and are on the *Critical Information/Document List* shall only be disposed of using one of the approved OPSEC disposal methods/procedures. Said articles ***shall never*** be disposed of or discarded in the common trash.
3. Hard drives, mobile devices and storage media containing, or previously used for handling and/or processing OPSEC material shall not be transferred to another owner until the hard drive has been wiped and restored to the original factory settings.

   i. If the item cannot be restored to the original factory settings, it must be destroyed in accordance with this SOP.
   ii. The exception would be if the item was being returned to the Department of Information of Technology, in which case they may be instructed to properly wipe the device.

4. Hard drives, mobile devices and storage media containing, or previously used for handling and/or processing OPSEC material shall be wiped prior to proper disposal.

100.22.07 Approved Disposal Methods/Procedures

The following are the ONLY approved disposal methods and/or procedures for articles of information that meet the OPSEC criteria:

1. Shredding of OPSEC documents shall be performed in a HIPAA compliant shredder,
2. Incineration of articles if optioned, shall be performed in an approved incinerator;
3. Shredding of wiped hard drives, mobile and/or storage devices shall be disposed of in a hard drive shredder;
4. Wiped hard drives, mobile and/or storage devices may be returned to the Department of Information Technology;
5. Disposal of articles if optioned, may be performed by a private security contractor.