



Jefferson County - City of Port Townsend
COMPREHENSIVE EMERGENCY MANAGEMENT PLAN



Part 3: Emergency Operations Guide

EOG 3.3.11 - EOC INFORMATION SECURITY – SENSITIVE INFORMATION HANDLING POLICY

(March 2008)

INFORMATION SECURITY - Information security is the protection of the confidentiality, integrity, and availability of information related to the business of the Department of Emergency Management. In the course of business of the Emergency Operations Center certain information must be considered sensitive for legal, ethical or procedural reasons. Members of the Incident Management Team must respect internal communications and protect privacy.

OBJECTIVE - The objective is to protect the vital interests of emergency management activities and provide for personal privacy, while permitting candid discussion, development of plans and strategy, and the exchange of critical analysis beyond the direct public view.

REDUCTION OF RUMORS - Good information management philosophy reduces the propagation of harmful rumors.

PUBLIC RECORDS ACCESS POLICY – Most activities of the EOC will eventually be subject to disclosure under open records policies. The purpose of this EOC is to provide guidance to the EOC team members during emergency operations to assure confidentiality. While the incident is in progress, including the immediate recovery period, the incident record is not complete.

INTERPRETATION - Interpretation of the Records Access Policy is beyond the scope of this document. Requests for public records will be coordinated by the Clerk of the Board of County Commissioners who oversees compliance with the policy. Release of information after an incident is closed will be in accordance with the Washington State Public Disclosure Act.

RESPONSIBILITY FOR IMPLEMENTING THE SENSITIVE INFORMATION MANAGEMENT POLICY - Each individual who creates, uses, processes, stores, transfers, administers or destroys information is responsible for complying with these information security standards. Oversight is the responsibility of the EOC Manager or designee.

OVERALL INFORMATION SECURITY STATEMENT - This statement will be posted in the Emergency Operations Center - ***Any information marked FOR OFFICIAL USE ONLY (FOUO), and/or pertaining to criminal investigation, identification of disaster victims, related medical information¹, their addresses, internal planning, draft plans or documents, un-cleared bulletins or news releases, the content of in-house briefings, overheard conversations or radio traffic, or unconfirmed speculation will not be released to the public unless cleared in advance by the EOC Manager/unified command.***

FOR OFFICIAL USE ONLY (FOUO) - Documents or information labeled FOUO is done so by the originator to limit external distribution. Such documents, information or bulletins are not be released either in written, oral or electronic form to the media, the general public, or other personnel who do not have a valid "need-to-know" without prior approval of the originator.

ORIGINATOR DETERMINES SENSITIVITY - The designation of FOUO, unless that category is already clearly exempt from disclosure by rule, will be determined by the originator. Information

¹ Members will be familiar with HIPPA guidelines.

may be categorized as FOUO which may have a “substantial likelihood of threatening public safety” pertaining to criminal terrorist acts. See RCW 42.56.420.

DISPOSAL OF FOUO - Except for those documents retained for documentary and historical purposes according to the law, hardcopy FOUO materials are to be disposed of by shredding, burning, pulping, or pulverizing beyond recognition or reconstruction. Electronic FOUO material shall be sanitized appropriately by overwriting or degaussing.

INDIVIDUALLY IDENTIFIABLE INFORMATION - The disclosure or dissemination of “individually-identifiable” health information or the names and addresses of deceased persons is prohibited.

RESTRICTED INFORMATION - When the EOC and any part of the Incident Management Team is activated in support of a law enforcement for an incident involving criminal activity, all related information shall be considered sensitive.

STATUS OF DRAFT (PRELIMINARY) INFORMATION - Preliminary information, including but not limited to draft strategic planning, Incident Action Plans in the development stage, draft press releases and unreleased Situation Reports, shall be considered sensitive.

CRIMINAL HISTORY INFORMATION - ACCESS rules require an additional sensitive information classification for persons working near ACCESS terminals who may have direct or casual contact with criminal history information. Persons with access to criminal history data in performance of their official duties at the Emergency Operations Center will satisfy the Sheriff’s Office information management standards.

RESPONSIBILITIES OF THE DEPARTMENT OF EMERGENCY MANAGEMENT

- Establish and maintain policies and procedures for protection of sensitive information before, during, and after an activation of the Incident Management Team.
- Provide for suitable secure storage for sensitive information.
- Provide a capability for destruction of sensitive according to policy.
- Act as the point of contact for requests for public disclosure addressed to the Incident Management Team.

RESPONSIBILITIES OF MEMBERS OF THE EOC INCIDENT MANAGEMENT TEAM

- Recognize the conditions of the Sensitive Information Handling Policy when referring to the official business of the Department of Emergency Management or the Incident Management Team.
- Safeguard sensitive information before, during, and after an activation of the Emergency Operations Center.
- Prevent incidental casual observation or access to sensitive information.
- Clear the release of possible sensitive information with Unified Command or the EOC Manager prior to dissemination outside the EOC.
- Refrain from repeating rumors or unverified information except where necessary to clarify or refute them.

RESPONSIBILITIES OF JEFFCOM

- Establish and maintain security measures for sensitive information originating in the dispatch center.
- Support the FOUO designation for any such designated information originating in the course of business in the EOC.

RESPONSIBILITIES OF THE SERVED AGENCY

- Take the necessary precautions to maintain reasonable security control of RESTRICTED information (criminal history, criminal activity, etc.).
- Approve the release of any sensitive information and coordinate with the joint Public Information process where appropriate.

TRUST - In the course of business team members are going to hear things and know things that are incident-specific but the circulation of which outside of the business of the EOC may be misinterpreted by others. This organization will not be respected by the agencies we serve if we violate their trust.

EXAMPLES OF INTERNAL AND SENSITIVE INFORMATION

- Addresses of damaged or destroyed private homes or businesses
- Content of briefings and planning meetings, formal or informal
- Criminal history
- Criminal suspect information
- Discussions among team members, formal or informal
- Draft versions of any document
- Drivers records
- Health information about disaster victims
- Incomplete logs, reports, forms, and incident files
- Individually-identifiable information about disaster victims
- Names and addresses of disaster victims
- News releases not yet cleared by Incident Command
- Preliminary incident action plans not yet IC approved
- Preliminary/draft strategic plans
- Preliminary/draft tactical plans
- Public safety radio traffic overheard
- Rumors and unsubstantiated reports
- Social Security numbers
- Telephone numbers of disaster victims and claimants
- Unsubstantiated information or conjecture


IMPLEMENTATION OF THE SENSITIVE INFORMATION HANDLING POLICY

- Consider all preliminary (draft) information not to be disclosed unless otherwise indicated.
- Consider all law criminal history or activity to be RESTRICTED unless otherwise indicated by the law enforcement command agency.
- Clearly mark FOUO information. Use a cover sheet where necessary to prevent casual observation.
- Clearly mark NEED-TO-KNOW information with the intended recipients.
- Obscure sensitive information from observation by guests and visitors to the EOC.
- Close the blinds on the EOC windows when showing sensitive information on the display boards, projector screens, TV displays, etc. Implement additional security measures as needed (see EOG 3.3.16 – EOC Physical Security Plan).
- Expect that all information may eventually be requested as a public record subject to interpretation by the proper legal authorities after the incident.
- Properly dispose of documents, when appropriate, to prevent accidental access to sensitive information.

CLARIFICATION OF SOME OF THE TERMS USED HERE

- ACCESS – A Computerized Enforcement Security System (computer criminal history terminals located in Jeffcom).
- Classified – any information, regardless of its physical form, that is determined by rule to require special legal protection against unauthorized use.
- Disseminate – distribution of information in any form, including electronic.
- Document – any record in any form that is made by or received by the Department of Emergency Management or the EOC Incident Management Team, in connection with the transaction of public business.
- For Official Use Only (FOUO) – intended to be used for the conduct of official business use of the immediate recipient addressee.
- Individually-identifiable – information which by inference or circumstance is sufficient to identify a specific individual.
- Information – any written document, paper, correspondence, completed form, bound record book, photograph, film, sound recording, map drawing, machine readable material, or other documents, regardless of physical form or characteristics. For the purpose of this guidance, information also includes internal planning discussion and analysis, overheard radio traffic, the content of briefings, informal discussion of strategy or tactics, or any verbal business of the EOC.
- Need-to-know – additional limitation of dissemination beyond the FOUO designation; “need-to-know” limits the information to persons with the direct business reason for having it.
- Released – disseminated or discussed outside of the Emergency Operations Center with or without approval.

APPROVED



Robert W. Hamlin, Program Manager
April 2008