Indiana Department of Homeland Security WebEOC Policy

18 January 2017

Scope

The State of Indiana, specifically the Indiana Department of Homeland Security (IDHS), maintains a crisis information management system, commonly referred to as WebEOC, to manage large-scale events and disasters, and to support and increase public safety information sharing. One of the primary objectives of WebEOC is to provide the State Emergency Operations Center (SEOC) with a platform to manage information from all 92 counties. WebEOC also serves as a collaborative tool for each county to provide local incident commanders, county command level personnel and city/county leaders with one common operating picture and to maintain situational awareness of public safety operations, sensitive information and utility problems and/or disruptions.

WebEOC is also used as a gateway to share information among County EOCs, IDHS Districts, State EOC, state, federal and local public safety entities and critical infrastructure partners. This information sharing allows authorized users to make informed decisions regarding public safety operations during events and/or disasters and supports vast statewide boundless collaboration. WebEOC is also the primary means of communication between County EOCs and the State EOC.

Policy

IDHS shall maintain control of user access to WebEOC and limit such access to key personnel involved in emergency operations and/or those who have the need to communicate with a County EOC or the State EOC. All users are required to sign a User Agreement (see appendix A) in accordance with this policy. Additionally, all users are required to attend the standard WebEOC class prior to use. All users shall comply with the User Agreement.

County emergency managers shall have the ability to create positions for their own county. Each county shall have three separate positions for their county, including emergency management position, public safety position and general position. Emergency Management Directors will be provided with a Personal Access Code (PAC) for each position in order to create positions. Directors will safeguard their PAC. Only the IDHS WebEOC Administrator shall have the ability to create or delete PACs.

IDHS reserves the right to terminate use of the WebEOC system or user at any time, including violations of this policy, operational security or negligent use.

Access

Access to the WebEOC system is intended for IDHS employees involved in response operations and state or federal operational personnel who require access to real time information for the purpose of making informed decisions during events, incidents or disasters. Access is also intended for county emergency management personnel, county public safety commanders who serve in an operational management capacity during large-scale events or disasters and utility or critical infrastructure operational directors. Personnel will only be granted access if there is a true need to communicate with an EOC, a need for operational situational awareness, or access to management tools used within WebEOC. WebEOC access shall be limited to the listing of personnel/positions on the following pages. Access by individuals not fitting these categories may be considered on a case-by-case basis, and approval for access will be determined solely by the IDHS WebEOC Administrator. The general public, news media or others not outlined in this policy shall not have access to WebEOC.

In order to maintain security of the system and manage the large number of users, access requirements will be strictly enforced. All users are required to maintain a valid agency email address in the system. Users are required to log into the system at least once during **each 30-day period**. Failure to successfully log into the system during this time frame will result in termination of access. Users are required to change their password every 90 days. Passwords will meet strong password criteria to ensure system security as determined by the WebEOC Administrator.

User Names

All user names need to identify the users by their name. All user accounts shall comply with the standard of last name, first name. See the example below. Smith, John.

State Level Access
Homeland Security Personnel
All IDHS employees involved with response or recovery operations shall maintain access to the system along with all division leadership. Persons with volunteer or associate status will be approved on a case –by-case basis by the WebEOC Administrator.
Departments/Bureaus of the State of Indiana
State Agency Directors shall have access to WebEOC along with department/division managers who serve in an operational level capacity during emergency operations. Personnel who serve in the State Emergency Operations Center with the authority to allocate resources may receive access upon approval of their departmental director and approved by the WebEOC Administrator.
National Guard Indiana
Commanders with operational management shall have access to WebEOC. All personnel who serve in the Joint Operations Center (JOC) shall have access to WebEOC. Additional personnel may receive access upon approval of their divisional

commanding authority.
Health Services
The Director of Indiana State Department of Health or a designee shall control access to restricted health information. Only approved personnel will have access to such information.
Indiana Intelligence Fusion Center
Only personnel approved by the Director of the Indiana Intelligence Fusion Center may have access to area controlled by the IIFC.
Non-Governmental Organizations/Non-State Employees
Select personnel from non-governmental organizations may be granted access based upon the need to support the State EOC and operational functions as determined by the WebEOC Administrator. This may include personnel serving in the capacity as an Emergency Support Function (ESF) or subject matter expert.

County Level Access
Emergency Management Personnel
Emergency Management Directors, emergency management personnel, including full-time, part-time; volunteer staff as determined by the Emergency Management Directors.
Law Enforcement
Sheriff, Chief of Police, designated command personnel who serve at an operations level, SWAT commanders, intelligence analysts, officers assigned to full-time homeland security/domestic preparedness roles and dispatchers.
Fire
Fire Chief, designated command personnel who serve at an operations level, special operations officers such as Hazmat commanders, dive commanders or officers assigned to a district task force and/or Indiana Task Force 1 and dispatch supervisors.
Emergency Medical Services, Health Departments and Hospitals
Director of Operations and Shift Commanders, HazMat personnel, pandemic managers, hospital emergency operations center personnel, security directors, emergency room staff, epidemiologists and dispatch supervisors.
Public Works, Other City Departments and Transportation Groups
Department Directors and Division administrators involved in emergency operations. Operations managers and personnel involved in emergency operations as approved by department directors. Emergency management personnel and dispatch supervisors.
Utilities

Utility Directors and/or operational managers, personnel who acts as the liaison with emergency management and dispatch supervisors.
Critical Infrastructure
Facility managers, operations managers, security personnel, building owners and business owners involved with emergency operations.
Emergency Management Partners
Select personnel from the Red Cross, communications groups, ESFs and others as determined by the County Emergency Management Director.

Termination and Separation

Personnel who have been granted access to WebEOC shall immediately notify their County Emergency Management Director and/or the WebEOC Administrator upon separation from the agency or entity in which access rights were granted. Additionally, personnel shall immediately notify the Emergency Management Director and/or the WebEOC Administrator should their position change within their agency to a position that no longer requires access.

Approval

This policy is hereby approved as represented by the signature below.

_____ _____

Stephen Cox
Executive Director
Indiana Department of Homeland Security

Date

Appendix A

WebEOC User Agreement

Last Updated: 18 January 2017

All personnel with access to WebEOC shall observe and strictly adhere to the following access requirements:

1. Official Business Only
The Indiana Department of Homeland Security crisis information management system, known as WebEOC, is for official business use only. Users shall have no expectation of privacy in its use.

2. Audit of User Activities
All transactions are subject to recording and routine review for inappropriate or illegal activity conducted.

3. Sanctions
A violation of security requirements could result in termination of WebEOC access privileges and appropriate disciplinary action up to and including civil and criminal actions to the extend allowed by law. The Indiana Department of Homeland Security declares that all information in WebEOC that meets an exception under IC 5-14-3-4(b) is considered confidential.

4. Downgrading/Declassifying
WebEOC is authorized to transmit and store sensitive but unclassified information, such as Controlled Unclassified Information (CUI), For Official Use Only (FOUO) Information and Law Enforcement Sensitive Information (LES) for use by authorized users only. Classified information designated as such by an agent or representative of the federal, state and/or local government may not be used or transmitted on WebEOC unless that information has officially been declassified by the originating classification authority.

5. User IDs and Passwords
Each user is assigned a unique User ID and password to be used for authentication. Passwords must be kept secret. It is your responsibility to protect your password. You may be held accountable for all activity under your User ID. If your account is compromised, report it to the WebEOC Administrator immediately.

a. Your password is for your use only. Lending it to someone else is a security violation and may result in termination of your WebEOC account.

b. Never disclose your password to anyone. Memorize it; do not put it in writing. Safeguard it; your password is the key to one of Indiana's most valuable resources.

c. If you forget your user name and password, you may retrieve the information using the retrieval feature on the log in page using your agency email address.

d. Immediately following a suspected or known compromise of a system password, a new password will be issued and the compromised password will be deleted.

e. A user account not accessed in a 90-day period will be locked out of the system, requiring an email to the WebEOC Administrator and positive identification to re-activate it. A user account not accessed within a 90-day period will be removed, requiring a user to be re-vetted before being granted access.

f. If you leave the terminal unattended for any reason, log off. An unattended terminal is vulnerable to masquerading.

6. Report Security Violations
If you become aware of any violation of these requirements or suspect that your password may have been used by someone else, it is your responsibility to report that information immediately to the WebEOC Administrator at WebEOC@dhs.in.gov.

7. Displaying Information
You will not provide demonstrations of WebEOC to contractors or other vendors at any time. WebEOC is not to be displayed where it could be viewed by unauthorized users, the general public or the news media.

8. Demonstrating the Software
Users are not permitted to demonstrate the software to non-WebEOC users, vendors, Contractors and/or private companies involved in software development. Failure to comply with this requirement is a direct violation of the WebEOC license and may carry civil penalties.

Appendix B

WebEOC User Agreement Signature Page

If you have any questions about the proper operation or security of the WebEOC system entrusted to you, contact WebEOC Administrators at WebEOC@dhs.in.gov

Agency & Supervisor Information

Agency/Organization: _____

Department: _____

Supervisor's Name: _____

Supervisor's Email: _____

Supervisor's Phone: _____

User Information

Printed Name: _____

Signature: _____

Office Phone Number: _____

Mobile Phone Number: _____

Location (City, State): _____

Email Address: _____

Date: _____