

Last Updated 10/23/13

A. STATEMENT OF PURPOSE

This document is intended to outline the guidelines, policies, and procedures that govern the use of the WebEOC Incident Management System in the State of Arizona. All Users of Arizona's State WebEOC program must agree to these guidelines, policies, and procedures in order to access and use WebEOC.

B. POLICY

1. Definitions

- a. WebEOC – is a Crises Incident Management System (CIMS). It is a web-based system hosted by the State of Arizona and is accessible on the internet. The Uniform Resource Locator (URL) is <https://webeoc.azdema.gov>.
- b. Jurisdictions – governmental entities whose boundaries reside, all or in part, within Arizona to include the State of Arizona, excluding Pima and Maricopa counties.
- c. Agencies – governmental entities that are stakeholders within Arizona but do not have jurisdictional boundaries within Arizona and non-governmental organization (NGOs) that are stakeholders within Arizona.
- d. Stakeholders – any group or entity that will or may be involved in the processes of the four phases of a disaster: planning, response, recovery, and mitigation.
- e. Vendor – Intermedix, the creator and marketer of WebEOC.
- f. State of Arizona WebEOC User Advisory Committee - representatives from Arizona Departments and local governments within the state to provide direction, advice, and decision making regarding board creation, editing, processes, and use of the WebEOC system.
- g. Administrator – a user of WebEOC who has been granted full rights to access, modify, any component of the system for which the vendor has allowed modification, includes board editing, user creation, password changes, styles and appearance, etc. *Consult license agreement for allowable style and appearance modifications.*
- h. Primary Administrator – designated as the Arizona Division of Emergency Management (ADEM) and will be an employee of ADEM. Must have at least one backup. To include Mapper, Resource Manager, and Fusion.
- i. User Advisory Committee (UAC) – A representative group of users who consider, define, and approve proposals to new boards and processes, or changes to existing boards or processes and recommend changes to this policy document. The WebEOC Primary Administrator will lead the User Advisory Committee.
- j. Incident Administrator – a user of WebEOC that has been given permission to create or modify incidents for their jurisdiction. Incident Administrators do not have permission to delete or archive incidents.
- k. Unlock Administrator – a user of WebEOC that has been given permission to unlock users from having their accounts disabled.
- l. Mapper Administrator – a user of WebEOC that has been given permission to create or modify GIS data for their jurisdiction to be shown in Mapper.

- m. Resource Manager Administrator – a user of WebEOC that has been given permission to create or modify inventory data for their jurisdiction.
- n. User – a user of WebEOC that has been given access credentials to access and interact with the system. A user may have read only, read/write, read/write/delete permissions for any given item. A user may have more or less items to view depending on the credentials used to access the system.
- o. Position – positions are used in WebEOC to define roles a user(s) is assigned to fulfill in the Emergency Operations Center (EOC) during a disaster, exercise, or training incident.
- p. Groups – positions are assembled into groups and it is within these groups that the permissions to view more or less items in the control panel are defined as well as the allowable operations within each item.
- q. Control Panel – the main operating window of WebEOC after log on to the system. Can be composed of Boards, Menus, Tools, Plug-ins, and links.
- r. Boards – control panel items that are used to document, display, or share information.
- s. Menus – a collection of related control panel items.
- t. Tools – a collection of vendor supplied functionality and basic plug-ins.
- u. Plug-ins – a collection of specific and more advanced vendor supplied applications and functionality that hook into WebEOC’s existing framework.
- v. Links – a collection of links to documents or websites in or outside of the local network.

2. Responsibilities

- a. The Arizona Division of Emergency Management (ADEM) – acts as the Primary Administration body of WebEOC; designates staff members to act as primary and backup Administrators; completes and updates this and any additional policies or procedures for the administration, use, and maintenance of the system; trains Unlock Administrators and maintains the unlock procedures documents; trains staff from jurisdictions and agencies to use the system; trains designated staff from jurisdictions to be Incident Administrators; work with Department of Emergency and Military Affairs (DEMA) IT to coordinate support and update of WebEOC Hardware, web server and database software; work with vendor to resolve issues with the WebEOC software and any updates to the software;
- b. Jurisdictions and agencies – designate personnel who will be trained on WebEOC as users and identify at least two (2) users that will be trained as Incident Administrators; identify at least two (2) users that will be trained to train internal staff on WebEOC and its role in their respective jurisdiction (can be the same 2 users that act as Incident Administrators); may also be asked to provide at least one user to participate in the State of Arizona User Advisory Committee (UAC)
- c. User Advisory Committee – consider, define, and approve proposals to new boards and processes, or changes to existing boards or processes and recommend changes to this policy document. The WebEOC Primary Administrator will lead the User Advisory Committee.
- d. Administrator – manage the system; board building, process building, user, position, and group maintenance of the system; assist users with questions and issues about the system including unlocking user accounts, resetting passwords, and adding appropriate incident access

- e. Incident Administrators – create incidents in WebEOC that need to be managed by their respective jurisdiction and add the appropriate groups to access the incidents; edit existing incidents to remove appropriate groups from access to incidents; request an incident be archived by a Primary Administrator
- f. Unlock Administrators – assist users that have been disabled access to the system by unlocking their user accounts
- g. Mapper Administrator - adhere to proper symbology standards (see guidelines on symbology at [Federal Interagency Geospatial Concept of Operations](#)), are responsible for the maintenance of their data, and its publication on the GIS server.
- a. Resource Manager Administrator - Resource manager administrators are responsible for the upkeep of their data within the Resource Manager application of WebEOC.
- b. Users – use the system within the operating procedures and guidelines as part of the position assigned by the respective jurisdiction

3. Proper Usage

- a. Administrators
 - i. Create and edit boards and processes approved by the UAC
 - ii. Create and edit menus of related boards approved by the UAC
 - iii. Organize users and/or positions into groups based on jurisdictional and positional operations
 - iv. Document all changes made in the system
 - v. Use built-in board builder to create or edit boards; may use built-in code editor or third party code editor; must ensure well-formed XML and use proper HTML coding; JavaScript may also be used to enhance user experience
 - vi. Utilize the system Application Programming Interface (API) to interact with other non-WebEOC systems to extract data out of or enter data into WebEOC; use proper security measures to protect the system, database, log on credentials, and sensitive incident information
 - 1. Should the UAC provide guidance regarding the use of the API?
 - 2. If so, Primary Administrator will provide input as to the feasibility to create the interfaces that interact with WebEOC's API and third-party systems
- b. Incident Administrators
 - i. Create Incidents for their respective jurisdictions using proper procedures
 - ii. Edit active Incidents by adding or removing groups' access to a closed Incident
 - iii. Request the Archiving of an Incident by a Primary Administrator
- c. Unlock Administrators
 - i. Assist Users that have been disabled access to the system
- d. Mapper Administrators
 - i. Publish data for their respective jurisdictions using proper procedures
 - ii. Edit active GIS data to better reflect the incident as needed
- e. Resource Manager Administrators
 - i. Upload inventory data from their respective jurisdictions using proper procedures.

- ii. Edit and maintain their inventory data to best reflect its status
- f. Users
 - i. Use the system during actual emergencies as well as in the following situations: exercises, training, or any other demonstration that constitutes an education of the system or its related processes.
 - ii. A jurisdiction or agency may use the system in a non-emergency capacity if the procedures and processes further the response capabilities of the jurisdiction or agency and approved by the UAC. Examples include: 24 hour watch desk/office, monitoring a board that is continuously updated programmatically via the API, making board, feature, or process enhancements suggestions via the Feature Requests Board, etc.
 - iii. Ensure that all information entered during a real emergency into the system is correct to the best of one's ability to determine, timely, and appropriate. During exercises, false or fabricated information may be used to further the play of the exercise if it is within the objectives of the exercise. This also applies to demonstrations and training sessions.
 - iv. Individual users must ensure that contact and profile information is current at all times. This information will be reviewed and updated each time a User logs into WebEOC. If individual user information is not updated within at least ____ days, a notice will be sent to the user requesting that they update their profile. If user information has not been updated within ____ days of notification then the user's access to WebEOC will be suspended and the user's agency/jurisdiction will be notified. Failure to keep user profile information current may result in termination of user access.

C. PROCEDURES

1. Delegation of Administrative Permissions
 - a. Within ADEM – As the primary administrative body, ADEM Logistics Chief will designate one Primary Administrator and at least one back up administrator.
 - b. Within State of Arizona Government –
 - i. The Primary Administrator will have discretion to assign or remove administrative privileges to individual users in other State of Arizona Departments or Offices
 - ii. An administrator outside of ADEM cannot assign or remove full administrative privileges to any other user, but must request it from the Primary Administrator
 - iii. An administrator outside of ADEM may assign or remove users from Admin Profiles in their own department or office new assignments must have the Primary Administrator's approval
 - c. Jurisdictions and agencies outside of State of Arizona Government
 - i. The Primary Administrator will have discretion to assign or remove incident administrative privileges to individual users in jurisdictions and agencies
 - ii. Incident administrators for individual jurisdictions cannot create incidents for other jurisdictions and cannot modify access to incidents created by other jurisdictions

2. Creation of New Positions and Groups
 - a. ICS/NIMS Organization – Administrators that create positions shall adhere to National Incident Management (NIMS) principles when creating and naming positions where possible and in accordance with the respective agency's Emergency Operations Plan
 - b. Within ADEM – the Primary Administrator will create new positions and groups for ADEM
 - c. Within Arizona Government – the Primary Administrator will create new positions and groups for any users within Arizona Government; Departmental Administrators can create positions and groups in their respective Departments
 - d. Jurisdictions and Agencies outside of Arizona Government – the Primary Administrator will create new positions and groups for any jurisdictions and agencies outside of Arizona Government
 - e. Naming of Groups and Positions – one of two options below
 - i. Names will have a recognizable acronym depicting the name of the Department within the state Arizona in the front of the Group or Position Name separated by a space. Example: ADEM Operations Section
 - ii. Names will have the county's/agency's 4 letter acronym name in front of the Group or Position name separated by a space. Example: YAVA Operations Section Chief
 - iii. Names will have the Tribal Nation's 4 letter acronym name in front of the group or Position name separated by a space.
3. Creation of New User Accounts
 - a. Within ADEM – the Primary Administrator will create all user accounts for ADEM staff.
 - b. Within Arizona Government
 - i. the Primary Administrator will create all user accounts for all staff in the state of Arizona that are designated to respond to the Emergency Operations Center in an activation event
 - ii. a Department Administrator may create new user accounts for personnel in their respective departments
 - c. In jurisdictions and agencies outside of Arizona government – the Primary Administrator will create all user accounts for all staff in jurisdictions and agencies outside of Arizona government
4. Change or Deletion of Positions and Groups
 - a. Within ADEM – the Primary Administrator will change or delete any positions or groups as necessary
 - b. Within Arizona Government – Department Administrators may only change or delete positions or groups they have created for their respective departments
 - c. Jurisdictions and Agencies outside of Arizona Government – the Primary Administrator will change or delete any positions or groups as necessary; changes or deletions that could affect the usage, processes, or operations of multiple municipalities should be approved by the Primary Administrator
5. Change or Deletion of User Accounts
 - a. Within ADEM – the Primary Administrator will change or delete user accounts as necessary

- b. Within Arizona Government – the Primary Administrator will change or delete user accounts as necessary; Department Administrators can change or delete user accounts of their respective departments
 - c. Jurisdictions and Agencies outside of Arizona Government – the Primary Administrator will change or delete user accounts as necessary
6. Creation of New Boards
- a. Within ADEM operations – the Primary Administrator will create new boards as necessary in consultation with the management
 - b. Within Arizona Government – the Primary Administrator will create new boards as necessary in consultation with that department; Department Administrators can create new boards used by their respective departments in consultation with their respective management AND when such changes could affect the interoperability between departments
 - c. Jurisdictions and Agencies outside of Arizona Government – the Primary Administrator will create new boards as necessary in consultation with the UAC
 - d. Naming of Boards – names should contain the naming conventions, should contain a long enough name to be descriptive, but not unreasonably long;
7. Editing Boards
- a. Within ADEM operations – the Primary Administrator will edit boards as necessary in consultation with the management
 - b. Within Arizona Government – the Primary Administrator will edit boards as necessary in consultation with that department; Department Administrators can edit boards used by their respective departments in consultation with their respective management AND when such changes could affect the interoperability between departments
 - c. Jurisdictions and Agencies outside of Arizona Government – the Primary Administrator will edit boards as necessary in consultation with the UAC
 - d. Data linking of Boards – before editing any boards, care must be taken to ensure data communication between boards is not affected or if communication between boards is among the edits that consultation is coordinated between creators/owners of each board data linked or data links from other boards to the board being edited
8. Deleting Boards
- a. Within ADEM operations – the Primary Administrator will delete boards as necessary in consultation with the management
 - b. Within Arizona Government – the Primary Administrator will delete boards as necessary in consultation with that department; Department Administrators can delete boards used by their respective departments in consultation with their respective management AND when such changes could affect the interoperability between departments
 - c. Jurisdictions and Agencies outside of Arizona Government – the Primary Administrator will delete boards as necessary in consultation with the UAC
 - d. Data linking of Boards – before deleting any boards, care must be taken to ensure data communication between boards is not affected or coordination is made with the creators/owners of boards that send data via data links to the board being deleted

9. Creation of New Incidents
 - a. Within ADEM operations
 - i. the Primary Administrator or Incident Administrators will create new incidents when a situation warrants that ADEM document a specific emergency; the Primary Administrator or Incident Administrators may create incidents to support an exercise, training, or demonstration and assign the appropriate groups to access the incident
 - ii. the Primary Administrator, Department Administrator, and Incident Administrator will create a new incident for their respective agencies at the beginning of each quarter to document routine incidents or duty officer logs for ADEM and assign the appropriate groups to access the incident
 - b. Within state of Arizona Government
 - i. the department Administrator will create incidents when a department requests an incident be created
 - ii. Department Administrators can create incidents to be used by their respective departments to document and respond to an emergency
 - iii. a Department Administrator can create incidents to support an exercise, training, or demonstration and assign the appropriate groups to access the incident and notify the Primary Administrator when an incident is created
 - c. Jurisdictions and Agencies outside of state of Arizona Government
 - i. the agency or jurisdiction Administrator will create incidents for jurisdictions and agencies when requested by them
 - ii. Incident Administrators can create incidents to document and respond to emergencies in their respective jurisdictions and assign the appropriate groups to access the incident
 - iii. Incident Administrators can create incidents to support an exercise, training, or demonstration and assign the appropriate groups to access the incident and notify the Primary Administrator when an incident is created
 - d. Naming of Incidents – one of two options below
 - i. Names will have a recognizable acronym depicting the name of the Department within state of Arizona in front of the Incident Name separated by a space and include the month and year the incident was created. Example: *ADEM Palo Verde Exercise March 2011*
 - ii. Names will have the county/city/state agency name in front of the Incident Name separated by a space and include the month and year the incident was created. Examples: *Flagstaff Mall Shooter Oct 2011, La Paz County Flooding March 2011, ADHS 2009 Flu Season*
 - e. Duty Officer/Watch Officer and other monitoring Incidents
 - i. Each entity that has the staff capability will have a monitoring incident that is archived quarterly while a new monitoring incident is created in its place.
 - ii. These incidents are meant to capture any activity during the quarter that DO NOT rise to the level of full or partial EOC response, but documentation is needed or the incident has the potential to rise to a full or partial EOC response in the future.
10. Addition of GIS data for Mapper
 - a. Within ADEM operations

- i. The GIS coordinator will publish GIS data to a GIS server and will add it to Mapper.
 - ii. Proper caching, scaling and symbology will be observed
 - b. Within State of Arizona government
 - i. The agency GIS coordinator will publish GIS data to a GIS server and ADEM's GIS coordinator will add it to Mapper.
 - ii. Proper caching, scaling and symbology will be observed
 - iii. The agency GIS coordinator will notify the ADEM GIS coordinator each time that GIS data is published to the WebEOC Mapper
 - c. Jurisdictions and Agencies outside of state of Arizona Government
 - i. The agency GIS coordinator will publish GIS data to a GIS server and ADEM's GIS coordinator will add it to Mapper.
 - ii. Proper caching, scaling and symbology will be observed
 - iii. The agency GIS coordinator will notify the ADEM GIS coordinator each time that GIS data is published to the WebEOC Mapper
11. Addition of Resource Manager data
- a. Within ADEM operations
 - i. The person uploading the data is considered the custodian of the data
 - ii. Custodians are responsible for the accuracy of the resource data at all times
 - b. Within State of Arizona government
 - i. The person uploading the data is considered the custodian of the data
 - ii. Custodians are responsible for the accuracy of the resource data at all times
 - c. Jurisdictions and Agencies outside of state of Arizona Government
 - i. The person uploading the data is considered the custodian of the data
 - ii. Custodians are responsible for the accuracy of the resource data at all times
12. Termination
- a. Termination Of Use
 - i. Renewal. This agreement has no termination date and shall remain in effect as long as the user(s) continue to utilize WebEOC.
 - ii. Termination Without Cause. Any user may terminate use of this program by notifying the Primary Administrator with 30 days notice and requesting that their access (profile) be terminated.
 - iii. The Primary Administrator may terminate a user's access to WebEOC at any time without prior notification. If a user's access is terminated the Primary Administrator will notify the user within 30 days of the reason for termination.
 - iv. Upon termination of access any and all user data may be overwritten, erased, encrypted or otherwise rendered unrecognizable at the discretion of the Primary Administrator
13. Costs
- a. Fees and Payment
 - i. There shall be no cost or payment required for users to access WebEOC.
 - ii. User's shall maintain, at their expense, a secure high speed internet connection and valid license to any third party software products required to effectively and lawfully access WebEOC.
 - iii. Number of user profiles: Although WebEOC is provided at no cost to agencies, there shall be a limit on the number of users allowed from

agency. The number of users will be commensurate with the effective operations of the agencies emergency response program. Not every staff member in an agency will have access to WebEOC.

- b. Cost of additional Features or add-ons
 - i. Any user requesting the addition of add-on features, plug-ins or other software linked to WebEOC may be required to pay for the addition. All additional add-on features, plug-ins or software must be approved by the UAC.
 - ii. Any add on features, plug-ins or software linked to WebEOC shall be made available to all users as a matter of course.
 - iii. Users funding special add-on features, plug-ins or software to be used for classified information may request restricted access to the data. For instance, some features may be relevant to law enforcement or intelligence gathering activities and the funding User may request that the Primary Administrator restrict access to limited number of users.
- c. At any time the Primary Administrator may enter into a separate agreement with a user for fee based access. Any such agreement shall define the roles and responsibilities of each party and the costs to the user(s), if any. Any such agreement will be reviewed and approved by the ADEM Assistant Director for Logistics.

14. Service Levels Provided by Primary Administrator

- a. All support calls from users shall be logged and tracked by the customer support desk. All requests for support shall be assigned a severity level. In each case every attempt will be made by the Primary Administrator to respond within 24 hours.
 - i. Severity Level 1: Any and all issues that prevent users from accessing WebEOC. This may include forgotten passwords, creation of user profile, etc. Resolution: access granted to user within 24 hours.
 - ii. Severity level 2: Interruption of WebEOC such as internet, network, or server/software breakdown affecting some or all users access to some or all features of WebEOC. Resolution: Response to support request within 24 hours; restoration of WebEOC access is variable dependant of cause of interruption.
 - iii. Severity Level 3: Catastrophic failure of WebEOC, internet, network, or server/software such that WebEOC is completely unusable or inaccessible and restoration will be a significant period of time. Resolution: Primary Administrator will immediately notify all users of the interruption and may initiate WebEOC Failover procedure. In accordance with the WebEOC Failover Procedure checklist all users will be notified and redirected to alternate WebEOC location.
- b. Scope of Services Provided by Application Service Provider
 - i. The Primary Administrator will be the sole contact with the application service provider hosting Arizona's State WebEOC program.
- c. The Primary Administrator will coordinate WebEOC Failover procedure with the application service provider in accordance with the WebEOC Failover Checklist.

15. Limitations on Use

- a. Access to the WebEOC may not be rented, leased, sold, sub-leased, assigned or otherwise transferred for value by a user to any third party. All new user credentials will be created by the Primary Administrator.

- b. Users shall not conduct any load testing, performance testing or any other test of the system which may degrade performance or limit or adversely impact availability of the system for other customers.
16. Security of Information
- a. All organizations must use accepted standards of information management to ensure the overall security of WebEOC.
 - b. Users will establish and adhere to organizational policies and procedures with respect to data classification and management, data and system back-ups, account and password management, physical security and access, network configuration and access, change management, media management and destruction, security training and awareness, and continuity of operations.
17. Hybrid Failover Procedures
- a. In the event of interruption to the usability of WebEOC in the Arizona Department of Emergency and Military Affairs data center, a failover procedure may be initiated.
 - b. DEMA IT and the WebEOC Primary Administrator will determine the need for failover. Failover will be conducted in accordance with the SEOC WebEOC Hybrid Failover Checklist.
18. Policy Development and Maintenance
- a. Overall responsibility for the coordination, development, revision and maintenance of this policy lies with the ADEM Assistant Director for Logistics. The WebEOC Primary Administrator is tasked by the Logistics Director with daily policy management.
 - b. The policy will be reviewed and updated at least annually by the UAC.
 - c. The UAC will meet quarterly to review this policy and any recommendations and changes by UAC members, agencies or other users to WebEOC.