



STATE OF WASHINGTON
MILITARY DEPARTMENT
Camp Murray • Tacoma, Washington 98430-5000

WebEOC User Policy

Scope

The Washington Military Department maintains a crisis information management system, commonly referred to as WebEOC, available for use by Washington State agencies, local governments, tribes, private entities and federal entities ("Users") as a collaborative tool for managing and sharing emergency management and public safety related information. The purpose of WebEOC is to provide a network platform for Users to post, receive, share, organize, process, and manage emergency and public safety information from and with the State Emergency Operations Center (EOC) for emergency management purposes authorized under chapter 38.52 Revised Code of Washington (RCW). This policy addresses User access and responsibilities related to use of the WebEOC platform.

Definitions

- Emergency Management Division Director (EMD Director): The Director of the Military Department's Emergency Management Division, and sponsoring authority for WebEOC. The EMD Director or designee approves requests to become a WebEOC User and revokes such approval, if needed.
- User: A Washington state agency, local government, tribe, federal entity, private entity, or other entity that has been authorized use of WebEOC by the EMD Director or designee.
- WebEOC Administrator: The position within the Military Department responsible for the administration, training, and technical support of WebEOC. The WebEOC Administrator creates User accounts and grants data access permissions based on User credentials.
- WebEOC Coordinator: Each User will designate a WebEOC Coordinator to provide local administrative and technical support. WebEOC Coordinators will serve as liaisons with the WebEOC Administrator.

Policy

WebEOC is a communication network platform provided as a service by the Military Department for Users to manage and share emergency management and public safety related information as each User deems appropriate subject to its own statutory authority and control. In providing this service, the Military Department (1) retains the right and sole discretion to grant, deny or terminate access to WebEOC by any User for any or no reason, with or without cause, and (2) will provide a WebEOC Administrator to maintain WebEOC functional capability, create WebEOC accounts, and provide operational administration and technical support.

User access to WebEOC shall be authorized pursuant to this policy.

An entity seeking establishment of one or more WebEOC accounts shall not be granted access to WebEOC until the entity has submitted a request to, and received approval from, the EMD Director (or designee) to become a User. EMD Director (or designee) approval will not be considered until an authorized representative of the entity has signed and submitted a User Agreement to the EMD Director (see Appendix A), which is incorporated into this agreement by reference.

Approval or denial of any request for User accounts shall be at the sole discretion of the EMD Director (or designee). Upon approval of the User Agreement by the EMD Director (or designee), the WebEOC Administrator will create one or more WebEOC accounts for the User. User personnel who may access the User's WebEOC accounts must complete the standard WebEOC class at the direction of the WebEOC Administrator prior to using WebEOC, which training will be available by webinar, classroom, or tutorial. Only the WebEOC Administrator is authorized to create or delete WebEOC accounts. Access by any User may be terminated at any time, with or without notice, and for any or no reason, with or without cause, at the sole discretion of the EMD Director (or designee).

Each User is solely responsible for ensuring that the User's WebEOC accounts are used, operated and maintained in accordance with this policy, the User Agreement, and all applicable state and federal laws and regulations. It is the User's responsibility to ensure all User personnel who may access the User's WebEOC accounts abide by this policy and the User Agreement.

Each party to this agreement agrees to defend and indemnify the Military Department for any fees, costs or penalties imposed in any disagreement, mediation or litigation related to that party's records retained in the WebEOC repository, including a third party request for an injunction. The obligation to defend and indemnify remains in full force and effect regardless of an allegation or finding that Military Department personnel violated the Public Records Act.

The following entities may be approved as WebEOC Users by the EMD Director (or designee):

- Washington Military Department
- State agencies and other entities with Emergency Support Function roles in the State Comprehensive Emergency Management Plan
- Local government, private, and other entities with Emergency Support Function roles in local comprehensive emergency management plans

The Military Department may temporarily suspend elements of this policy during Phase II or higher activations of the State Emergency Operations Center (EOC) to allow specific non-User entities interim access to WebEOC to support emergency response efforts for a period of no longer than 30 days after the State EOC transitions from response to recovery operations. The Military Department will track interim accounts and terminate them within 30 days of transition to recovery unless provisions of this policy are met and a signed User Agreement is in place.

Signed: _____ Date: _____

Robert Ezelle, Director, Emergency Management Division



STATE OF WASHINGTON
MILITARY DEPARTMENT
Camp Murray • Tacoma, Washington 98430-5000

WebEOC User Agreement

As a condition of being approved as a WebEOC User, the undersigned, as the User's authorized representative, agrees to observe and strictly adhere to the following requirements:

1. Official Business Only

The Washington Military Department maintains a crisis information management system, commonly referred to as WebEOC, available for use by Washington state agencies, local governments, tribes, private entities and federal entities ("Users") as a collaborative tool for managing and sharing emergency management information. The purpose of WebEOC is to provide a network platform for Users to post, receive, share, organize, process, and manage emergency and public safety information from and with the State Emergency Operations Center (EOC) for emergency management purposes authorized under chapter 38.52 RCW. No other use shall be permitted, and personal use is prohibited. Users shall have no expectation of privacy in the use of WebEOC.

2. Disclosure of Public Records

All information retained on the Military Department's WebEOC server, including information about use of WebEOC or posted by a User onto WebEOC, is a public record subject to public disclosure by the Military Department under chapter 42.56 Revised Code of Washington (RCW). In cases where information within WebEOC created by or pertaining to a User ("User information") is responsive to a public records request, and it appears that information may be exempt from public disclosure, the Military Department will notify the User of the request, and include in the notification the following:

- a. A copy of the public records request.
- b. A copy of the User information pending disclosure.
- c. The need (if any) for assistance to identify information that may be exempt from public disclosure.
- d. The date the records will be released to the requestor unless the User obtains a court order enjoining that disclosure under RCW 42.56.540.

If the User fails to obtain a court order enjoining disclosure prior to the release date, the records will be released to the requestor on the date specified.

3. Audit of User Activities

While the Military Department does not monitor and is not responsible for information posted on WebEOC, all activity is subject to recording and routine review for inappropriate, unauthorized, or illegal activity conducted.

4. Termination of Use

The Military Department reserves the right to terminate use of the WebEOC system and a user account for any reason and at any time within its sole discretion, including, but not limited to, violations of law, this Agreement, operational security or negligent or unauthorized use.

5. Account Restrictions

If the User or the Military Department determines that an individual's use of the User's WebEOC account violated a law, this Agreement, or operational security, or was for an unauthorized purpose, the Military Department and the User may agree the User can continue using WebEOC if the User restricts the individual from accessing any User account, investigates the violation or unauthorized use, and implements appropriate disciplinary actions, if applicable.

6. Sanctions

A violation of law, this Agreement or operational security involving the use of WebEOC may result in termination of WebEOC access privileges, appropriate disciplinary action (if applicable), and civil and criminal sanctions as allowed by law.

7. Defense and Indemnification

The User agrees to defend and indemnify the Military Department for any fees, costs or penalties imposed in any disagreement, mediation or litigation related to that party's records retained in the WebEOC repository, including a third party request for an injunction. The obligation to defend and indemnify remains in full force and effect regardless of an allegation or finding that Military Department personnel violated the Public Records Act.

8. User Accounts and Passwords

Each User is assigned an appropriate number of accounts, usernames, and passwords to be used for authentication. Passwords must be kept secret. It is the User's responsibility to protect User passwords. The User will be held accountable for all activity under the User's accounts. If a User account is compromised, the User must report it to the WebEOC Administrator immediately.

- a. A User password is for the User's use only. Disclosing the password outside to a non-User entity or individual is a security violation and may result in termination of the User's WebEOC accounts.
- b. Never disclose a User password to anyone. Memorize it; do not put it in writing.
- c. Users may retrieve forgotten usernames or passwords by emailing the WebEOC Administrator.
- d. Immediately following notification to the WebEOC Administrator of a suspected or known compromise of a User password, a new password will be issued and the compromised password will be deleted. If the compromise was due to non-compliance with the WebEOC policy or User Agreement, the User's accounts may be terminated.
- e. A User account is locked out of the system if the User makes 5 unsuccessful login attempts. The User can contact their designated WebEOC Coordinator or the WebEOC Administrator to have their account unlocked, or wait 30 minutes.

- f. If the User leaves a terminal unattended for any reason while accessing WebEOC, the User must log off WebEOC. An unattended terminal is vulnerable to masquerading and is a security risk.

9. Report Security Violations

If the User becomes aware of any violation of these requirements or suspect that the User's password(s) may have been compromised or acquired by a non-User, it is the User's responsibility to report that information immediately to the WebEOC Administrator.

10. Displaying Information

Users are not permitted to display information on, or provide demonstrations of, WebEOC to contractors, vendors, or unauthorized persons at any time. WebEOC is not to be displayed where it could be viewed by unauthorized persons, the general public, or the news media. Refer any such requests to view WebEOC to the WebEOC Administrator.

11. Demonstrating the Software

Users are not permitted to demonstrate the software to unauthorized persons, 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 in addition to resulting in termination of WebEOC access privileges and appropriate disciplinary action.

Users shall direct any questions regarding the proper operation or security of the WebEOC system to the WebEOC Administrator.

User's Authorized Representative:

I have read and agree to the User Agreement.

Organization/Entity: Pacific County

Print Name: Lisa Ayers

Title: Chair, Board of County Commissioners

Signature: _____ Date: _____

Emergency Management Division Director or Designee:

I have authorized the User organization/entity named above to have one or more Washington State WebEOC Accounts.

Print Name: _____

Title: _____

Signature: _____ Date: _____