

Service Level Agreement

Between: \_\_\_\_\_ and \_\_\_\_\_  
Dispatch Center Name Department Servicing IT Organization

I. PURPOSE

This service level agreement establishes guidelines to be employed in support of the \_\_\_\_\_ in its role of providing district coordination and dispatching support via networked computers which are utilized by a variety of temporarily detailed, short-term, non-federal emergency response personnel. Specifically, it defines security procedures and processes to initiate and maintain user profiles and passwords for the Dispatch Center computers on the Servicing Agency IT corporate network.

II. RESPONSIBILITIES

The Servicing Agency Information Technology (IT) Specialist in their role of system administrator will establish, maintain, and reset necessary user profiles (also referred to as user IDs) for short-term non-federal emergency response personnel. The user ID and password will be provided to the Dispatch Center Manager or Office Coordinator in a sealed envelope that has been signed across the seal. The Dispatch Center Manager or Office Coordinator will keep these user IDs in a secure location and manage their distribution to all short-term, non-federal emergency response personnel while ensuring accountability of the secure user IDs and passwords. The Dispatch Center Manager or Office Coordinator will notify the Agency IT Specialist when short-term, non-federal emergency response personnel terminate and the user id password is reset and the ID is available for reuse.

III. OPERATIONAL PROCEDURES

The Agency IT Specialist will initially create \_\_\_\_\_<sup>1</sup> user accounts and provide a list of them along with the sealed envelopes containing account IDs and passwords to the Dispatch Center Manager or Office Coordinator. The Dispatch Center Manager or Office Coordinator will keep these items in a secured area. When short-term, non-federal emergency response personnel are requested and report to work, the Dispatch Center Manager or Office Coordinator will distribute the information packet that contains the IT Security Awareness and Best Practices handout. The user will read the IT Security Awareness handout, fill out the *Short-Term Emergency Response Personnel User Log* and sign it to acknowledge agreement to follow Agency IT Security best practices. The user receives a sealed envelope that contains the user’s assigned ID and password. During initial login, the user will be prompted to immediately change the provided password to a strong password, which will only be used by that user. Any required password reset or account unlock activity will need to be coordinated with the user’s dispatch supervisor. When the user’s assignment is completed, the Dispatch Center Manager or Office Coordinator is notified and the user ID profile list is documented with the date released. The Dispatch Center Manager or Office Coordinator notifies the Agency IT Specialist that the user ID is available for reuse and a new password is requested.

\_\_\_\_\_  
Dispatch Center Manager or Office Coordinator Date

\_\_\_\_\_  
Fire Management Officer Date

\_\_\_\_\_  
Information Technology Manager or Specialist Date

<sup>1</sup> Recommend # of workstations x 3 to accommodate possible off hour provisioning needs.