

Service Level Agreement
<Name of Office>
<Date>

I. PURPOSE

This service level agreement establishes guidelines to be employed in support of the **<name of Office>** in its role of providing district coordination and dispatching support via networked computers which are utilized by a variety of temporarily detailed short-term emergency response personnel. Specifically, it defines security procedures and processes to initiate and maintain user profiles and passwords for **<Office>** computers on the **<Bureau>** Bureau network.

II. RESPONSIBILITIES

The **<Office>** 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 emergency response personnel. The user id and password will be provided to the Office Coordinator in a sealed envelope that has been signed across the seal. The Office Coordinator will keep these user ids in a secure location and manage their distribution to all short-term emergency response personnel while ensuring accountability of the secure user ids and passwords. The Office Coordinator will notify the **<Office>** IT Specialist when short-term emergency response personnel terminate and the user id is available for reuse.

III. OPERATIONAL PROCEDURES

<Office> IT Specialist will initially create **<number of workstations x 3>** user accounts and provide a list of them along with the sealed envelopes containing account passwords to the **<Office>** Manager. The **<Office>** Manager will keep these items in a secured area. When short-term emergency response personnel are requested and report to work, the Coordinator on Duty (COD) 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 *User Log for Short-Term Emergency Response Personnel* and sign it to acknowledge agreement to follow Bureau IT Security best practices. The user receives a sealed envelope that contains the password for the login that is assigned to them. 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 immediate supervisor. When the user's assignment is completed, the COD is notified and the user id list is documented with the date released. COD notifies the **<Office>** IT Specialist that the user id is available for reuse and a new password is requested.

Dispatch Office Manager	Date	Fire Management Officer	Date
Information Technology Specialist	Date		
<Office > Information Technology Security Manager	Date	Assistant Director for Information Resources	Date