Montgomery County Fire and Rescue Service

FIRE CHIEF'S GENERAL ORDER

NUMBER: 09-16

September 10, 2009

TO: All MCFRS Personnel

FROM: Fire Chief Richard Bowers

SUBJECT: Policy for Securing Portable Data

Maintaining the security of the County's electronic data is essential to protect personal data and other sensitive/confidential information. All MCFRS personnel must comply with the applicable requirements below to ensure the necessary level of protection.

LAPTOP HARD DRIVES. All primary laptops are supported by the Desktop Computer Modernization program and are required to have hard drive encryption. The DCM program funds the cost of encryption software licenses (PointSec) and annual software maintenance for all primary laptops. If Pointsec encryption software is installed on a laptop, the Pointsec encryption icon will be visible in the system tray near the clock in ***Windows***.

If the laptop is ***not*** supported by the Desktop Computer Modernization program and Pointsec encryption software is ***not*** installed, ***County data must not be stored on the local drive of the laptop***. Please contact MCFRS IT staff if a Pointsec encryption license is required. Note that all LFRDs must fund the cost of PointSec licenses and annual maintenance for each secondary County laptop that requires a Pointsec license.

USB FLASH DRIVES. By law or regulation, protected data ***cannot*** be stored on USB Flash Drives without the approval of the Fire Chief or designee. If approved, a standard off-the-shelf USB Flash Drive, bundled with a high level of encryption and with the self-destruct function, must be used. Personnel must sign a statement that they have read the Policy and agree to comply with its provisions. Protected data includes:

- Data that can be used to identify a person, e.g., a picture or social security number;

- Medical records that are related to the physical or mental health condition of a person;
- Personnel financial information and employment records; and
- Criminal information, both adult and juvenile data, including information related to a criminal investigation.

Sensitive data may be stored only on a USB Flash Drive bundled with 256 bit AES encryption. Only USB Flash Drives issued by the MCFRS IT Office may be used**.** Personnel must sign a statement indicating that they have read the Policy and agree to comply with its provisions. Sensitive data includes:

- Identifiable information that is likely to, or that might easily be matched, to a specific person by age, gender, a home address, or nine-digit zip code;
- Medical information that describes the physical or mental health condition of a population, by medical statistics or research that involves human subjects;
- Education records that contain information directly related to a student; or
- Electronic photos, such as electronic images of fire and rescue incidents.

All other County data may be stored on an off-the-shelf USB Flash Drive, but the drive must be encrypted with shareware or freeware storage security. The MCFRS IT Office will assist staff with encrypting a USB Flash Drive. All other County data includes data that is a matter of public record.

Portable/External Hard Drives may be used only with the approval of the Fire Chief or designee. These drives must be kept in a locked office in a County facility and must be encrypted if removed from its location.

Blackberry Devices or other PDA devices that are configured to receive County messaging must be password-protected. Passwords must be activated when the device is holstered, or after 30 minutes of inactivity.