203-25

COMPUTER USAGE REQUIREMENTS

1. PURPOSE: The purpose of this Written Directive is to formulate guidelines and regulations as they pertain to computer workstation usage and security.

2. SCOPE: This directive is applicable to all personnel.

3. RESPONSIBILITY: All personnel are responsible for compliance with this directive.

4. COMPUTER WORKSTATIONS: Computer workstations are business tools, and are to be used for business purposes only. Each workstation is set up to provide the tools necessary to accomplish the tasks performed by the signed on employee. Any attempt to deliberately access any software not available to the signed on employee, or to access any restricted functions of the software provided is strictly prohibited.

5. PASSWORDS:

   A. Employees shall not disclose their password to any person other than their immediate supervisor, the Administrative Services Commander, or Information Technology Technicians for computer maintenance and repair.

   B. Employees shall not use any computer workstation that is signed on under another employee's password.

   C. Employees shall change their passwords any time that it is suspected or known that an unauthorized employee may have knowledge of it. If you need assistance in changing your password, contact the Technical Services Division office.

6. SOFTWARE: Employees are prohibited from installing any software not provided by and properly licensed to the City of Huntsville. This includes but is not limited to internet freeware. Employees may request permission from the Administrative Services Commander to install software they have purchased, provided that the original license will be on file at the Huntsville Police Department as long as the software is installed on the workstation. The manipulation or alteration of current software running on agency-owned mobile, desktop or handheld computers is prohibited.

7. HARDWARE: Employees are prohibited from installing any hardware, excluding speakers, not provided by the City of Huntsville. Requests for exceptions to this standard are to be addressed to the Administrative Services Commander and are to include approval by the appropriate Bureau Commander.

8. SECURITY: Workstations shall not be left signed on and unattended where they can be accessed by an unauthorized person. The workstation is to be locked when it is to be left unattended but the employee will return in a brief time. If the workstation cannot be locked by the utilization of a password, the workstation must be shut down to prevent unauthorized access. When employees utilize a shared workstation, the employee vacating the workstation

shall log off or otherwise shut down the computer.

9. INTERNET SITE ACCESS: Internet and e-mail are provided for business purposes only, and may be monitored at any time. Access to websites may be filtered or restricted based on an employee's assignment within the department. Access for non-sworn employees may be determined by their assignment (for example, the Police Academy secretary can have the same access as the rest of the Police Academy staff). Regardless, the Chief of Police maintains full authority to adjust any restrictions at all times. Anyone requesting to change their access must first contact the Services Bureau Commander for approval.

    A. Access to various websites is as follows:

        1. Major Crimes, Robbery and DV:

            a. Social Media;

            b. Business; and

            c. Adult sites (includes sexual and violence)

        2. Burglary, General Investigations, Police Academy, Internal Affairs, Community Resource, Crime Analysis, Web Technician, Software Technician, School Resource Officers, all sworn supervisors:

            a. Social Media; and

            b. Business

    B. Monitoring Protocol and Emergency Access:

        1. Monitoring Protocol – City IT has agreed to run monthly reports on internet activities performed by Huntsville Police personnel. These reports will be sent to the Deputy Chief of Administrative Services for review. If any abnormal activity is detected, the Deputy Chief of Administrative Services will notify the employee's supervision for review and possible action unless circumstances dictate otherwise.

        2. Emergency Access – City IT has agreed to assist the Huntsville Police Department in the event there is a critical need for immediate access to a blocked website during after hours, weekends, or holidays (non-business hours). Sworn personnel requiring immediate access to a blocked website during non-business hours must obtain supervisory approval before dispatch can call-out City IT. Supervisors approving these callouts must send an email notification to the Deputy Chief of Administrative Services.

10. VIRUS PROTECTION: All employees must be aware of the possibility of introduction of viruses by utilizing computer data from unverifiable sources. If any employee has a question of whether or not a source contains harmful data or a virus, they should contact the Huntsville Police Department, Technical Services Division for assistance.