Purpose

The Cecil County Sheriff's Office provides and maintains messaging agents and Internal and External Electronic Mail (e-mail), Internet access and computer hardware and software. As a condition of providing the previously identified network access to its employees, the Sheriff's Office places certain restrictions on workplace use.

Policy

It is the policy of the Cecil County Sheriff's Office to provide and manage Internet access, computer hardware and software to applicable personnel for the performance of their duties.

Procedures

A. System Information

1. The internal communications systems, as well as the equipment and data stored, are and remain at all times the property of the Sheriff's Office. Accordingly, all messages and files created, sent, received or stored within the system should be related to this Office's business. System wide distribution of e-mail (announcements, bulletins, etc.) requires command approval prior to distribution.

2. The Sheriff's Office reserves the right to retrieve and review any messages or file composed sent or received. It should be noted that although a message or file is deleted or erased, it is possible to retrieve the message. Therefore, the privacy of messages cannot be assured to anyone. Although electronic mail may allow the use of passwords for security, confidentiality cannot be guaranteed. It is possible for messages to be retrieved and viewed by someone other than the intended recipient.

B. E-Mail

1. When using e-mail, etiquette is important. The strategies for effective e-mail communications are as follows:
    a. Keeping messages as brief as possible will minimize reading time for recipient, therefore keeping communications efficient.
    b. Avoid communicating through e-mail on a sensitive subject that should be addressed in person if possible.
    c. Communicate confidential information in another form other than e-mail.

d. Check for accuracy and apply all good business writing, using correct grammar, spelling and punctuation.
e. Follow up if a response has not been received in a timely manner.
f. Read all messages and respond regularly.
g. Ensure that messages are deleted or saved to your hard drive, flash drive, or external storage device if applicable.

2. The content of e-mail messages may not contain anything that would reasonably be considered offensive or disruptive to any employee. Offensive content would include, but is not limited to, sexual comments or images, racial slurs, gender specific comments or any comments that would offend someone on the basis of their age, sex, ancestry, citizenship, color, creed, pregnancy, marital status, sexual orientation, gender identity or expression, religious or political beliefs, national origin, mental or physical disability.

C. Internet

1. While the Sheriff's Office encourages employee's use of Internet for work related purposes, its use is restricted to the following:
   a. To communicate with employees, vendors or clients regarding matters within an employee's assigned duties.
   b. To acquire information related to, or designed to facilitate the performance of regular assigned duties.
   c. To facilitate performance of any task or project in a manner approved by an employee's supervisor or department head.

2. Employees accessing the Internet are representing the Sheriff's Office and therefore all communications shall be for professional reasons. Employees are responsible for seeing that the Internet is used in an effective, ethical and lawful manner. Regarding Internet and e-mail access and usage, be advised that use of the Internet and e-mail provided by the Sheriff's Office expressly prohibits the following:
   a. Sending, receiving, printing or otherwise disseminating proprietary data, trade secrets or other confidential information of the Sheriff's Office, or any other governmental unit or agency in violation of Sheriff's Office policies, State or Federal law.
   b. Offensive or harassing statements or language including disparagement of others based on based on age, ancestry, citizenship, color, creed, marital status, mental or physical disability, national origin, pregnancy, race,

religion, sex, sexual orientation, gender identity or expression.

c. Sending, soliciting, or reviewing sexually oriented messages or images.

d. Operating a business, usurping business opportunities or soliciting money for personal gain or searching for jobs outside the Sheriff's Office or sending chain letters.

e. Gambling or engaging in any other activity in violation of local, state, or federal law.

f. The circulating of jokes, comics or non-job related computer graphics.

3. Employees may not install other on-line software services to access the Internet.

4. If an employee received material that they feel is offensive or inappropriate, they will notify their supervisor in writing immediately. Questions should be directed to the County IT Department.

D. Laptops

1. Agency issued laptops are not to be used for personal use.
2. Laptops are not to be left unsecure in an unattended vehicle.
3. When a laptop is no longer in use, the operator should "log off".

E. Passwords

1. Employees shall not divulge any password(s) to anyone to include another employee. Policy violations under an employee's password are the responsibility of the employee who holds the violating password as well as the employee using that of another.

F. Computer Hardware/Software

1. No employee shall attach, connect or otherwise use, place or cause to be placed any unauthorized hardware to agency equipment. Hardware not owned by this agency must be approved prior to any installation. Hardware that has been authorized shall be installed by a member of the County IT department.

2. Employees are prohibited from downloading software from the Internet without prior approval. This would include but is not limited to downloading games and applications, or downloading of any executable files or programs, which change the configuration of your system. All files and software will be passed through virus protection programs prior to use.

3. If an employee finds that any damage occurs as a result of downloading software or files, the incident shall be reported immediately to the County IT Department.

G. Disciplinary Action for Violation of this Policy

1. Disciplinary action for violation of this policy may include but is not limited to termination, suspension or transfer of the offending employee. In cases involving less serious violations, disciplinary action may consist of warning or reprimand as listed under the Policy and Procedure Manual. Remedial action may also include counseling, changes in work assignments, loss of Internet and e-mail privileges or other measures designed to prevent future misconduct. The measure of discipline will correspond to the gravity of the offense as weighed by its potential effect on the Sheriff's Office, on other parties, and/or fellow employees.