



HARFORD COUNTY SHERIFF'S OFFICE ADMINISTRATIVE POLICY

Acceptable Computer Usage

Jeffrey R. Gahler,
Sheriff

| | | | |
|--------------------------|------------------------------|------------------|------------------------------|
| Distribution: | All employees | Index: | ADM 1101 |
| Responsible Unit: | Computer Support Unit | Rescinds: | ADM 1101 dated 6/1/18 |
| DLI Program: | | MD Code: | |

| | | | | | |
|----------------|-----------------|------------------|-----------------|---------------------|-----------------|
| Issued: | 09/22/21 | Reviewed: | 09/21/21 | Next Review: | 09/21/24 |
|----------------|-----------------|------------------|-----------------|---------------------|-----------------|

1. Purpose

Provide members of the Harford County Sheriff's Office (HCSO) with guidelines regarding the acceptable use of HCSO software systems, computer equipment, networks, and email.

2. Policy

The HCSO will provide computer equipment and technical support to Agency members to ensure members operate equipment in a professional manner, and in conformance with HCSO policies, as well as federal, state, and local laws.

3. Definitions

AUTHORIZED SOFTWARE: HCSO owned or licensed software used in accordance with the software license or software approved for use by the Agency for a specific job function.

COMPUTER SYSTEM: refers to an arrangement of interconnected computers that share a central storage system and various peripheral devices.

DATA: information which is being processed by means of equipment operating automatically in response to instructions given for that purpose, is recorded with the intention that it should be processed by means of such equipment, or is recorded as part of a relevant filing system, computerized or not, or with the intention that it should form part of a relevant filing system.

ELECTRONIC COMMUNICATION: any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system.

NETWORK: a system containing any combination of computers, computer terminals, printers, audio or visual display devices or telephones interconnected by telecommunications equipment or cables used to transmit or receive information.

OBSCENE MATERIAL: material that the average person, applying contemporary community standards, would find, taken as a whole, appeals to the prurient interest.

PERSONALLY IDENTIFIABLE INFORMATION (PII): information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

SOFTWARE: computer programs, instructions, procedures or associated documentation that are concerned with the operation of a computer system.

STREAMING MEDIA: audio and video that are transmitted on the internet in a continuous fashion, using data packets.

USER: all employees, contractual personnel, and temporary personnel and others, including those affiliated with third parties, who access HCSO software systems and computer networks.

4. Procedures

A. General

1. HCSO owns and operates various computer systems which are provided for use by employees in support of Agency activities.
2. HCSO computer systems will generally be used for official business, however, personal use is permitted as long as:
 - a. No official activity is preempted by the personal use;
 - b. The personal use does not interfere with the employee's duties; and
 - c. The personal use conforms to this policy and other Agency policies.
3. Employees are required to use computer resources in compliance with technical and formal rules.
4. Access and privileges on HCSO computer systems are assigned and managed by the Computer Support (CS) Unit.
5. Access to HCSO email or internet services may be wholly or partially restricted without prior notice and without user consent.
6. All computer data contained on any computer, computer system, network storage device, or other data storage device is the property of the HCSO.
7. All employees have unique usernames and passwords to access HCSO systems to separate and identify the activities of different users.
8. Access to systems is based on user credentials and ensures that passwords meet minimum security requirements.
9. No computerized information will be disclosed to any individual or organization unless specifically authorized by law and specifically authorized by a supervisor.
10. CS will be responsible for approval, purchase, installation, inventory, and maintenance of HCSO computer systems.
11. Employees accessing the internet or other electronic communications through HCSO resources must be aware that these activities are monitored.

12. HCSO software, documentation, or other types of internal information will not be sold or otherwise disclosed or shared with any other party outside of the HCSO except for official business.

B. User Responsibilities

1. Users will maintain an environment in which HCSO computer resources are shared equitably among users.
2. Users agree that the HCSO role in managing these systems is only as an information carrier and they will never consider transmissions through these systems as an endorsement of said transmission by the HCSO.
3. Users will report outages or service needs based on the priority of service as outlined below.
4. Users are prohibited from using streaming internet radio or television via the Agency network for non-work-related reasons.
5. Users are prohibited from connecting/installing non-approved and/or non-Agency hardware or software on Agency networked PC's.
 - a. Only CS can authorize the connecting/installing of hardware/software on any Agency device.
6. Users must use genuine, new (not refilled), printer cartridges in Agency printers.
7. All users of Agency computers agree to "Notice of User" warning presented upon startup of Agency computers.
8. Agency members sending email messages that are addressed to "All Agency," to include retirement farewell emails, must receive prior authorization from a commander (Captain or above) and must include the authorizing commander's name at the end of the message by stating, "Approved by (the respective authorizing commander)."
9. Agency members sending email messages that are addressed to "All Law Enforcement," to include retirement farewell emails, that are not urgent officer safety messages or wanted violent offender related emails, must receive prior authorization from a commander (Captain or above) and must include the authorizing commander's name at the end of the message by stating, "Approved by (the respective authorizing commander)."

C. Software Use

1. Only HCSO owned and authorized computer software that is properly licensed is to be used on HCSO computer systems.
 2. Users will not download, install, remove, or alter any files or programs unless authorized by the CS Director.
 3. Employees will abide by all federal and state statutes and regulations pertaining to the use of computer hardware and software and the copying or installation of software in a manner that is not consistent with the vendor's license is prohibited.
-

4. CS is responsible for the storage and issuance of software licenses.

D. Prohibited Acts

1. Electronic communications systems may not be used for any purpose that could strain or compromise network resources.
2. HCSO computer systems will not be used for any illegal, unethical, harassing, unprofessional, or annoying purpose (e.g., spam, jokes, viewing or downloading obscene or pornographic material).
3. HCSO computer systems may not be used:
 - a. To access streaming media, except for official purposes;
 - b. For political purposes;
 - c. To establish a website or other internet presence that represents the HCSO; or
 - d. To obtain, reveal, or publicize sensitive, confidential, personally identifiable or proprietary information without the authorization or permission of the Sheriff.
4. No personally owned computer equipment will be connected to the HCSO network without express permission from the CS Director.
 - a. Requests to use personal computer equipment on the HCSO network will be submitted in writing to the employee's commander or director and forwarded through official channels to the CS Director.

E. Security of Email and Electronic Communications

1. Internet and email resources are provided to enhance communication and to conduct HCSO related business.
2. All messages generated on, or handled by, electronic communications systems owned or operated by the HCSO are the property of the HCSO.
3. There is no expectation of privacy when using any HCSO computer resources, including email. Employees must acknowledge and understand that:
 - a. Electronic communications can be forwarded, intercepted, printed, and stored by others and cannot be deleted by the sender; and
 - b. The content and the use of electronic communications systems will be subject to random monitoring to support operation, maintenance, auditing, security, and investigative activities.
 - c. Electronic communications may be subject to a discovery motion in a criminal case, civil case, or internal investigation.
4. Users will exercise discretion in any electronic communication sent using HCSO computers.
5. HCSO reserves the right to review any material on user accounts for purposes of ensuring compliance with this policy or any other internal policy, applicable law, rule, or regulation.

6. There is no expectation or assumption that any communication or information accessible via the HCSO network is private property.

F. Network Passwords

1. Network passwords are designed to secure the resources of the HCSO.
2. All passwords will be constructed and implemented according to this policy.
3. Criteria:
 - a. All passwords will be a combination of alpha and numeric characters.
 - b. Will be a minimum of eight (8) characters.
 - c. Will contain at least one (1) capital letter.
 - d. Will contain at least one (1) number.
 - e. Will not contain your name, address, date of birth, username, nickname, social security number, or information that can be related back to the user.
 - f. Will not be dictionary words or acronyms.
4. Passwords will not be shared with anyone other than the user.
5. Passwords will not be displayed in the workspace.
6. Passwords will be changed every forty-five (45) days or as prompted.
7. Password history will be maintained to prevent the reuse of a password.
8. Passwords must be unique to the HCSO network and will not match any other password the user has.

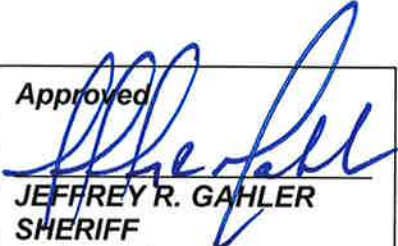
G. Priority of Service

1. CS manages calls for service on a priority system as follows:
 - a. Priority 1 - System or component down causing critical impact, no alternative available with bypass/recover within four (4) hours, respond within twenty-four (24) hours.
 - b. Priority 2 - System or component down or degraded, alternative or bypass available with response within seventy two (72) hours.
 - c. Priority 3 - Not critical, deferred maintenance acceptable, circumvention possible with no operational impact with response within one (1) week.

H. Requesting Service

1. All requests for service will be logged into the CS call tracking system.

2. Response will be based on a priority system as described above.
3. Requests will be sent as follows:
 - a. Priority 3 requests will be sent by e-mail to: ComputerSupport@harfordsheriff.org.
 - b. Priority 2 requests between the hours of 0700-1600 call 410-836-5417 or e-mail.
 - c. Priority 1 requests between the hours of 0700-1600 call 410-836-5417, after hours 443-417-6911.

Approved

JEFFREY R. GAHLER
SHERIFF
DATE 9/21/2021