



# HARFORD COUNTY SHERIFF'S OFFICE OPERATIONAL POLICY

Jeffrey R. Gahler,  
Sheriff

## Asset Security

<b>Distribution:</b>	<b>All personnel</b>	<b>Index:</b>	<b>OPS 1601</b>
<b>Responsible Unit:</b>	<b>Police Services Bureau</b>	<b>Rescinds:</b>	<b>MAN 3000</b>
		<b>MD Code:</b>	

<b>Issued:</b>	<b>12/15/21</b>	<b>Reviewed:</b>	<b>12/15/21</b>	<b>Next Review:</b>	<b>12/15/24</b>
----------------	-----------------	------------------	-----------------	---------------------	-----------------

### 1. Purpose

To provide members of the Harford County Sheriff's Office (HCSO) with guidelines relating to security of the HCSO facilities and computer assets. In addition, this policy will provide guidance for agency personnel, support personnel, and private contractors/vendors for the physical, logical, and electronic protection of Criminal Justice Information (CJI).

### 2. Policy

The HCSO will provide security for personnel and equipment to enhance the safety of employees and citizens utilizing facilities. All physical, logical, and electronic access must be properly documented, authorized, and controlled on devices that store, process, or transmit unencrypted CJI.

### 3. Definitions

**AUTHORIZED PERSONNEL:** those persons, sanctioned by the HCSO, or by a representative designated by the Sheriff of Harford County, to perform specified duties; or, those persons who have an agreement or contract with the Sheriff's Office, either on a temporary or permanent basis.

**CRIMINAL JUSTICE INFORMATION (CJI):** is the term used to refer to all of the Federal Bureau of Investigation (FBI) provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI Criminal Justice Information System (CJIS) architecture:

- a. **Biographic Data:** information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case;
- b. **Biometric Data:** data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include fingerprints, palm prints, iris scans, and facial recognition data;
- c. **Case/Incident History:** information about the history of criminal incident;

- d. Identity History Data: textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual; and
- e. Property Data: information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).

**CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS):** is a computerized system maintained by the Department of Justice (DOJ) in each state and includes the National Crime Information Center (NCIC), Uniform Crime Reporting (UCR), the Integrated Automated Fingerprint Identification System (IAFIS), NCIC 2000, and the National Incident-Based Reporting System (NIBRS). The CJIS can be accessed through any of the three law enforcement communication systems: National Law Enforcement Telecommunications System (NLETS), a more localized state criminal information system (name varies by state), and the International Law Enforcement Telecommunications System (INLETS).

**CJIS SYSTEM AGENCY INFORMATION SECURITY OFFICER (CSA ISO):** designated by the Sheriff of Harford County to serve as the security point of contact (POC) to the FBI CJIS Division ISO. The CASISO will document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA's user community, to include the local level; will document and provide assistance for implementing the security-related controls for the Interface Agency and its users; and will establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI. ISOs have been identified as the POC on security-related issues for their respective agencies and will ensure LASOs institute the CSA incident response reporting procedures at the local level.

**Escort:** an escort is defined as an authorized person who always accompanies a visitor while within a physically secure location to ensure the protection and integrity of the physically secure location and any CJI therein.

**LOCAL AGENCY SECURITY OFFICER (LASO):** designated by the Sheriff of Harford County to use the state approved hardware, software, and firmware, and who ensures no unauthorized individuals or processes have access to the same. The LASO will identify and document how the equipment is connected to the state system; ensure that personnel security screening procedures are being followed as stated in this policy; and ensure the approved and appropriate security measures are in place and working as expected.

**PHYSICALLY SECURE LOCATION:** a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the FBI CJI and associated information systems. The perimeter of the physically secure location will be prominently posted and separated from non-secure locations by physical controls. Security perimeters will be defined, controlled, and secured.

**TERMINAL AGENCY COORDINATOR (TAC):** designated by the Sheriff of Harford County to serve as the point-of-contact at the HCSO for matters relating to CJIS information access. The TAC administers CJIS systems programs within the agency and oversees the agency's compliance with Federal Bureau of Investigations (FBI) and state CJIS systems policies. The TAC will serve as the LASO and the CASISO.

**VISITORS:** a person who visits a HCSO facility on a temporary basis who is not employed by the HCSO, or a county employee who has not been granted regular access to HCSO facilities, and who has no unescorted access to a physically secure location within the HCSO where FBI CJI and associated information systems are located.

## 4. Procedures

### A. General Guidelines

1. All HCSO members, county employees who work in any agency facility on a daily basis, or who may need to access agency facilities from time to time, along with visitors to agency facilities, will be expected to conform to the guidelines set forth in this policy, or they will be denied entrance.
2. All sworn HCSO personnel not in uniform will be required to wear their law enforcement identification whenever they are inside of an agency facility.
3. All HCSO civilian personnel will be required to always wear an issued identification card while in an agency facility.

### B. Visitor Guidelines

1. Visitors to any agency facility will:
  - a. Check in before entering a physically secure location by signing the visitor's log upon entering the building, at which time they will be issued a temporary visitor's card, which they will be required to wear at all times while in the building.
  - b. Always be accompanied by a HCSO escort to include delivery or service personnel.
  - c. Show HCSO personnel a valid form of photo identification.
2. Visitors include but are not limited to:
  - a. Sales representatives;
  - b. Members of other law enforcement agencies not in uniform;
  - c. Family members
  - d. Consultants; and
  - e. Members of the public with business to conduct in the building.
3. Upon completing their business, visitors will be required to sign out at the security booth and return the visitor identification card.
4. Visitors must plan to check or sign-in multiple times if visiting multiple physically secured locations and/or building facilities that are not adjacent or bordering each other and that each have their own individual perimeter security to protect CJI.
5. Private contractors/vendors who require frequent unescorted access to restricted area(s) will be required to establish a Security Addendum between the HCSO and each private contractor personnel.

### C. Physical Access Authorization

1. Only authorized personnel will have access to physically secure non-public locations.
2. The HCSO will maintain and keep current a list of authorized personnel. Those persons wishing to have physical access into the agency's secure areas must be authorized before being granted access. The agency will implement access controls and monitoring of physically secure areas for the protection of all transmission and display mediums of CJI. All physically secure access points will be identified.
3. Authorized personnel will take necessary steps to prevent and protect the agency from physical, logical, and electronic breaches.
4. All personnel with CJI physical and logical access must meet the minimum personnel screening requirements prior to CJI access.
5. To verify identification, a state of residency and national fingerprint-based record checks will be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.
6. Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) will be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.
7. Prior to granting access to CJI, the HCSO, on whose behalf the contractor is retained, will verify identification via a state of residency and national fingerprint-based record check.

### D. Security Awareness

1. All authorized HCSO private contractor/vendor employees will receive security awareness training within six months of being granted duties that require CJI access and every two years thereafter. Security awareness training will cover areas specified in the CJIS Security Policy at a minimum, including:
  - a. Awareness of who is in their secure area before accessing confidential data;
  - b. Taking appropriate action to protect all confidential data;
  - c. Protection of all terminal monitors with viewable CJI displayed and not allowing viewing by the public or escorted visitors;
  - d. Protection from viruses, worms, Trojan horses, and other malicious code;
  - e. Web usage - allowed versus prohibited; monitoring of user activity (allowed versus prohibited is at the agency's discretion); and
  - f. Not using personally owned devices on the HCSO computers with CJI access.
2. Use of electronic media is allowed only by authorized HCSO personnel. Controls will be in place to protect electronic media and printouts containing CJI while in transport.

3. When CJI is physically moved from a secure location to a non-secure location, appropriate controls will prevent data compromise and/or unauthorized access.
4. Hard copy printouts of CJI will be released only to authorized vetted personnel who will shred or burn hard copy printouts when no longer needed.
5. When CJI access is no longer needed, HCSO security personnel will be informed. In the event of ended employment, the individual must surrender all property and access managed by the local, state, and/or federal agencies.
6. Former employees will have no unescorted access to the buildings other than that afforded the public.

#### E. Delivery Guidelines

1. If a delivery is to be made directly to a specific office at any facility, the delivery person will follow the procedure set forth for visitors.
2. A representative of the section expecting the delivery will be contacted to accompany the delivery person while they are in an agency facility.
3. If numerous packages are received, or a large item is delivered and there is a need to have an entrance door open for an extended period, arrangements will be made to have a law enforcement member stand by the door to maintain security.

#### F. Sheriff's Office Headquarters Building

1. The **Community** Services Division will have primary responsibility for security of the Sheriff's Office Headquarters, located at 45 South Main Street; however, all members of the Agency will be expected to enforce this policy and take corrective action on any violation occurring in their presence.
2. HCSO personnel will enter and exit the building through the front entrance on Main Street or use the coded entrance on Courtland Street. Personnel using the Courtland Street entrance will ensure that the controlled access door closes behind them and that it is securely fastened to prevent unauthorized access.
3. All Harford County employees, visitors, and delivery personnel will be required to enter the building using the doors located at the front of the building on Main Street. **There will be no entry to the building utilizing the double glass doors on Courtland Street. The double glass doors located on Courtland Street may be utilized as an emergency exit only.**
4. County employees whose permanent assignments are within the building will gain access to the building utilizing the card reader system on the security door in the main lobby. County employees will be required to always wear their County identification card while in the building. Any County employee reporting to work prior to 7:00am, or leaving work after 6:00pm, will be required to sign in/out on the visitor's log at the security booth. Any County employee entering the building at any time during the weekend or on holidays will be required to sign in/out on the visitor's log.
5. All deliveries will be made to the front lobby on Main Street, and the items will be left in the interior lobby for pick up by the appropriate personnel.

6. HCSO personnel or county employees must present their proper identification for access to the building. If they do not have their ID with them, they will be required to sign in/out on the visitor's log at the security booth in the lobby and obtain a visitor's identification card to be displayed while in the building.
7. County employees who are not housed in the building but may need to gain access from time to time will be required to sign the visitor's log at the security booth and wear their County identification card at all times while in the building. Upon completing their business, they will be required to sign out at the security booth. County employees and visitors will exit the building utilizing the front doors on Main Street.
8. Prior to a person leaving employment with the County, it is incumbent upon the former employee's supervisor to collect any identification cards and building keys that have been issued. The supervisor must then notify the Court Services Division that the subject is no longer employed by the County. Former county employees will have no access to the building other than that afforded the public.
9. Visitors to the building will be required to sign the visitor's log upon entering the building, at which time they will be issued a temporary visitor's card, which they must always wear while in the building. Visitors include, but are not limited to:
  - a. Sales representatives;
  - b. Members of other law enforcement agencies not in uniform;
  - c. Family members;
  - d. Consultants; and
  - e. Members of the public with business to conduct in the building.
10. Unscheduled visitors will be required to wait in the lobby until the appropriate personnel can be contacted for approval, or so they may be escorted to their indicated destinations. Upon completing their business, they will return the card to the security booth and sign out on the log.
11. The rooftop entrance may be utilized for maintenance and emergency purposes only. Access to the rooftop may be gained by obtaining permission and coordinating access with the Harford County Government Facilities and Operations Division. The rooftop entrance will be closed and always locked when not in use.
12. The boiler room entrance will be controlled by the Harford County Government Facilities and Operations Division.

#### G. Information Technology Support

1. All vetted IT support staff will protect CJI from compromise at the HCSO by performing the following:
  - a. Protect information subject to confidentiality concerns - in systems, archived, on backup media, and until destroyed. Know where CJI is stored and planned end of life. CJI is stored on laptops, mobile data terminals (MDTs), computers, servers, tape backups, CDs, DVDs, thumb drives, RISC devices and internet connections as authorized by the HCSO. For agencies who submit fingerprints using

- Live Scan terminals, only Live Scan terminals that receive CJI back to the Live Scan terminal will be assessed for physical security;
- b. Be knowledgeable of necessary HCSO technical requirements and policies taking appropriate preventative measures and corrective actions to protect CJI at rest, in transit, and at the end of life;
  - c. Properly protect the HCSO's CJIS system(s) from viruses, worms, Trojan horses, and other malicious code (real-time scanning and ensure updated definitions);
  - d. Install and update antivirus on computers, laptops, MDTs, servers, etc.;
  - e. Perform data backups and take appropriate measures to protect all stored CJI;
  - f. Ensure only authorized vetted personnel transport off-site tape backups or any other media that store CJI that is removed from physically secured locations;
  - g. Ensure any media released from the HCSO is properly sanitized/destroyed;
  - h. Identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws;
  - i. Address least privilege and separation of duties; and
  - j. Enable event logging of:
    - i. Successful and unsuccessful system log-on attempts;
    - ii. Successful and unsuccessful attempts to access, create, write, delete, or change permission on a user account, file, directory, or other system resource;
    - iii. Successful and unsuccessful attempts to change account passwords;
    - iv. Successful and unsuccessful actions by privileged accounts; and
    - v. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.
  - k. Prevent authorized users from utilizing publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
  - l. Conduct account Management in coordination with TAC.
  - m. Ensure that all user IDs belong to currently authorized users.
  - n. Keep login access current, updated, and monitored. Remove or disable terminated or transferred or associated accounts.
  - o. Authenticate verified users as uniquely identified.


- p. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs.
- q. Not use shared generic or default administrative user accounts or passwords for any device used with CJI. Passwords will:
  - i. Be a minimum length of eight characters on all systems;
  - ii. Not be a dictionary word or proper name;
  - iii. Not be the same as the User Id;
  - iv. Expire within a maximum of 90 calendar days;
  - v. Not be identical to the previous 10 passwords;
  - vi. Not be transmitted in the clear or plaintext outside the secure location; and
  - vii. Not be displayed when entered.
- r. Ensure passwords are only reset for an authorized user.
- s. Take action to protect CJI-related data from unauthorized public access.
- t. Control access, monitor, enabling and updating configurations of boundary protection firewalls.
- u. Enable and update personal firewalls on mobile devices as needed.
- v. Ensure confidential electronic data is only transmitted on secure network channels using encryption and advanced authentication when leaving a physically secure location. No confidential data should be transmitted in clear text.
- w. Not use default accounts on network equipment that passes CJI like switches, routers, firewalls.
- x. Make sure law enforcement networks with CJI will be on their own network accessible by authorized personnel who have been vetted by the HCSO. Utilize Virtual Private Network (VPN) technology to segment CJI traffic from other noncriminal justice agency traffic to include other city and/or county agencies using same wide area network.
- y. Communicate and keep the HCSO informed of all scheduled and unscheduled network and computer downtimes, all security incidents and misuse. The ultimate information technology management control belongs to HCSO.

#### H. Violations of Procedure

1. Violations of these security procedures could allow persons with criminal intentions to enter the building unnoticed and place the security of persons inside of the building in jeopardy.
2. Violations will include, but are not limited to:



- a. Propping open entrance/exit doors;
  - b. Allowing unauthorized persons access;
  - c. Allowing persons to bypass the system; and
  - d. Entering/exiting through unauthorized doors.
3. Should a violation be noticed by a law enforcement member, immediate action should be taken to correct the violation, and if known, the name of the person committing the violation should be forwarded to the Division Commander.
  4. Should a violation be noticed by a County employee, or a civilian HCSO member, corrective action should be taken if possible (example: closing a door that is not completely secured).
  5. Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and/or termination.
  6. Violation of any of the requirements in this policy by any visitor can result in similar disciplinary action against the sponsoring employee and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.
  7. In the event of a serious violation, notification should be made to a law enforcement member to correct the violation. The name of the person committing the violation should be forwarded to the Division Commander.
  8. Upon being notified of a security violation, the Division Commander will determine if the person committing the violation is a member of the HCSO, or a county employee. Written notification will then be made to the person's immediate supervisor/agency head for further disposition.

Approved  
  
JEFFREY R. GAHLER  
SHERIFF  
DATE 12.15.2021