DIRECTIVE 305.2	TOLEDO POLICE DEPARTMENT STANDARD OPERATING GUIDELINES	
EFFECTIVE March 26, 2026	CHIEF OF POLICE: Michael C. Troendle	
REVISED October 13, 2026	PART: SUPPORT SERVICES CHAPTER: TELECOMMUNICATIONS	PAGES 8
RESCINDS March 26, 2026	**PHYSICAL AND ELECTRONIC MEDIA SECURITY**	

I POLICY

It is the policy of the Toledo Police Department to ensure the protection of Criminal Justice Information (CJI) and non-public media until such time as the information is either released to the public via authorized dissemination (e.g., Freedom of Information Act requests, within a court system, or when presented in crime report data), or is purged or destroyed in accordance with applicable record retention rules.

The Media Protection Policy was developed using the FBI Criminal Justice Information Services (CJIS) Security Policy. The Toledo Police Department shall comply with the most current version of the FBI Criminal Justice Information Services (CJIS) Security Policy and any state-specific CJIS Systems Agency (CSA) requirements. All personnel, contractors, and supporting entities with access to CJI shall adhere to CJIS administrative, technical, and physical safeguards requirements.

II DEFINITIONS

PHYSICAL MEDIA - Refers to tangible materials used to store or transmit data and content. This includes printed documents and imagery that contain CJI.

ELECTRONIC MEDIA - Any means by which information is communicated or expressed, including text, audio, video, or graphics, encoded in machine-readable formats and created, viewed, distributed, or modified on electronic devices. This includes memory devices in laptops and computers (hard drives) and any removable, transportable memory media, such as magnetic tape or disk, backup media, optical disk, flash drives, external hard drives, memory cards, or live monitoring.

PHYSICALLY SECURE LOCATION - A physically secure location is a facility, an area, a room, or a group of rooms within a facility with physical and personnel security controls sufficient to protect CJI, associated information systems, and non-public media. The perimeter of the physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled, and secured. Restricted non-public areas in the Toledo Police Department shall be identified with a sign at the entrance.

VISITOR ACCESS - A visitor is defined as a person who visits any Toledo Police Department facility on a temporary basis, who is not employed by the Toledo Police Department and has no unescorted access to physically secure locations within a Toledo Police Department facility where CJI, non-public media, and associated information systems are located.

PERSONALLY OWNED DEVICES - Physical media owned by any entity other than the Toledo Police Department, or devices contracted to assist with the functions of the Toledo Police Department. This includes personal devices such as cellular phones, tablets, laptops, and other devices with similar capabilities.

CRIMINAL JUSTICE INFORMATION (CJI) - Data that is not available to the general public and used for criminal investigations, identification, and intelligence. CJI includes Criminal History Record Information (CHRI), biometric data, identity history data, property data, case/incident history, and any information derived from FBI CJIS systems.

NON-PUBLIC MEDIA – Physical or electronic media containing Toledo Police Department information that is not authorized for public release. Non-public media includes audio or video recordings, live monitoring, electronic files, and other department information for which access is restricted to authorized personnel.

AUTHORIZED PERSONNEL – Individuals with current training, credentials, and authorization from the Chief of Police to access media, a secure location, or some other restricted entity.

LOCAL AREA SECURITY OFFICER (LASO) - The designated individual responsible for ensuring the agency complies with FBI Criminal Justice Information Services (CJIS) Security Policy requirements. LASOs manage access to sensitive criminal data, ensuring only authorized personnel use agency systems, and act as the primary liaison with state security authorities.

PRINCIPLE OF LEAST PRIVILEGE - Dictates that users, systems, and applications are granted only the minimum access rights necessary to perform their specific tasks in order to minimize security risks.

ROLE-BASED ACCESS CONTROL - A framework that implements security by assigning permissions based on job roles rather than individual users, ensuring efficient, standardized, and secure access management.

VISITOR ESCORT - Authorized personnel who accompany a visitor at all times while the visitor is within a physically secure location to ensure the protection and integrity of the physically secure location and any CJI and non-public media therein.

III PROCEDURES

1. MEDIA STORAGE AND ACCESS

Controls shall be in place to protect electronic and physical media containing criminal justice information (CJI) and non-public media while at rest, stored, or actively being accessed. Only authorized personnel shall access CJI, non-public media, or secure locations. Non-public media and CJI shall only be used for law enforcement purposes. To protect CJI and non-public media, Toledo Police Department personnel shall:

1.1 Securely store electronic and physical media within a physically secure or controlled area. A secured area includes, but is not limited to, a locked drawer, cabinet, or room.

1.2 Properly protect any individually issued keys, proximity cards, computer account passwords, and other access credentials.

1.3 Restrict access to electronic and physical media to authorized individuals.

1.4 Ensure that only authorized users remove printed forms or electronic media containing CJI or non-public media.

1.5 Physically protect CJI or non-public media until the media reaches end of life. End-of-life media containing CJI or non-public media shall be destroyed or sanitized using approved equipment, techniques, and procedures in accordance with CJIS Security Policy media sanitization standards (e.g., NIST SP 800-88 or successor guidance). Sanitization methods shall be appropriate to the type of media and documented.

1.6 Personnel shall not use personally owned information systems or devices to access, process, store, or transmit CJI or non-public media unless authorized by the Chief of Police or designee, and only when all safeguards in this directive are in place. Any authorized personally owned device accessing CJI or non-public media shall:

- 1.6.1 Utilize CJIS-compliant encryption for CJI or non-public media at rest and in transit.
- 1.6.2 Store CJI or non-public media locally unless specifically authorized.
- 1.6.3 Require multi-factor authentication.
- 1.6.4 Be configured with department-approved security controls.
- 1.6.5 Be subject to remote wipe capability where feasible.
- 1.6.6 Be documented and approved by the LASO. The LASO shall maintain documentation of approved devices. Documentation shall include device identification, approval date, and applicable security controls.

1.7 Personnel shall not utilize publicly accessible computers to access, process, store, or transmit CJI or non-public media.

1.8 Store all hardcopy CJI or non-public media printouts maintained by the Toledo Police Department in a secure area accessible to only those employees whose job functions require them to handle such documents.

1.9 Safeguard all CJI and non-public media within the Toledo Police Department against possible misuse.

1.10 Take appropriate action when in possession of CJI and non-public media while not in a secure area:

- 1.10.1 CJI and non-public media shall not leave the employee's immediate control. CJI and non-public media printouts shall not be left unsupervised while physical controls are not in place.
- 1.10.2 Precautions must be taken to obscure CJI and non-public media from public view, such as by means of an opaque file folder or envelope for hard copy printouts. While using electronic devices such as laptops, a session lock or privacy screen shall be used. CJI and non-public media shall not be left in plain public view.
- 1.10.3 When CJI or non-public media is electronically transmitted or stored outside the boundary of the physically secure location, the data shall be encrypted using

FIPS 140-2 or FIPS 140-3 validated cryptographic modules, or a successor standard, in accordance with CJIS Security Policy.

(a) Storage devices include external hard drives from computers, printers, and copiers used with CJI or non-public media. Storage devices also include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.

(b) Encryption keys shall be properly managed, stored separately from encrypted data where applicable, and access shall be restricted to authorized personnel.

1.11 Lock or log off computers when not in the immediate vicinity of the work area to protect CJI and non-public media. The agency shall enforce automatic session lock after a period of inactivity consistent with CJIS requirements. Access permissions shall be granted on a need-to-know basis. Personnel without a work-related need to access the data shall not have access to the information.

1.12 Access to CJI and non-public media systems shall require unique user identification and authentication. Shared accounts are prohibited.

1.13 Establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of CJI and non-public media.

1.13.1 Systems accessing, processing, or storing CJI and non-public media shall generate and retain audit logs sufficient to reconstruct events related to CJI and non-public media access, modification, dissemination, and deletion.

1.13.2 Audit logs shall be reviewed periodically in accordance with CJIS policy and retained consistent with CJIS retention requirements.

1.14 Access permissions shall be reviewed at least annually and upon role change or termination.

1.15 Access to live monitoring or recordings from privately owned cameras may be granted to department personnel through express consent or via legal processes.

1.16 Personnel assigned to the Training Section, or personnel assisting the Training Section, may utilize non-public media if needed and relevant to the scope of the training.

2. MEDIA TRANSPORT

Controls shall be in place to protect electronic and physical media containing CJI or non-public media while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. Dissemination to another agency is authorized under the following circumstances:

2.1 The other agency is an Authorized Recipient of such information and is being assisted by the accessing agency, or

2.2 The other agency is performing personnel and appointment functions for criminal justice employment applicants. The Toledo Police Department personnel shall:

2.2.1 Protect and control electronic and physical media during transport outside of controlled areas.

2.2.2 Restrict the pickup, receipt, transfer, and delivery of such media to authorized personnel. Toledo Police Department personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

(a) When CJI or non-public media is transported electronically outside a physically secure location, encryption meeting CJIS standards shall be used.

(b) Use of privacy statements in electronic and paper documents.

(c) Limiting the collection, disclosure, sharing, and use of CJI and non-public media to law enforcement purposes only.

(d) Following the least privilege and role-based rules for allowing access. Limit access to CJI and non-public media to only those people or roles that require access.

(e) Securing hand-carried confidential electronic and paper documents. When mailed or shipped, the agency must document procedures and only release to authorized individuals. Packages containing CJI or non-public media material that are mailed shall NOT be marked "Confidential." Packages containing CJI or non-public media material shall be sent by methods that provide for complete shipment tracking, history, and signature confirmation of delivery.

2.2.3 Hand-carried electronic media shall remain under the physical control of authorized personnel at all times.

2.2.4 Chain-of-custody documentation shall be maintained for transported media containing CJI or non-public media.

2.2.5 Personnel shall not take CJI or non-public media home or take it while traveling unless authorized by the Toledo Police Department. When disposing of confidential documents, use a shredder or a document destruction service.

3. LOSS OF INFORMATION OR ACCESS; PERSONNEL ROLES AND RESPONSIBILITIES

If CJI or non-public media is improperly disclosed, lost, or reported as not received, or another security concern is discovered including facility access violations, loss of CJI or non-public media, loss of laptops, cell phones, thumb drives, CDs/DVDs and printouts containing CJI, or if CJI or non-public media has been improperly accessed, the following procedures shall be followed:

3.1 Personnel shall immediately notify their supervisor upon discovery of the incident. Report loss of issued keys, proximity cards, etc. to the on-duty supervisor, or the employee's direct supervisor if the assigned bureau/section/unit has restricted hours.

3.2 A report must be completed and submitted. The submitted report shall contain a detailed account of the incident, events leading to the incident, and steps taken in response to the incident.

3.3 Report any security incidents involving CJI to the Toledo Police Department's LASO immediately and in accordance with CJIS Security Policy incident reporting requirements.

4. LOSS OF INFORMATION OR ACCESS; SUPERVISOR RESPONSIBILITIES

Upon being informed that an individual under the supervisor's responsibility has been involved in a situation where CJI or non-public media has been improperly accessed, disclosed, lost, or reported as not received, or another security concern is discovered, including facility access violations, loss of

CJI or non-public media, loss of laptops, cell phones, thumb drives, CDs/DVDs and printouts containing CJI, the following procedures shall be followed:

4.1 Make arrangements to have authorized credentials resecured, such as a proximity card deactivated, door locks possibly re-keyed, passwords reset as necessary, or take steps to prohibit improper access to CJI or non-public media.

4.2 Ensure a satisfactory report is filed and that communication is made regarding the situation to the LASO. The LASO shall notify the Information Security Officer (ISO), CJIS Systems Agency, and/or FBI CJIS Division in accordance with CJIS Security Policy incident response timelines.

4.3 If appropriate, a Departmental Investigative Form (DIF) shall be completed.

5. VISITORS; PERSONNEL ROLES AND RESPONSIBILITIES

The responsibility for the visitor procedure rests with the employee allowing access or continued access to the facility. Personnel physically allowing the visitor into the secured area accept responsibility for that individual, and either pass the responsibility to another Toledo Police Department employee, or remain with the visitor until the visitor exits the secure area. Toledo Police Department personnel shall ensure visitors comply with the following:

5.1 All visitors must complete the visitor access log before entering a physically secure location by listing their name, their agency, purpose for the visit, date of visit, time of arrival, and name and section of the person visited. Time of departure must be noted upon departure.

5.2 The visitor will be screened by Toledo Police Department personnel for weapons. No weapons are allowed in the agency except when carried by personnel authorized by the Chief of Police or designee.

5.3 All visitors in secure areas must be accompanied by a Toledo Police Department visitor escort at all times, including delivery or service personnel. Visitor escort personnel shall ensure visitors do not access CJI systems, non-public media, or view CJI unless authorized and properly screened in accordance with CJIS policy. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

5.4 The visitor will be screened for electronic devices. Personal electronic devices may not be used in any secure area within the agency facility except when authorized by the Chief of Police or designee. Personnel shall ensure visitors are not permitted to enter a secure area with electronic devices, including cameras and mobile devices, unless approved by the Toledo Police Department Local Area Security Officer (LASO). Photographs are not allowed unless the command officer responsible for the area grants permission.

5.5 The visitor must show Toledo Police Department personnel a valid form of photo identification.

5.6 Visitors must adhere to Toledo Police Department policy for authorized unescorted access.

5.6.1 Noncriminal Justice Agency (NCJA) personnel (e.g., city information technology worker) who require frequent unescorted access to restricted areas will be required to establish a Management Control Agreement between the Toledo Police Department and the NCJA. Each NCJA employee with CJI or non-public media access will have a state and national fingerprint-based record check prior to being granted access to the restricted area.

5.6.2 Private contractors/vendors who require frequent unescorted access to restricted areas will be required to establish a Security Addendum between the Toledo Police Department and each private contractor or vendor. Private contractor or vendor personnel will have a state and national fingerprint-based record check prior to being granted access to the restricted area.

5.7 Personnel shall ensure visitors are not permitted to view screen information.

5.8 Individuals not having any legitimate business in a restricted area shall be escorted to a public area of the facility. Individuals in physically secure areas without an escort shall be stopped. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel shall be notified.

5.9 Visitors shall not be allowed to sponsor another visitor.

5.10 Escort personnel will confirm the visitor is not leaving the building with any agency-owned equipment or sensitive data prior to the visitor's departure. All Toledo Police Department personnel and supporting entities are responsible for reporting any unauthorized physical and electronic access, by either visitors or department personnel, to the Toledo Police Department through the chain of command.

5.11 All requests by groups for tours of the Toledo Police Department facility will be referred to the proper agency point of contact for scheduling. Visitor rules apply for each visitor within the group. The group leader will provide a list of names to the proper agency point of contact.

5.12 Escort personnel are responsible for properly evacuating visitors in cases of emergency.

6. AUTHORIZED PHYSICAL ACCESS

Only authorized personnel will have access to physically secure non-public locations. The Toledo Police Department will maintain a list of authorized personnel. The agency will implement access controls and monitoring of physically secure areas to protect all transmission and display media of CJI and non-public media. Authorized personnel will take necessary steps to prevent and protect the agency from physical and electronic breaches.

6.1 Department personnel shall use only the appropriate door for entry to and exit from the Toledo Police Department buildings and secure areas within those buildings, and shall use marked, alarmed emergency exits only in emergency situations.

6.2 Department personnel shall ensure the perimeter security door securely locks after entry or departure. No perimeter door shall be propped open. Unauthorized individuals shall not be permitted to enter after the perimeter door has been opened for an authorized purpose.

6.3 All personnel with CJI and non-public media access shall meet the minimum personnel screening requirements prior to being granted access.

6.3.1 To verify identification, a state of residency check and national fingerprint-based record check shall be conducted prior to assignment for all personnel who have unescorted access to CJI and non-public media and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI and non-public media. Personnel shall be re-screened in accordance with state and CJIS requirements.

6.3.2 Support personnel, private contractors/vendors, and custodial workers with access to physically secure locations or controlled areas during CJI and non-public media processing shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

6.3.3 Any subsequent arrest or disqualifying event shall be reported in accordance with CJIS policy.

6.3.4 Employees shall keep appropriate Toledo Police Department personnel informed when CJI or non-public media access is no longer needed. In the event of termination of employment, the individual must surrender all property and access credentials managed by the local agency, state, and/or federal agencies.

6.4 All authorized personnel shall complete security awareness training.

6.4.1 All authorized Toledo Police Department personnel, Noncriminal Justice Agencies (NCJA) personnel such as city IT employees, and private contractor or vendor personnel will receive security awareness training prior to initial assignment and annually as required by the CJIS Systems Agency.

6.4.2 Security awareness training will cover areas specified in the CJIS Security Policy, at a minimum.