Georgia Crime Information Center
Reference Materials
Non-Criminal Justice
Media Protection Policy Example

Standard Operating Procedure

Subject:
Media Protection Policy for information derived from the Georgia Crime Information Center (GCIC) Criminal Justice Information System (CJIS) Network

Effective Date: 00/00/0000 Revised Date: 00/00/0000

Purpose:
The purpose of this policy is to ensure the protection of Criminal Justice Information (CJI)/Criminal History Record Information (CHRI). This policy applies to all agency employees, non-paid employees, and vendors/contractors with access, to include physical and logical access, to any electronic or physical media containing CJI/CHRI while being stored, accessed, or physically moved from a physically secure location. Transporting CJI outside the agency's assigned physically secure area must be monitored and controlled.

Authorized personnel that have a current Security Awareness training certificate shall protect and control electronic and physical CJI/CHRI while at rest and in transit. The agency will take appropriate safeguards for protecting CJI/CHRI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate disclosure and/or use must be reported to the agency head or designee and the Local Agency Security Officer (LASO). All employees, non-paid employees, and vendors/contractors are required to follow the policies, rules and procedures set forth by GCIC, GCIC Council Rules, CJIS Security Policy, and the laws of the State of Georgia.

Controls shall be in place to protect electronic and physical media containing CJI/CHRI while at rest, stored, or actively being accessed. "Electronic media" includes memory devices in laptops and desktop computers (hard drives), printers, and scanners and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CJI/CHRI.

Media Storage and Access:
To protect CJI/CHRI, personnel shall:
1. Securely store within a physically secure location or controlled area. A secured area includes a locked drawer, cabinet, or room.
2. Restrict access to authorized individuals.
3. Restrict the pickup, receipt, transfer, and delivery to authorized individuals. 4. Ensure that only authorized users remove printed form or digital media from the CJI/CHRI. 5. Physically protect until media end of life.
6. Not use personally owned information system to access, process, store, or transmit CJI/CHRI.

Georgia Crime Information Center
Reference Materials
Non-Criminal Justice
Media Protection Policy Example

7. Not utilize publicly accessible computers to access, process, store, or transmit CJI/CHRI. Publicly accessible computers include but are not limited to hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.
8. Store all hard copy printouts maintained in a secure area accessible to only personnel whose job function require them to handle such documents.
9. Safeguard against possible misuse.
10. Take appropriate action when in possession, while not in a secure area a. Must not leave the employee's immediate control. CJI printouts cannot be left unsupervised while physical controls are not in place.
    b. Precautions must be taken to obscure CJI from public view, such as by means of an opaque file folder or envelope for hard copy printouts. For electronic devices like laptops, use session lock use and /or privacy screens. CJI shall not be left in plain public view. When CJI is electronically transmitted outside the boundary of the physically secure location, the data shall be immediately protected using encryption.
    i. When CJI is at rest (i.e., stored electronically) outside the boundary of the physically secure location, the data shall be protected using encryption. Storage devices include external hard drives from computers, printers and copiers used with CJI. In addition, storage devices include thumb drives, flash drives, back-up tapes, mobile devices, laptops, etc.
    ii. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.
11. Lock or log off computer when not in immediate vicinity of work area. 12. Establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of CJI.

<u>Digital and Physical Media Transport</u>:

The agency shall protect and control digital and physical media during transport (physically moved from one location to another) outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. Physical media shall be protected at the same level as the information would be protected in electronic form. Encryption of digital media is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data.

Georgia Crime Information Center
Reference Materials
Non-Criminal Justice
Media Protection Policy Example

Electronic Media Sanitization and Disposal:

The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. Physical media shall be securely disposed of when no longer required, using formal procedures.

Physical Media Disposal:

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

Incident Response:

Personnel with access to CJI/CHRI are required to be familiar with their agency disciplinary policy. Agencies must report all GCIC violations in writing to the GCIC Division Director.

Penalties:

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, as outlined in the Disciplinary Policy.