DALTON FIRE DEPARTMENT

Standard Operating Procedure

S.O.P.: GP-14
Effective: 07/25/2017
Revised: 07/25/2017
Reviewed: 07/27/2021

_____ _____
Fire Chief Signature **DATE**

Title: Media protection for information derived from the Georgia Crime Information Center (GCIC) Criminal Justice Information System (CJIS) Network

Scope: All personnel 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 secure location.

Policy:

The purpose of this policy is to ensure the protection of Georgia Crime Information Center (GCIC) Criminal History Record Information (CHRI). This policy applies to all employees 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 secure location. Transporting CJI outside the agency's assigned physically secure area must be monitored and controlled.

Authorized personnel shall protect and control electronic and physical CJI/CHRI while at rest and in transit. Dalton Fire Department 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 must be reported to the Fire Chief or designee. All employees are required to follow the policies, rules and procedures set forth by GCIC, GCIC Council Rules, CJIS Security Policy, and 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 computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, backup medium, optical disk, flash drive, 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:
- Securely store within a physical secure location or controlled area.
- Restrict access to authorized individuals.
- Restrict the pickup, receipt, transfer and delivery to authorized individuals.
- Ensure that only authorized users remove printed from or digital media from the CJI/CHRI.
- Physically protect until media end of life.

- Not use personally owned information system to access, process, store, or transmit CJI/CHRI.
- Not utilize publicly accessible computers to access, process, store, or transmit CJI/CHRI.
- Publicly accessible computers include but not limited to: hotel, business center, convention center, public library, public kiosk, etc.
- Store all hard copy printouts maintained in a secure area accessible to only personnel whose job function require them to handle such documents.
- Safeguard against possible misuse.
- While being used, must not leave employee's immediate control. Documents shall not be unsupervised while physical controls are not in place.
- Precautions shall be made to obscure from public view.
- CJI transmitted or stored electronically shall be protected using encryption.
- When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.
- Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality.

Electronic Media Sanitation and Disposal:

Dalton Fire Department 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.). Dalton Fire Department shall maintain written documentation of these steps taken to sanitize or destroy electronic media. Dalton Fire Department shall ensure the sanitation or destruction is witnessed and carried out by authorized personnel. Physical media shall be securely disposed of using the same procedures when no longer required.

Penalties:

Violation of any of the requirements in this policy by any personnel will result in suitable disciplinary action, as outlined in the Disciplinary Policy. Any violations must be reported in writing to the GCIC deputy director.