

IDAHO STATE POLICE PROCEDURE

11.05 DISPOSAL OF CRIMINAL JUSTICE INFORMATION SYSTEM MEDIA

I. General

Proper disposal of media at the Idaho State Police (ISP) is a critical process that ensures protection of sensitive and classified FBI CJIS information, including employee, and ISP information. Employees of ISP, as well as contractors, temporary staff, and any other workers who have access to sensitive and classified data and media at ISP are responsible for properly disposing of the media when the information is no longer required for authorized purposes. The disposal or destruction of information applies to originals as well as copies and archived records, including system logs that may contain personally identifiable information. Physical media will be destroyed by crosscut shredding or incineration. If a professional service is used to shred or incinerate media, it must be supervised by an authorized ISP employee unless the outside entity personnel have been fingerprint background checked and approved. Employees who violate this procedure may be subject to disciplinary action up to and including, termination of employment.

II. Definitions

- A. "Authorized Personnel" means an individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to Criminal Justice Information as well as undergone at least level one security awareness training.
- B. "Criminal Justice Information (CJI)" means all of the FBI CJIS 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.
- C. "Physical Media" refers to media in printed form. This definition includes, but is not limited to, printed documents, printed imagery, printed facsimile.
- D. "Digital media" includes but is not limited to flash drives, external or removable hard disc drives (e.g., solid state, magnetic), compact discs (CDs), digital versatile discs (DVDs), diskettes, and magnetic tapes.
- E. "Non-digital" media includes paper and microfilm.

III. Disposal of Media

- A. Sanitize or destroy digital and non-digital media prior to disposal, release out of agency control, or release for reuse using overwrite technology at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media will be destroyed (cut up, shredded, etc.). Physical media will be securely disposed of when no longer needed for

IDAHO STATE POLICE PROCEDURE

investigative or security purposes. Non-digital media will be destroyed by crosscut shredding or incineration.

- B. CDs and DVDs are placed in properly marked shredding bins marked “Confidential CD/DVDs Only”, to be shredded and disposed of by a professional shredding company and supervised by an authorized ISP personnel.
- C. Paper copies are placed in properly marked shredding bins marked “Confidential Paper Only”, to be shred and disposed of by a professional shredding company and supervised by an authorized ISP personnel.
- D. Diskettes and tape cartridges are taken apart or shredded using the proper shredder. The shredded media material is then incinerated.
- E. IT systems having processed, stored, or transmitted information that is classified and/or sensitive is sanitized, with all information cleared or wiped using National Security Association approved measures.
- F. All copies must be destroyed. For example, if media was entered into evidence and a duplicate was placed elsewhere (e.g., in the case file or the investigating officer’s personal file), all copies must be destroyed or documented where it is retained.