IDAHO STATE POLICE PROCEDURE

11.06 CRIMINAL JUSTICE INFORMATION MEDIA PROTECTION

I. GENERAL

ISP recognizes that Criminal Justice Information (CJI) must be protected until such time as it is released to the public via authorized dissemination, purged, or destroyed according to applicable record retention rules, or safely stored in a physically secure location.

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 CJI, as well as undergone at least level one security awareness training.

B. “Criminal Justice Information” 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. “CJISSECPOL” is the FBI Criminal Justice Information Systems Security Policy. The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

D. “Electronic media” means 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 drives, external hard drives, or digital memory card.

E. “Physical media” means printed documents and imagery that contain CJI.

F. “Physically Secure Location” means a facility, a criminal justice conveyance, an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

G. "CSO” is the CJIS Systems Officer, at Idaho State Police, this is the Bureau of Criminal Identification Chief.

H. "ILETS ISO" Is the Idaho Public Safety and Security Information Security Officer, at the Idaho State Police, this is the Bureau of Criminal Identification Information Security Engineer.

III. MEDIA PROTECTION

Authorized ISP personnel protect and control electronic physical CJI while at rest and in transit. ISP personnel take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported.

A. Electronic and physical media is stored within a physically secure or controlled area (this may include a locked drawer, cabinet, or room).

B. Access to electronic and physical media is restricted to authorized individuals with a criminal justice job responsibility related to that data.

C. Only authorized users remove physical or digital media from the physically secure location with a criminal justice job responsibility related to that physical or digital media.

D. CJI is physically protected until media end of life. End of life CJI is destroyed or sanitized per 11.05 Disposal of Criminal Justice Information.

E. The use of personally owned information systems or publicly accessible computers is not allowed to access, process, store, or transmit CJI or information derived from ILETS.

F. Hardcopy CJI printouts maintained by ISP are stored in a physically secure location accessible to only those employees whose job functions require them to handle such documents.

G. Personally owned electronic media is not to be used for storage or transport of CJI.

H. While not in a secure area, appropriate action is taken when in possession of CJI:
1. the employee maintains control of CJI at all times; printouts are not left unsupervised while physical controls are not in place;
2. opaque file folders or envelopes are used to protect printouts of CJI from public view;
3. session lock use and/or privacy screens are used to protect view of electronic devices such as laptops;
4. CJI at rest (i.e. stored electronically) outside the boundary of the physically secure location is protected using CJISSECPOL compliant encryption. Storage devices include hard drives from computers, printers and copiers

used with CJI, thumb drives, flash drives, backup tapes, mobile devices, laptops, etc.;
5. the cryptographic module used for encryption is compliant with the latest version of the CJISSECPOL.
6. personnel lock or log off a computer when not in the immediate vicinity of the work area; and
7. appropriate administrative, technical and physical safeguards ensuring security and confidentiality of CJI are followed per 11.04 Physical Protection of Criminal Justice Information.

IV. MEDIA TRANSPORT

A. Privacy statements in electronic and paper documents are used.

B. Collection, disclosure, sharing, and use of CJI is limited.

C. Hand carried confidential electronic and paper documents are secured by:
1. storing CJI in a locked briefcase or lockbox;
2. restricting viewing or accessing CJI in a physically secure location to authorized personnel, unless technical requirements have been met; and
3. packaging hard copy printouts or CJI documents so they are visually inaccessible.

D. CJI transmitted electronically outside the boundary of the physically secure location is immediately protected using CJISSECPOL compliant encryption.

E. CJI may only be sent via email if following a program unit specific written procedure that has been approved by the CSO or ILETS ISO.

F. ISP releases mailed or shipped CJI only to authorized individuals.
1. packages **are not** marked CONFIDENTIAL; and
2. packages are sent by method(s) that provide complete shipment tracking and history, and signature confirmation of delivery.