Media Protection

812.1 PURPOSE AND SCOPE

The intent of the Media Protection Policy is to ensure the protection of Criminal Justice Information (CJI) until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

The scope of this policy applies to any electronic or physical media containing FBI Criminal Justice Information (CJI) or CLETS information while being stored, accessed or physically moved from a secure location from the Irvine Police Department. This policy applies to any authorized person who accesses, stores, and/or transports electronic or physical media. Transporting CJI outside the agency's assigned physically secure area must be monitored and controlled.

Authorized Irvine Police Department personnel shall protect and control electronic and physical CJI while at rest and in transit. The Irvine Police Department will take appropriate safeguards for protecting CJI to limit potential mishandling or loss while being stored, accessed, or transported. Any inadvertent or inappropriate CJI disclosure and/or use will be reported to the Irvine Police Department Agency CLETS Coordinator (ACC), or our Local Agency Security Officer (LASO). Procedures shall be defined for securely handling, transporting and storing media.

812.2 STORAGE AND ACCESS

Controls shall be in place to protect electronic and physical media containing CJI 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 drives, external hard drives, or digital memory card. "Physical media" includes printed documents and imagery that contain CJI.

To protect CJI, Irvine Police Department personnel shall:

1. Securely store electronic and physical media within a physically secure or controlled area. A secured area includes a locked drawer, cabinet, or room.
2. Restrict access to electronic and physical media to authorized individuals.
3. Ensure that only authorized users remove printed form or digital media from the CJI.
4. Physically protect CJI until media end of life. End of life CJI is destroyed or sanitized using approved equipment, techniques and procedures.
5. Store all hardcopy CJI printouts maintained by the Irvine Police Department in a secure area accessible to only those employees whose job function require them to handle such documents.
6. Take appropriate action when in possession of CJI while not in a secure area:
    (a) CJI 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.

1. 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.
2. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

7. Lock or log off computer when not in immediate vicinity of work area to protect CJI. Not all personnel have same CJI access permissions and need to keep CJI protected on a need-to-know basis.
8. Establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of CJI.

812.3 TRANSPORTING

Controls shall be in place to protect electronic and physical media containing CJI while in transport (physically moved from one location to another) to prevent inadvertent or inappropriate disclosure and use. “Electronic media” means electronic storage media including 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.

Dissemination to another agency is authorized if:

1. The other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or
2. The other agency is performing personnel and appointment functions for criminal justice employment applicants.

Irvine Police Department personnel shall:

1. Protect and control electronic and physical media during transport outside of controlled areas.
2. Restrict the pickup, receipt, transfer and delivery of such media to authorized personnel.

Irvine Police Department personnel will control, protect, and secure electronic and physical media during transport from public disclosure by:

1. Limiting the collection, disclosure, sharing and use of CJI.
2. Limit access to CJI to only those people or roles that require access.
3. Securing hand carried confidential electronic and paper documents by:

(a) Only viewing or accessing the CJI electronically or document printouts in a physically secure location by authorized personnel.

(b) For hard copy printouts or CJI documents:

1. Package hard copy printouts in such a way as to not have any CJI information viewable.

2. That are mailed or shipped, agency must document procedures and only release to authorized individuals. DO NOT MARK THE PACKAGE TO BE MAILED CONFIDENTIAL. Packages containing CJI material are to be sent by method(s) that provide for complete shipment tracking and history, and signature confirmation of delivery.

812.4 ELECTRONIC MEDIA SANITIZATION AND DISPOSAL

The agency shall sanitize electronic media prior to disposal or release for reuse by unauthorized individuals. All data is sanitized using software, tools, or techniques to overwrite each disk sector of the machine with zero-filled blocks. Electronic drives are degaussed or overwritten at least three times with disk cleaning software. Inoperable electronic media shall be destroyed via shredding under supervision. The Irvine Police Department 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.

812.5 BREACH NOTIFICATION AND INCIDENT REPORTING

The Irvine Police Department shall promptly report incident information to appropriate authorities as described below. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

812.6 ROLES AND RESPONSIBILITIES

In the event that CJI is improperly disclosed, lost, or reported as not received, the following procedures shall be followed:

1. Irvine Police Department personnel shall notify their supervisor and an incident report must be completed and submitted within 24 hours of discovery of the incident. The submitted report is to contain a detailed account of the incident, events leading to the incident, and steps taken in response to the incident.
2. The supervisor will communicate the situation to the ACC to notify of the loss or disclosure of CJI records.
3. The ACC will ensure the CJIS System Agency Information Security Officer is promptly informed of security incidents.

812.7 PENALTIES

Violation of any of the requirements in this policy by any authorized personnel may result in disciplinary action up to and including termination. Violations may also result in criminal prosecution and/or civil liability.