IDAHO STATE POLICE PROCEDURE

11.04 PHYSICAL PROTECTION OF CRIMINAL JUSTICE INFORMATION

I. GENERAL

Physical protection of Criminal Justice Information (CJI) is necessary to protect the full lifecycle of CJI from insider and outsider threats. This includes ISP personnel, support personnel, and private contractor/vendors with access to CJI, whether logically or physically.

II. DEFINITIONS

A. "Authorized personnel" means an individual (or group) who has been appropriately vetted through a national fingerprint-based record check and has been granted access to CJI, 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. "Escort" means authorized personnel who accompany a visitor at all times within a physically secure location to ensure the protection and integrity of the physically secure location and any CJI therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

D. "Physically secure location" means a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect the CJI and associated information systems. The perimeter of the physically secure location is prominently posted and separated from non-secure locations by physical controls. Security perimeters are defined, controlled, and secured. Restricted non-public areas in ISP are identified with a sign at the entrance.

E. "Visitor" means a person who visits an ISP facility on a temporary basis who is not employed by ISP and has no unescorted access to the physically secure location within ISP where FBI CJI and ILETS information systems are located.

F. "Tailgating" or "Piggybacking" is either an intentional or accidental security violation where someone enters a secure area without proving authorization to enter. Examples include holding a door open for someone behind you with their arms full.

G. "CJI Clean Desk/Screen process" means any CJI must be hidden from view on your screen or desk if a visitor may see it.

III. VISITORS

A. ISP personnel allowing access to a visitor in a physically secure location will:
   1. Maintain a visitor log in the appropriate area utilizing the approved ISP Visitor log;
   2. Keep the visitor log for one year or longer if required by compliance policies;
   3. Review visitor log quarterly;
   4. Report anomalies in visitor logs to district captain or program manager;
   5. Request valid identification;
   6. Instruct the visitor to display the badge on visitor's outer clothing and return the badge prior to leaving. Visitor should be instructed to check or sign-in multiple times if visiting multiple physically secure locations and/or building facilities that are not adjacent or bordering each other; and
   7. Escort or ensure an escort at all times, inclusive of delivery or service personnel.

B. Visitors are not allowed to view screen information or shoulder surf.

C. Individuals who have no legitimate business in a restricted area are courteously escorted to a public area of the facility.
   1. Strangers in physically secure areas without an escort should be questioned.
   2. If resistance or behavior of a threatening or suspicious nature is encountered, sworn personnel should be notified or the employee should call 911.

D. Visitors are not permitted in secure areas with electronic devices including cameras and mobile devices unless approved by ISP. Photographs are not allowed without permission of ISP District Captains/Program Managers.

E. Requests by groups for tours of the ISP facilities are referred to Human Resources for the Meridian Campus, or the District Captain in the district facilities.
   1. Groups are handled by a single log in, signed by a designated group leader or representative.
   2. The group leader provides a list of names to ISP for instances of emergency evacuation and accountability of each visitor while on agency premises.
   3. Remaining visitor rules apply for each visitor within the group.

IV. AUTHORIZED PHYSICAL ACCESS

A. All ISP employees and vendors/private contractors who require frequent access needing (1) unescorted physical and/or logical access to a physically secure ISP location, (2) terminal access to ILETS, or (3) who provide IT related service/support will, to the level of requirement:
   1. Verify their identity by undergoing a state of residency and national fingerprint-based record check before being granted physical and/or logical access per 03.09 Pre-Employment Background Investigations.

2. Complete the appropriate level of security awareness training before being granted access to areas with CJI.
3. Take security awareness training as they test/certify to meet ILETS requirements if they have terminal access to ILETS. All other personnel will receive security awareness training via CJISonline.com.
4. Be aware of who is in their area before accessing confidential data.
   a. take appropriate action to protect all confidential data; and
   b. A CJI clean desk/clean process must be followed if CJI can be seen by a visitor. Visitor escort should announce the visitor before CJI can be seen.
5. Properly protect and do not share any individually issued keys, proximity cards, computer account passphrases, etc.
   a. report loss of issued keys, proximity cards, compromised combinations etc. to supervisor;
   b. if the loss occurs after normal business hours, or on weekends or holidays, personnel call the ISP Control Center to have such authorized credentials deactivated and/or door locks possibly rekeyed;
   c. change keys or combinations when confirmed lost or compromised;
   d. combinations changed when persons with knowledge of combination are no longer employed in a position requiring their knowledge of combination.
   e. inventory agency-issued physical access devices (keys, combinations, access cards) annually; and
   f. safeguard and do not share passphrases, Personal Identification Numbers (PIN), Security Tokens (i.e., Smartcard), Yubikeys, any devices used for multifactor authentication, and all other facility and computer systems security access procedures.
6. Properly protect from viruses, worms, Trojan horses, and other malicious code.
7. Not use personally owned devices on the ISP computers with CJI access.
8. Follow the procedure to protect electronic media and printouts containing CJI while in transport.
9. Report any physical security incidents to the ISP Local Agency Security Officer (LASO) to include facility access violations, loss of CJI, and loss of laptops, mobile devices, thumb drives, CDs/DVDs and printouts containing CJI.
10. Properly release hard copy printouts of CJI only to authorized vetted and authorized personnel in a secure envelope and shred or burn hard copy printouts when no longer needed. Information is shared on a “need to know” basis.
11. Ensure ISP data centers with CJI are physically and logically secure.
12. Keep appropriate ISP security personnel informed when CJI access is no longer needed. In the event of ended employment, the individual will surrender all property and access managed by the local agency, state and/or federal agencies.
13. Know which door to use for proper entry/exit of ISP and only use marked, alarmed fire exits in emergency situations.
14. Ensure the perimeter security door securely locks after entry/departure. Perimeter doors are not propped or blocked open. Doors to secure areas that fail to auto close/lock should be reported to the district captain or program manager overseeing that area.

15. "Tailgating" or "piggybacking" should not be allowed into CJIS secure areas. Signage warning against tailgating should be posted at all external ingress points.

V. INFORMATION TECHNOLOGY SUPPORT

A. Information subject to confidentiality concerns in systems, archived, and on backup media is protected by Information Technology (IT) support staff until destroyed.

B. IT support staff is aware that CJI is stored on laptops, mobile data terminals (MDTs), computers, servers, tape backups, CDs, DVDs, thumb drives, RISC devices, and internet connections as authorized by ISP.

C. IT support staff ensures maximum uptime of CJI and expedited backup restores by using power and data backup such as generators, and backup universal power supplies on ILETS terminals, servers, switches, etc.

D. IT support staff properly protect the ISP's ILETS system(s) from viruses, worms, Trojan horses, and other malicious code by installing and updating antivirus on computers, laptops, MDTs, servers, etc. and scanning any outside non-agency owned CDs, DVDs, thumb drives, etc.

E. IT support staff perform data backups while taking appropriate measures to protect stored CJI. Only authorized personnel transport off-site backups or any media storing CJI from physically secured locations.

F. IT support staff properly sanitize/destroy media released from ISP per 11.05 Disposal of Criminal Justice Information Media.

G. IT support staff ensures timely application of system patches by identifying applications, services, and information systems containing software of components affected by recently announced software flaws and resulting potential vulnerabilities.

H. IT support staff sets access control measures, which:
   1. address least privilege and separation of duties;
   2. enable event logging of:
      a. successful and unsuccessful system log-on attempts;
      b. successful and unsuccessful attempts to access, create, write, delete, or change permission on a user account, file, directory, or other system resource;
      c. successful and unsuccessful attempts to change account passwords;
      d. successful and unsuccessful actions by privileged accounts; and
      e. successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.

3. prevent authorized users from utilizing publicly accessible computers to access, process, store, or transmit CJI. Publicly accessible computers include but are not limited to computers at: hotel business centers, convention centers, public libraries, and public kiosks.

I. IT support staff is responsible for Account Management in coordination with TACs:
   1. all user IDs are verified as belonging to currently authorized users;
   2. login accesses are current, updated, and monitored. Remove or disable terminated, transferred, or associated accounts;
   3. verified users are uniquely identified;
   4. multiple concurrent active sessions for one user identification for those applications accessing CJI are prevented, unless the agency grants authority based on operational business needs;
   5. shared generic or default administrative user accounts or passwords for any device used with CJI are prohibited; and
   6. IT support staff ensure that passwords are:
      a. a minimum length of eight characters on all systems;
      b. not dictionary words or proper names;
      c. not the same as User ID;
      d. set to expire within a maximum of 90 calendar days;
      e. not identical to the previous ten passwords;
      f. not transmitted in the clear or plaintext outside the secure location;
      g. not displayed when entered; and
      h. only reset for authorized user.

J. IT support staff protect network infrastructure by preventing unauthorized public access of CJI-related data:
   1. access, monitor, enabling and updating configurations of boundary protection firewalls are controlled.
   2. personal firewalls on mobile devices are enabled and updated.
   3. confidential electronic data is only transmitted on secure network channels using encryption and advanced authentication when leaving a physically secure location. No confidential data is transmitted in clear text.
   4. media that is removed from a physically secured location is encrypted in transit by a person or network.
   5. default accounts on network equipment that passes CJI like switches, routers, and firewalls are not used.
   6. Virtual Local Area Network (VLAN) technology to segment CJI traffic from other noncriminal justice agency traffic to include other city/county agencies using same wide area network is used.

K. ISP personnel are informed of all scheduled and unscheduled network and computer downtimes, all security incidents, and misuse.