IDAHO STATE POLICE PROCEDURE

02.11 USE OF INFORMATION TECHNOLOGY

A. General

The Idaho State Police (ISP) provides information technology (IT) to enhance the capabilities and productivity of its employees. IT use requires a balance between the individual or public's ability to benefit fully from IT and the department's need for a secure and reasonably allocated IT environment. All systems and information must be used in accordance with policies established by the Idaho Technology Authority (ITA).

There is no expectation of privacy for information created or stored in taxpayer-provided resources. ISP-issued electronic devices are subject to audit or search by the agency to ensure they are being properly used for work purposes.

All employees must be conscientious about the amount and type of information stored on ISP network drives. Photos, video, audio or other files or documents produced or stored solely for personal enjoyment are not appropriate material created or stored on the network drives and may be deleted without notice by IT staff.

B. Definitions

"Agency systems" or "systems" means all agency electronic information devices, interconnections, and related technical information including computers and any connected or related devices. Systems also include other systems accessed by or through those devices, such as the Internet, electronic mail (e-mail), and phone services.

"Mobile devices" means a handheld or tablet-sized computer that is easily carried, and which can be used to access business information. These include, but are not limited to, Smartphones, notebook/netbook computers, Tablet PCs, iPads and other similar devices.

"Wipe" means to run a device through a process of erasing stored information.

C. Standardized Software Packages

1. The ITA establishes standard software packages for use by Idaho state governmental agencies.

2. Criminal Justice Information Systems (CJIS) identifies and implements these packages for the ISP.

3. IT must approve all software for specialized use.

4. Programs that are written by non-IT personnel must be screened by IT programmers.

5. Procedures for using standardized software must be consistent with training provided, coordinated, or approved by IT with the following restrictions:
   a. system access is limited through use of unique usernames and passwords or passphrases;
   b. access to the system is disabled if any account has 12 failed logon attempts;
   c. access must be manually reset by IT personnel;
   d. use of the e-mail preview pane and auto preview is prohibited because these features make ISP's IT systems vulnerable to computer viruses;
   e. 25 megabytes (MB) is the maximum size limit for e-mail transmissions both inbound and outbound;
   f. 100 MB is the maximum size limit established for each mailbox including incoming and outgoing e-mail/voicemail messages, Quick Record material, Calendar, Contacts, Tasks, Notes, Journal entries, and any deleted items;
      (1) an automatic message is sent to the mailbox user when the mailbox size approaches this limit;
      (2) when the limit is exceeded, another message is sent informing the user that the mailbox is closed, and no further e-mail can be sent or received;
      (3) the size of each item rather than just the number of items determines the size of items in a mailbox compared to the limit. Attachments, voice messages, and graphics tend to be large files;
      (4) personal folders (M: drive) may be established on an individual's personal computer to allow e-mail archiving.

D. Restricted Access Software Packages

1. Some software packages are restricted and access is granted only as necessary in the performance of official duties.

2. Access and software are provided as a system enhancement with the following additional authorizations:
   a. Public Safety and Security Information System (ILETS) – authorization in accordance with established ILETS/NCIC procedures;
   b. case management and Evidence Tracking System (ETS) – authorization by the appropriate program Major/Manager;
   c. remote dial-in access – authorization by the appropriate program Major/Manager.

E. Personal Computer File Maintenance

1. The local drive, C: and/or D: on the personal computer is used to store software programs.

2. Data and informational files are stored on appropriate network drives as noted in F. Use of Network Drives, below.

3. Storage in this manner eliminates the need to perform backups or other utilities unless instructed by IT.

F. Use of Network Drives

1. Each computer system user has access to shared network drives for storage and information sharing as required to perform official duties.

2. Network drive storage space is a limited, shared resource:
   a. users store informational and data files on network drives;
   b. files on network drives are backed up nightly by IT and can be restored in the event of loss or damage;
   c. file retention is in accordance with ISP procedure 02.07 Records Management;
   d. users will consider CD-ROM and/or DVD copies for long-term file storage greater than 2 years;
   e. all non-work related files will be deleted without notification; and
   f. no evidence can be stored on the global drive.

3. Drive configuration:
   a. M: or P: is the drive with folders assigned to each user for individual use:
      (1) folders on this drive are not accessible by other users;
      (2) this is where a user generally stores data and informational files.
   b. N:, or global, is the drive accessible by every system user. Information available to everyone is stored on the drive:
      (1) folders for each section of the agency have been established;
      (2) additional folders on the root directory of this drive may only be created with prior permission of IT;
      (3) files being transferred to another user must be deleted as soon as the transfer is complete.
   c. H:, I:, or J: are established as program or work unit common drives:
      (1) these drives are for storing information used within work groups;
      (2) access is limited to the membership of that group as identified by work group managers.
   d. Other network drives may be established by IT as required to meet agency need.

G. Mobile Devices

1. The ability of mobile devices to store and transmit information through both wired and wireless networks poses potential risks to ISP security. To be utilized within the ISP network, mobile devices must:
   a. be agency owned and provided by the agency;
   b. have make and model approved by IT;
   c. support password protection;
   d. have screen locking and screen timeout functions;

e. have the ability to encrypt files in onboard storage or removable storage;
f. be capable of being wiped remotely and disabled in the event the device is lost or stolen (if the device is wireless); and
g. have the ability to be protected from and scanned for viruses.

2. Users of mobile devices will:
   a. Use password protection;
   b. Report missing or lost devices immediately to the System Administrator and the cell phone account manager;
      (1) The System Administrator or the cell phone account manager does a security wipe on the device; and
      (2) The cell phone account manager deactivates the device and makes arrangements for a replacement device.

H. Networked Communications Systems (VoIP Telephone Systems)

1. Some ISP offices receive telephone services through the networked communications system.

2. User information and instruction on using networked communications devices is in the ISP Intranet Library Manuals and Operation Guides section.

3. Voice messages and Quick Record material in the networked communications system reside on the Exchange server, count against the mailbox maximum size limits, and are managed in the same manner as e-mail messages in section C., above.

4. Certain features of the networked communication system require supervisory or Major/Manager approval for initial setup and change:
   a. assignment of the quick record feature requires additional user licensing, may incur expense, and must be approved by the program Major/Manager prior to setup or addition;
   b. initial setup of line appearances or changes to line appearances require supervisory approval.

5. The quick record function creates a record of the telephone call potentially subject to the state Records Management Guide and ISP procedures, in addition to policies established by the ITA:
   a. recordings retained as evidence are handled as non-drug evidence according to ISP procedure 06.09 Evidence and Property;
   b. recordings not retained as evidence are handled according to their classification in the state Records Management Guide or ISP records retention schedule;
   c. recordings retained as records, whether evidentiary or non-evidentiary, must be copied to a CD or other storage device for retention within 60 days of receipt, and the original recording deleted from the networked system;

d. recordings residing on the Exchange server count against the mailbox maximum size limits and are managed in the same manner as e-mail messages in section C., above.

I. Forms for Changes to IT Services or Configurations

1. Human Resources initiates a Security form for new hires and forwards it to the supervisor of the employee to complete. Supervisors initiate and submit this form for the deletion and modification of agency employee access to Meridian and Jerome building security systems, computer, and telephone systems.

2. Submit a Non-Employee security form request for the addition, deletion and modification of non-agency personnel access to the building security system.

J. Processing Requests

1. Fill in forms as completely as possible to avoid delays in researching information.

2. Include any information relating to special considerations, deadlines or required coordination.

3. Route forms through the requesting program chain-of-command to the appropriate Major/Manager:

4. The EH 03 04-01 ISP Security Form is also routed through the Human Resource Office in accordance with ISP procedure 03.04 Hiring.

5. Route forms to the IT Manager.

6. Allow five business days for IT processing.

7. Either a copy of the form returned to the requesting office or direct contact from IT personnel is notification of completed work.

8. The requesting party confirms that the work meets requirements as requested.

9. Requests for special handling or processing should be directed to the IT Manager or the Police Services Major/Manager.

K. Equipment, Software and Contract Service Purchases

1. All requests for IT equipment, software, or contract service purchases must be coordinated through IT.

2. Requests are processed in accordance with ISP procedure 04.07 Purchasing.

3. ISP standardizes computer equipment and software based upon identified needs and support requirements.

4. A detailed specification listing is available by contacting IT.

5. A memo requesting non-standard equipment/software with detailed system/business requirements and any documentation supporting the request must be sent to the IT Manager.

L. Reissue of Identification Cards

1. Lost, stolen or damaged identification cards must be reported immediately to the affected employee's supervisor.

2. The supervisor requests a replacement card by e-mailing the Replacement Card mailbox.

3. Old cards are returned to IT for destruction.