INDIANA STATE POLICE	***STANDARD OPERATING PROCEDURE*** State Form 39870 (R/ S- 06)	Reference Number CIS-006
	Subject Department Technology	
	Special Instructions Replaces CJD-006 dated April 30, 2015	Effective Date **September 15, 2018**

I. PURPOSE

Establish guidelines for the use and care of all Department computers and systems to include the use of Department email, the Internet, and the Intranet.

II. POLICY

Department computers and all related systems shall be properly maintained and used as established in this procedure. All personnel shall maintain proper levels of security when utilizing Department computers to include the contents, transfer, and distribution of the contents.

III. DEFINITIONS

A. Personal Computer Use − De minimis* personal use of Department computers is permitted as outlined in the State Ethics Rule 42 IAC 1-5-12 and in this procedure. *(*De minimis means so insignificant that it does not give rise to a level of sufficient importance to be dealt with judicially).*

B. Department Technology – For the purposes of this SOP, Department technology is defined as any computer (desktop, laptop, or other in-car computers), tablet, smart device or any other electronic devices (as defined by the Indiana Office of Technology-Information Resource Agreement-IRUA) and used for Department business.

IV. TABLE OF CONTENTS

V. DEPARTMENT TECHNOLOGY

A. Use and responsibility.

1. All Department (owned or provided) technology, associated equipment, software, and all information developed while on the job* and/or while using state facilities or resources is the exclusive property of the Department and the State of Indiana.

* This also includes information, data, and software downloaded, moved to, or stored on personal external hard drives, flash drives, or other external storage devices.

2. Employees shall not have any expectation of privacy with respect to any computer files/data or electronic communication conducted with or through any Department or state computer.

3. The Department reserves the right to monitor the use of all Department computers, including the associated software, equipment, external storage devices, writeable media, and information contained on any external device; including, but not limited to, in and out going e-mail, messaging, and Internet/Intranet usage to determine whether there has been a violation(s) of Department policy, breach of security, or an unauthorized action(s) on the part of an employee, or for any other lawful purpose.

a. Internal audits of all information resources, as defined by the IRUA, may occur at any time;

b. All electronic business shall be conducted in a professional manner, consistent with all state and Department procedures; and

c. Accessing or transmitting unauthorized messages/materials such as: obscene language, images, or jokes; sexually explicit messages/materials; messages/materials that disparage any person, group, or classification of individuals; or solicitations pertaining to buying or selling is strictly prohibited whether or not a recipient has consented to or has requested such message/material. The provisions of this section do not prevent the access or transmittal of the above described materials if done solely for legitimate Departmental business purposes.

4. *De minimis* use of Department computers for reasonable and limited personal use is permitted. **Limited "personal use,"** as it applies to this SOP, **does not include** use of a Department computer for:

a. Social networking, e.g. Facebook, MySpace, etc.,
b. Non-Department employment,
c. Buying, selling or trading of a personal nature, e.g. eBay, Overstock, etc., or
d. Any other action that would tend to discredit or reflect unfavorably upon the employee, Department, or any of its employees.

5. Employees may, for legitimate Department needs or for investigative purposes, access social networking sites, or other normally prohibited sites when necessary to gather information or to aid in an investigation. Employees may request access to these sites, if needed, through channels to the Assistant Chief of Staff (AC/S) Communication and Information Systems (CIS).

6. Employees who wish to use Department computers or accounts to join or access professional business related networking sites shall request permission, through channels, from their appropriate Zone, Division, or Section Commander.

B. Non-Department software, programs, and games.

1. Department employees <u>SHALL NOT</u> install software or programs onto Department computers, tablets, and smart devices without authorization. *Note: if in the course of conducting official State Police business if exigent circumstances exist, programs may be downloaded and installed immediately. The affected employee will be required to forward a memo, through channels, to the AC/S CIS explaining the incident in detail, as soon as possible, as dictated by the situation.*

2. The AC/S CIS or a designee may grant permission to install additional software to support or enhance specific job functions. Examples of such functions include, but are not limited to: cyber crime investigations, computer forensics, CIU, and DES Technical Services.

3. Games of any type are not authorized to be on any Department technology unless such games are needed for a legitimate Department business. Employees shall not play unauthorized games using a Department computer, regardless of whether the game is installed on the computer itself or is run from a CD or any other external storage device. Employees shall not play computer games while on duty, except as noted above.

4. Employees shall not circumvent, or attempt to circumvent any system security measure, including security software or computer security settings, on any Department or state computer unless authorized by the AC/S CIS.

5. No person shall copy, share, distribute, disclose, sub-license, modify, reverse engineer, or sell any software that is the property of the Department without prior written approval of the Superintendent or proper designee.

6. All state owned software shall be procured through the appropriate state procedures.

7. The use of state owned software on non-state owned equipment shall be permitted only with the written approval of the AC/S CIS or a designee.

C. Any computer, computer peripheral (e.g. printer, hard drives, burners, etc.) or IT-related items purchased for Department use by an employee or outside person or entity (e.g. a prosecutor's office, a grant, etc.) shall be approved by AC/S CIS or a designee prior to purchase and installation.

D. **Passwords and encryption keys** are the property of the Department and the individual employee. Passwords are confidential and shall not be shared with unauthorized persons. Employees shall immediately disclose the password or encryption key for any and all files, emails, applications, or other materials stored on a Department owned computer or storage device when directed to do so by the AC/S CIS.

VI. PROTECTION OF SENSITIVE INFORMATION

A. It is the responsibility of all employees to properly protect all sensitive information contained within a Department computer. Transportation or transfer of sensitive information, as defined below, on external drives, writeable media, wireless devices, or any other removable or portable device is prohibited without the use of an approved encrypted device. The approved encrypted device is an encrypted flash drive that is purchased, through the proper Department procedures, from the Indiana Office of Technology (IOT).

B. Sensitive information includes, but is not limited to, the following:

1. Material that is law enforcement sensitive;
2. Criminal investigative information that is not publicly disclosable;
3. Information that is not disclosable under Access to Public Records laws;

4. Grand Jury material;
5. Criminal intelligence information; and
6. Material that contains a Social Security Number, financial information, or any personal information that is protected from disclosure by law.

C. If electronic transmission of sensitive information is necessary; the warning in section IX. B. 3. must be included.

D. Employees utilizing a computer containing sensitive information shall lock the computer when it is unattended.

E. Employees will only use Department issued or authorized encryption applications, software, or schemes. In accordance with IOT policy, passwords will be at least eight (8) characters in length and must contain three (3) of the following: lower case letters, upper case letters, special characters (*,&^), or numbers. The password will not be a word or phrase that can commonly be found in a dictionary or encyclopedia.

F. Classified material shall be maintained and accessed in accordance with applicable law.

VII. CARE/MAINTENANCE OF DEPARTMENT COMPUTERS

A. Employees provided with computers are personally responsible for the care and upkeep of the computer and associated equipment. Employees shall maintain the computer in its original condition and appearance, except for normal use and wear. Employees shall not affix stickers or otherwise alter the appearance of the computer, its lid, or case.

B. Employees shall use care in protecting Department computers from unauthorized access, misuse, theft, damage, destruction, modification, or disclosure. If observed, Department employees shall report violations included in this procedure to their immediate supervisors.

C. Any equipment damage or loss shall be reported, in writing, using the Report of Automobile Crash or Equipment Loss (PD-49, State Form 601).

VIII. CARE AND USE of DEPARTMENT TECHNOLOGY

A. All issued Department technology) shall:

1. Be properly cared for, maintained, and secured by the employee to whom it is issued;
2.. Be guarded from extreme heat, extreme cold, and theft; and
4. When not in use, set to the locked screen

B. While a commission is in motion, the laptop screen shall be in the lowered position. Under exigent circumstances, an officer may conduct a vehicle license check while the vehicle is in motion. When doing such an inquiry, any entry made while in motion does not interfere with the safe operation of the commission.

C. Upon receiving notification of a wanted person or a stolen item (referred to as a “hit”), a follow up confirmation must occur before enforcement action is taken.

IX. USE OF EMAIL, INTERNET, INTRANET and SHAREPOINT

All employees' network and email accounts will be terminated upon their last regular duty workday. Upon special request, through channels to the AC/S CIS, email privileges may remain in effect until a date determined by the AC/S CIS.

A. **Email**:

1. All Department emails shall be written in a professional and courteous manner consistent with all state and Department procedures.

2. The Department also reserves the right to disclose any electronic message(s) sent or received by an employee for use in an authorized investigation without prior notice to that employee.

3. Employees shall not have a privacy interest in emails sent or received on any State owned system or computer. Emails and other correspondence may be accessed, reviewed, and/or copied for the purposes of Open Records requests, discovery requests, disciplinary inquiries, internal investigations or any other matter in the course of conducting responsible government.

However, an employee shall not access another employee's email account for any illegitimate or non-business purpose.

4. No employee shall misrepresent themselves or another person as the author of an email message ("spoofing" sender identification,) unless authorized to do so as part of an investigation.

B. **Business-sensitive, restricted, or confidential information** may be sent by email under the following conditions:

1. The information shall only be sent within the scope of an employee's official duties;
2. Proper care will be taken to ensure the information is sent to the proper recipient; and
3. All applicable emails or faxes shall include (at a minimum) the following notice:

Statement of Confidentiality: This message is intended only for the individual or entity to which it is sent and may contain information that is privileged, confidential, and protected from disclosure under applicable law. If you are not the intended recipient, or the agent responsible for delivering the message to the recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is prohibited. If you have received this message in error, please notify the sender immediately and destroy all copies of the original message.

C. Retention of "official-business" related email correspondence.

1. All email correspondence sent or received, in an official capacity, while conducting Department business shall be retained by the employee for:

a. A minimum of three (3) years from the date the email was sent or received; or
b. If the subject of the e-mail falls within existing Department records retention schedules, the e-mail shall be retained for the time period specified on that schedule.

2. Routine or casual correspondence, even when that correspondence is in regards to "official business," is not covered under this retention policy and may be deleted at any time.

D. Connecting non-agency "Smartphones or tablets" to the State's email system

Department personnel are authorized to connect to the email system and shall:

1. Review IOT's policy on Smartphone connections;
2. Protect any state information, emails, or attachments contained on the personal Smartphone;
3. Notify their supervisor if a "connected" Smartphone is lost or stolen;
4. Personnel shall not attempt to bypass any IOT or CIS security standards; and
5. Shall install MobileIron from IOT onto the device.

E. Use of the Internet/Intranet/SharePoint.

1. Personnel shall not download programs from the Internet, unless authorized to do so.

2. Individuals authorized to download programs shall comply with copyright or licensing agreements.

3. The Internet shall be used to explore information useful to the Department.

4. If an employee, who does not have a legitimate Department business purpose, accesses an inappropriate or questionable Internet site, the employee shall immediately notify their immediate supervisor, by email, with a brief description of the content and the address of the accessed site.

5. Information obtained from the Department's Intranet or SharePoint is for Department use only.

F. Any inappropriate use of the Department's email, Internet, or other electronic services may result in the loss of access privileges and/or disciplinary action. In the course of their duties, system operators, managers, supervisors, and commanders shall monitor the use of the email, Internet systems and may review the contents of applicable stored records.

G. This procedure is to be used in conjunction with all relevant Department regulations, rules, policies and procedures.