Effective: 07/19/1999
Last Revised: 09/15/2019

CSU FULLERTON POLICE DEPARTMENT
GENERAL ORDER NUMBER 6-11

COMPUTER CRIMES INVESTIGATIONS

SUBJECT: Computer Crimes Investigations

PURPOSE: To establish specific basic protocol in the receiving and investigation of crimes and incidents involving California State University, Fullerton electronic communications mediums, data, files and equipment.

POLICY: It shall be the policy of this Department to investigate all computer crimes. This Department shall develop and maintain a basic computer crimes investigation function, which will provide initial follow-up investigation of reported computer crimes, and coordinate supplemental investigative steps when necessary.

On-campus computer services personnel may be considered for assistance and guidance in additional investigative steps. It is the intention of this Department to collaborate efficiently and effectively with the University Computer Center administrators in maintaining the level of information accessibility currently enjoyed and expected for the educational process of the University.

PROCEDURE:

I. Definitions:

A. Computer Data: "is information processed or stored by a computer. This information may be in the form of text documents, images, audio clips, software programs, or other types of data."

B. Computer Forensic: "is the application of computer investigation and analysis techniques to gather evidence suitable for presentation in a court of law."

II. According to the United States Department of Justice, computer crimes are classified into the three following categories:

A. Computer Abuse: "Encompasses a broad range of intentional acts that may or may not be specifically prohibited by criminal statutes. Any intentional act involving knowledge of computer use or technology is computer abuse if one or more of the perpetrators made gain and/or one or more victims suffered or could have suffered loss."

B. Computer Fraud: "Is any crime in which a person 'may use the computer either directly or as a vehicle for deliberate misrepresentation or deception, usually to cover up the embezzlement or theft of money, goods, services, or information."'

C. Computer Crime: *"Any violation of a computer crime statute."*

Computer crimes may include:

1. Embezzlement
2. Computer hacking
3. Telecommunications fraud
4. Records tampering
5. Child Pornography
6. Drug crimes
7. Gaming crimes
8. Other organized crimes
9. Identity Theft
10. Extortion/Revenge porn

III. Computer Crimes Investigation – The basic investigation of any reported computer crime should follow these steps whenever possible:

A. Collecting Evidence - There are important factors to consider in reviewing any evidence. Officers should make the following assessments:

1. Determine the skills of the reporting party. Make sure that the victim is capable of illustrating what has occurred with the equipment concerned.
2. Determine if the equipment can be moved without jeopardizing the evidence.
3. Identify the complete number of affected pieces of equipment. If it appears the area involves a great deal of equipment, i.e., an educational Department or lab or classroom, it may be necessary to cordon off the area. However, if only one or two terminals are involved, these pieces can be taken as evidence and returned to the police station for further examination.
4. Whenever copies of suspect files are to be made, i.e., adult material or evidence of hacking, the Orange County District Attorney's Computer Forensics lab will be used to conduct a computer forensic examination.

B. Determine approximate Crime - Officers must make reasonable attempts to identify the possible violation, even if it involves only University policy breaches. By doing so, lesser violations will provide for swift administrative responses, as well as serve as an early warning sign for possible future criminal acts and areas of concern. In attempting to make this assessment, officers need to identify the following:

1. If the case involves theft of files, system sabotage involving any computer contaminant (virus), or hacking any University server for unauthorized information, services, monies or goods;

2. If the case involves any of the criteria listed above the officer must attempt to list the actions of the virus, files destroyed or hacked, etc. This is important as it will provide a more informed second phase of investigation, and avoid destruction of police Department equipment and/or files;

3. Officers are reminded that incident reports can include violations of the University Sexual Harassment, Workplace Violence and electronic communications policies, as well as criminal acts as outlined in the California Penal Code.

C. Preparing the Initial Report - First-responders are reminded to provide the following information when preparing the initial crime or incident report:

1. The computer format (PC, MAC, LINUX, OR UNIX);
2. The dates of occurrence as recorded by the computer;
3. The files affected (if known);
4. The service capabilities or functions of the violated equipment, i.e., educational department Internet, faculty office, records, information server or personnel files, intellectual properties, etc.

D. Notification –First responders need to be aware that Administrative historical files of access and logon information are only maintained for only a limited amount of time. An investigator should be notified as soon as possible in any serious cases so that tracing evidence is not lost due to historical logs being purged by the Information Technology System.

IV. Seizing Electronic Evidence [CALEA 83.2.5]

A. Personal or Laptop Computers

1. If the computer is "OFF", do not turn it "ON".
2. If the computer is "ON", consult a computer specialist. If there is no computer specialist available:
   a. Photograph the screen, then disconnect all power sources; unplug from the wall and the back of the computer.
   b. Place evidence tape over each drive slot.
   c. Photograph/diagram and label back of computer components with existing connections.
   d. Label all connectors/cable ends to allow reassembly as needed.
   e. If transport is required, package components and transport/store components as fragile cargo.
   f. Keep away from magnets, radio transmitters and other hostile environments.

B. Network Servers

1. Consult a Computer specialist for further assistance
2. Pulling the plug could:
    a. Severely damage the system
    b. Disrupt legitimate business
    c. Create officer and/or Department liability

C. Wireless Telephones, Smart Phones, Pagers, Personal Data Assistant

1. Potential Evidence Contained in Wireless Devices
    a. Contacts
    b. Incoming/outgoing call log
    c. Numbers stored for speed dial
    d. Caller ID for incoming calls
    e. Videos
    f. Pictures
    g. Text messages
    h. Cell phone apps
    i. Notes
    j. Internet browser history
    k. Other information contained in the memory of wireless telephones could include:
        1) Phone/pager numbers
        2) Names and addresses
        3) PIN numbers or passwords
        4) Voice Mail access number
        5) Voice Mail password
        6) Debit card numbers
        7) Calling card numbers
        8) E-mail/Internet access information
        9) The on-screen image may contain other valuable information.

2. "ON" / "OFF" Rule
    a. If the device is "ON", do not turn it "OFF".
        1) Turning it "Off" could activate a lockout feature.
        2) Write down all the information on display (photograph if possible)
        3) Power down prior to transport and take any power supply cords present.
        4) Make every effort to obtain user names and passwords.
    b. If the device is "OFF", leave it "OFF".
        1) Turning it "ON" could alter evidence on the device
        2) Upon seizure get it to an expert as soon as possible or contact a local service provider.
        3) Make every effort to locate any instruction manuals pertaining to the device.

D. Other Devices: fax machines, video game consoles, external hard drives, home digital recording devices.
   1. If a device is found "ON", powering it down may cause loss of data. If a device is found "OFF", leave it "OFF". Turning it "ON" could alter the device.
   2. Consult a computer forensics specialist for instructions on how to collect such devices.

E. Smart Cards

   1. A smart card is a plastic card the size of a standard credit card that hold a microprocessor(chip) which is capable of storing monetary value and other information.
   2. Examination of a Smart Card
      a. Label and identify the physical characteristics of the card
      b. Photograph the smart card
      c. Features are similar to credit cards/driver's license
      d. Examine for possible alteration or tampering
   3. The Uses of Smart Cards
      a. Point of sale transactions
      b. Direct exchange of value between cardholders
      c. Exchange of value over the Internet
      d. ATM Capabilities
      e. Capable of storing other data and files similar to a computer.
   4. Circumstances Raising Suspicion Concerning Smart Cards
      a. Numerous cards with different names or same issuing vendor
      b. Signs of tampering
      c. Cards found in the presence of computer and/or other electronic devices
   5. Questions to Ask When Encountering Smart Cards
      a. Who is the card issued to? Who is the valid cardholder?
      b. Who issued the card?
      c. What are the specific uses of the Smart Card?
      d. Why does the person have numerous cards?
      e. Can this computer or electronic device alter the card?
   6. Smart card technology is used in some cellular phones and may be found in or with cellular/wireless devices.

V. Precursory Search

A. A precursory search of an electronic device may be conducted if the owner of the device has given consent. The search may only be conducted in the following manner.

   1. The search is conducted by personnel having computer forensic training.
   2. The search is conducted using sound computer forensic software and hardware.

3. Digitally recorded or written consent to search the electronic device has been obtained by our Department.
4. The person conducting the search must document all searching information to include locations searched and content found.
5. The search must stop when any evidence or contraband is located and a search warrant obtained for a complete forensic examination.

VI. Training:

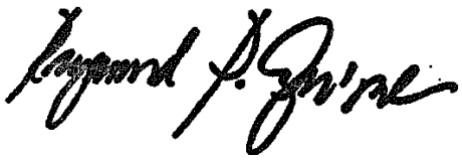
A. Whenever possible, Department Personnel will receive training to help increase their understanding and expertise in investigating computer crimes.

B. The training may consist of the following:

1. A basic computer crimes investigation course, POST approved.
2. Participation in existing CSU and Orange County Investigator's meetings when such cases are reviewed, or when pertinent material is available for distribution.
3. Regular monitoring of activity and trends on the Internet, as well as technological advances within the World Wide Web, Newsgroups, Internet Relay Chat Lines (IRC) and other mediums;
4. Regular exploration of equipment advances so as to maintain basic understanding of hardware and software functions and abilities, as well as advances in Operating Systems;
5. Regular conferencing with regional task forces, agencies and corporate law enforcement liaisons to maintain resource networks for investigative support.

REVIEWED BY:
P.Launi

APPROVED:



Raymund Aguirre
Chief of Police

California Penal Code Sections 502, 653(m):

California State University, Fullerton, *Human Resources Policy Manual, Student Handbook, University Library computer Center User's Agreement.*