California State University, Los Angeles
Department of Public Safety

NUMBER:	IV-20	APPROVED:	Gregory D. King, Chief of Police
EFFECTIVE:	May 1, 2007		
SUPERSEDES:	1/1/2001	Reviewed/Revised:	May 1, 2010
SUBJECT:	**Computer Crimes Investigations**		

I. PURPOSE:

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

II. POLICY:

It shall be the policy of this Department to investigate all computer crimes. The University Police 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.

III. DEFINITIONS:

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: *"Is 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; and/or
8. Other organized crimes.

IV. PROCEDURES:

A. Computer Crimes Investigation and procedures for the seizure of computer equipment and other devices capable of storing data in an electronic format.

1. 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. First responders 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 and without risk to remaining workstations. **Officers are reminded; however, that the most preferable solution is copying suspect files, if at all possible.**

4) Whenever copies of suspect files are to be made, i.e., adult material or evidence of hacking, utilize the violated terminal to complete the file copy process.

In any case, officers shall make investigative actions only on copies of suspect material so as to avoid the loss of evidence for court proceedings.

b. Determine approximate Crime - First-responders 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 or monies or goods;

2) The officer must attempt to list the actions of the virus, files destroyed or hacked, etc. This is important for it will provide for 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 or MAC);

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.

2. Transportation and storage of seized computer related equipment.

a. Notification to the Investigations Section personnel is recommended before any items are seized and transported.

b. The Property Evidence Custodian should be involved, if possible, in the packaging of the computer equipment on scene to ensure a strict chain-of-evidence.

c. Items seized will be entered into the evidence tracking system and included in the ARMS report. The crime/incident report will include specifics on the chain of custody and packaging processes employed.

B. Training:

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

2. The training may consist of the following:

a. A basic computer crimes investigation course, POST approved.

b. Participation in existing CSU local area Investigator's meetings when such cases are reviewed, or when pertinent material is available for distribution.

c. 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;

V. APPENDICES: None.