POLICY STATEMENT
Commonwealth of Pennsylvania • Department of Corrections

Policy Subject:		Policy Number:
Computer Forensic Investigations (CFI)		**2.4.1**
Date of Issue:	**Authority:**	**Effective Date:**
August 28, 2009	**Signature on File** **Jeffrey A. Beard, Ph.D.**	**September 4, 2009**

I. AUTHORITY

The Authority of the Secretary of Corrections to direct the operation of the Department of Corrections is established by Sections 201, 206, 506, and 901-B of the Administrative Code of 1929, 71 P.S. §§61, 66, 186, and 310-1, Act of April 9, 1929, P.L. 177, No. 175, as amended.

II. APPLICABILITY

This policy is applicable to all facilities operated under the jurisdiction of, or conducting business with the Department of Corrections.

III. POLICY

It is the policy of the Department to ensure the use of computers and any other devices capable of storing ***and transmitting*** electronic data are in compliance with Department policies, rules, regulations, and applicable laws and statutes of the Commonwealth of Pennsylvania and the United States.

IV. PROCEDURES

All applicable procedures are contained in the procedures manual that accompanies this policy document.

V. SUSPENSION DURING AN EMERGENCY

In an emergency or extended disruption of normal facility operation, the Secretary/designee may suspend any provision or section of this policy for a specific period.

VI. RIGHTS UNDER THIS POLICY

This policy does not create rights in any person nor should it be interpreted or applied in such a manner as to abridge the rights of any individual. This policy should be interpreted to have sufficient flexibility to be consistent with law and to permit the accomplishment of the purpose(s) of the policies of the Department of Corrections.

VII. RELEASE OF INFORMATION AND DISSEMINATION OF POLICY

A. Release of Information

1. Policy

   This policy document is public information and may be released upon request.

2. Confidential Procedures (if applicable)

   Confidential procedures for this document, if any, are not public information and may not be released in its entirety or in part, without the approval of the Secretary of Corrections/designee. Confidential procedures may be released to any Department of Corrections employee on an as needed basis.

B. Distribution of Policy

1. General Distribution

   The Department of Corrections' policy and procedures shall be distributed to the members of the Central Office Executive Staff, all Facility Managers, and Community Corrections Regional Directors on a routine basis. Distribution of confidential procedures to other individuals and/or agencies is subject to the approval of the Secretary of Corrections/designee.

2. Distribution to Staff

   It is the responsibility of those individuals receiving policies and procedures, as indicated in the "General Distribution" section above, to ensure that each employee expected or required to perform the necessary procedures/duties is issued a copy of the policy and procedures either in hard copy or via email, whichever is most appropriate.

VIII. SUPERSEDED POLICY AND CROSS REFERENCE

A. Superseded Policy

1. Department Policy

   2.4.1, Computer Forensic Investigations, issued November 17, 2006, by Secretary Jeffrey A. Beard, Ph.D.

2. Facility Policy and Procedures

   This document supersedes all facility policy and procedures on this subject.

B. Cross Reference(s)

1. Administrative Manuals

2. ACA Standards

   a. Administration of Correctional Agencies: None

   b. Adult Correctional Institutions: None

   c. Adult Community Residential Services: None

   d. Correctional Training Academies: None

PROCEDURES MANUAL
Commonwealth of Pennsylvania • Department of Corrections

Policy Subject:		Policy Number:
Computer Forensic Investigations (CFI)		**2.4.1**
Date of Issue:	**Authority:**	**Effective Date:**
August 28, 2009	**Signature on File** **Jeffrey A. Beard, Ph.D.**	**September 4, 2009**

Release of Information:

Policy Document: This policy document is public information and may be released upon request.

Procedures Manual: Confidential procedures for this document, if any, are not public information and may not be released in its entirety or in part, without the approval of the Secretary of Corrections/designee. Confidential procedures may be released to any Department of Corrections employee on an as needed basis.

Section 1 – General Procedures

Section 2 – Responsibilities

Section 3 – Evidence Control

Attachments (By Section)

Section 3 – Evidence Control

Section 1 – General Procedures

A. *Investigation Authorization Requests and Approvals*

1. The following Department personnel are authorized to approve/direct an investigation which involves the ***introduction of or confiscation of cellular phones, the*** use/misuse of computers and any other related devices capable of storing ***and transmitting*** electronic data:

   a. Secretary/designee;

   b. Executive Deputy Secretary/designee; and

   c. Regional Deputy Secretary(ies)/designee.

2. An investigation request can be submitted by e-mail, letter, and/or fax.

3. If the investigation request is approved, the request shall be forwarded to the Director of the Office of Professional Responsibility (OPR).

4. The Facility Manager/designee and/or Bureau Director shall make his/her investigation request through his/her respective Deputy Secretary.

B. *Shutdown of User Workstation*

1. When the OPR investigator is on-site and prepared to take custody of the user's workstation and at the request of the Director of OPR, the Network Administrator will issue a "Shutdown" command to the workstation. This will close all running applications and log the user off.

2. If the computer will not shutdown remotely and the user is not cooperative in logging off, then the investigator should pull the power plug on the workstation.

3. To disable and/or capture email, the OPR Director shall make the request in writing to the Deputy Secretary for Human Resources and Management, Office of Administration.

CONFIDENTIAL

2.4.1, Computer Forensic Investigations

Section 2 – Responsibilities

This section is confidential and not for public dissemination.

CONFIDENTIAL

2.4.1, Computer Forensic Investigations

Section 3 – Evidence Control

This section is confidential and not for public dissemination.

Application Administrator – A person assigned to perform restricted functions for specific computer applications/systems, such as assigning users, creating backup files, loading or restoring data from CD-ROMs or other media.

Application Administrator Password – A confidential alphanumeric code used to logon to a computer or system to perform restricted functions for specific computer applications/systems, such as assigning users, creating backup files, loading, or restoring data from CD-ROMS or other media.

Automation Coordinator – Person designated by his/her facility and approved/trained by the Bureau of Information Technology to perform tasks outlined in this policy.

Basic Input Output System (BIOS) – Initial instruction set used during the startup of a computer system.

Cellular Telephone – a long-range electronic device used for mobile voice or data communication over a network of base stations known as cell sites.

Central Office Managers – Central Office Bureau, Office Directors, and Division Chiefs.

Computers – Shall include, but is not limited to, microchips, desktop computers, lap top computers, notebook computers, portable computers, palmtop computers (PDA), minicomputers, mainframe computers, and any other devices that store electronic data (e.g., cellular phones, Blackberries, etc.)

Computer Crime – Any act(s) or conduct that constitutes a violation of the Pennsylvania Crimes Code, including Chapter 76, Computer Offenses, applicable Federal Laws, Department policies, Rules and Regulations, and related laws and statutes that involve the possession, control, and use of a computer and/or other related electronic communications devices.

Computer Forensics – The scientific examination and analysis of data held on, or retrieved from, computer storage media in such a way that the integrity of the information can be used as evidence in a court of law.

Computer Forensic Investigations (CFI) – A scientific investigation involving acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media.

Computer Forensic Unit (CFU) – An investigative unit employed by the Department with specialized training responsible for the recovery, analysis, and subsequent presentation of electronic evidence to a court of law.

Compact Disk (CD) – The storage of digital data in machine-readable form, accessible with a laser-based reader. CDs are 4-3/4” in diameter.

Computer Disc Read Only Memory (CD-ROM) – A data storage system using CDs.

Computer Inventory – The Department's official central inventory of information technology equipment and software as maintained by the Bureau of Information Technology.

Confidential Information – Information that is protected from disclosure by law, is treated or designated by law as confidential, specifically has been designated as confidential by the Department or another agency of the Commonwealth, as well as information the disclosure of which could threaten the security of the Department or any Departmental facility, facilitate an escape or create a danger to a member of the staff, a contractor, the public, or inmates.

Copyright – Legally enforceable ownership rights in published intellectual property, such as software. The copyright-holder for a piece of intellectual property possesses the exclusive rights to reproduce and distribute the intellectual property and power to grant the rights of reproduction and distribution to others.

Complementary Metal Oxide Semiconductor (CMOS) – Storage area for the initial instruction set used during the startup of a computer system.

Data Communications Network – A telecommunications medium and associated components responsible for the transportation of computer information from one location to another.

Desktop Computer – Desktop or tower configuration microcomputers used by employees, inmates, contractors, and individuals within the Department.

Document Password – A password used to restrict access to a single document.

E-Mail – Electronic mail sent or received by Department employees.

Employees – Full-time, part-time limited term wage, intern, or contracted staff employed by the Department, as well as volunteers and visitors.

Electronic Devices – All Commonwealth owned/controlled computer equipment that has a storage device or persistent memory, including but not limited to, desktop computers, laptops, servers, personal data assistants (PDAs), printers, routers, switches, firewall hardware.

Electronic Media – All media on which electronic data can be stored, including but not limited to, hard drives, magnetic tapes, diskettes, CDs, DVDs, and USB storage devices.

Floppy Disk – A thin, flexible plastic disk which has been coated with iron oxide, capable of storing computer data as a magnetic pattern.

Forensic Examiner – An investigator with specialized training responsible for the recovery, analysis, and subsequent presentation of electronic evidence to a court of law.

Full Access E-Mail User – A user who, in addition to having the capabilities of sending and receiving e-mail within the Department's e-mail system, has access to "Internet" or "Outside" e-mail.

Hard Drive – A mass storage device for digital data.

Internet – The worldwide network of networks that are connected to each other and provide unique identification of all computing resources connected.

Internet Browsing Software – Software used to locate and examine information accessible on the Internet.

Internet Connection – A PC that has the ability to connect to the Internet.

Internet or Outside E-Mail – E-mail that travels over the "Internet" between the Department's E-Mail system and the E-mail system of another state agency or private company. Any E-mail message sent to or received from someone outside the Department is referred to as either "Internet or "Outside" E-mail.

Limited Access E-Mail User – This user has the capability to send and receive E-mail only within the PA State Government E-Mail System (CWOPA Global Address List).

Microcomputer – Programmable desktop or portable (handheld, laptop, palmtop, etc.) computers each of which may have its own microprocessor, operating system, and application software. These units can function in a stand-alone mode, as part of a Local Area Network (LAN), and/or as a terminal emulation device connected to a mainframe computer. A microcomputer may also include a display screen, integral data storage, communication, and document scanners are also considered a part of the microcomputer.

Operating Systems – Program that runs other programs. They perform basic tasks, such as responding to input, displaying output, organizing files and directories, and they work devices such as disk drives and printers. Windows NT and Windows 2000 are examples of operating systems.

Password – An alphanumeric code used to log onto a computer or system to access its services, files, and programs. Use of a password is intended to limit the persons who can access certain functions or information.

Peripherals – A general term for any of the external devices (mouse, keyboard, CD-ROM, scanner, etc.) attached to information technology equipment.

Personal Password – A password used in conjunction with a person's own User-ID to provide access to computer systems.

Screensavers – Programs designed to automatically place graphics, pictures, etc. on a computer monitor in place of applications or data when it detects that a computer has not actively been used for a certain period of time. Also included are programs designed, for amusement purposes, to place images or animated characters on a screen either in place of or along with applications or data.

Secure Area – An area in which inmates are not assigned to work and which is always locked when staff members are absent.

Secured Perimeter – Barrier that defines the inner-compound of a correctional facility.

Secure Storage – A locking desk, file cabinet or similar non-portable storage.

Staff – Any employee of the Commonwealth of Pennsylvania or any person working under contract with the Commonwealth.

Subject Computer/Media – The computer or media that is being examined.

System Administrator Password – A confidential alphanumeric code used to logon to a computer or system to access restricted functions such as operating system and network configuration settings.

User-ID – A unique identifier (user name) used to identify a person who logs onto a computer. Generally, User-Ids are not confidential.

Virus – A program that is designed to copy itself, attach itself to other programs, and spread onto other computers and then to perform functions which annoy the user, interrupt normal computer operations, destroy files or access/copy information without authorization. Viruses are often unintentionally downloaded from web sites or passed via floppy disks or through attachments to E-mail.

Workstation – A microcomputer connected to a network for the purpose of using network resources.