POLICY TITLE: Access Control Security Standard CHAPTER: HIPAA Security Policy		PAGE 1 OF 4
	CHILD AND FAMILY SERVICES AGENCY Approved by:_____ Signature of Agency Director	PROFESSIONAL STANDARDS See Section VII.
EFFECTIVE DATE: May 1, 2008	LATEST REVISION: April 22, 2008	REVIEW BY LEGAL COUNSEL: April 15, 2008

I. AUTHORITY	The Director of Child and Family Services Agency adopts this policy to be consistent with the Agency's mission and applicable federal and District of Columbia laws, rules and regulations, including Health Insurance Portability and Accountability Act, Security Rule, 45 C.F.R. § 164.312 (a)(1) Access Control; DC Law 5-168, Section 4, 32 DCR 721; DC Law 11-259, Section 305(a), 44 DCR 1423; DC Code Section 1-1135, b, (6); DC Law 12-175. Act 12-239; and the LaShawn A. v. Fenty Amended Implementation Plan.
II. APPLICABILITY	Full or part-time CFSA employees; contractors who are authorized to use CFSA's equipment or facilities; and volunteers who are authorized to use and have been provided with a user account to access CFSA resources.
III. RATIONALE	This document establishes a policy for the workforce members of all HIPAA covered agencies to/your agency comply with the Access Control Standard of the Administrative Simplification provision of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The purpose of this policy is to establish and implement specific guidelines for gaining access to and procedures for automatic logoff from the computer networks, as well as, guidelines for the appropriate use of computer networks and equipment, and the encryption and decryption of sensitive or confidential information.
IV. POLICY	The CFSA will ensure appropriate access of all workforce members and shall establish procedures that, based upon the workforce members' job requirements, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
V. CONTENTS	**A.** Computer User Access Control **B.** Access Control User Guidelines **C.** Electronic Access Security **D.** Advanced Authentication Techniques **E.** Roles and Responsibility

VI. PROCEDURES	**Procedure A: Computer User Access Control** CFSA is committed to providing an environment that encourages the use of computers and electronic information. Computer facilities and systems include, but are not limited to, the computers, printers, networks, routers, and related equipment, as well as data files, programs and/or documents managed or maintained by CFSA, which reside on electronic media. Computer facilities also include computer rooms, telecommunication and data distribution areas, computer labs, offices, classrooms, and furnishings operated and maintained by CFSA. 1. CFSA's computer network system and facilities are to be used for legitimate business and education purposes only and are not for personal use. The following uses, among others, are considered violations of this standard, and are **strictly prohibited**: a. Game-playing; b. Use of CFSA computers for personal work or political purposes; and c. Accessing, viewing or downloading pornographic or other obscene material. 2. No CFSA computer or network system or facility shall be used to transmit or receive any material that may be considered offensive, demeaning, disruptive or harassing in nature. Such material includes, but is not limited to: • material that is inconsistent with CFSA's policies and regulations governing equal employment opportunity and harassment. 3. Computers network facilities are the property of CFSA, and in order to ensure compliance with applicable law and this standard and the Information Security Policy, CFSA reserves the right to inspect all computer files and any information transmitted via its computer network facilities. Such inspection may occur if CFSA has reasonable cause to suspect that anyone is using its facilities for illegal or illicit purposes, or for purposes inconsistent with these standards and other applicable policies. CFSA authorities without notice, consent or a search warrant may conduct an inspection. 4. Accordingly, no user should have any expectation of privacy in any information that is transmitted, received or stored on CFSA computer network facilities. This specifically applies to, but is not limited to, e-mail and Internet messages and information.
	Procedure B: Access Control User Guidelines 1. Never share your username, password, or security access token with anyone else. 2. Do not use someone else's username, password or security access token. If you need additional access or if you are having problems with your current access, contact the Help Desk.

3. Do not use obvious, trivial or predictable passwords such as; names of relatives or pets; street names; days and months; repetitive characters; dictionary words; and common words such as PASSWORD, SECURITY, SECRET, etc.

4. Beware of "Shoulder Surfers", (people who stand behind you and look over your shoulder) while you are keying in your password, or while you are working with confidential information.

5. Do not use your access privileges to enable other individuals to access information that they are not authorized to access, or to submit transactions that they are not authorized to submit.

6. Never write down your passwords, or, post them on your PC, or other obvious places.

7. Always change the initial password assigned to you by the Help Desk as soon as you receive it.

8. Always change your passwords when prompted, at least every 60 days or more often if necessary.

9. Log-off when you are finished using your terminal or workstation, or if you are stepping away from your desk, even momentarily. If you are going to be away from your office for an extended period, contact the Help Desk to have your username temporarily disabled until your return.

10. If you suspect that someone else knows any of your passwords, request a change via the Help Desk immediately.

11. If you lose your security access token, notify your supervisor immediately and/or notify the ISO.

Procedure C: Electronic Access Security

Users of CFSA computer network system must comply with the following guidelines:

1. Users must not deny or interfere with or attempt to deny or interfere with service to other users.

2. Users must not cause, permit, or attempt any destruction; modification or copying of software installed on computing or network facilities.

3. Users must not cause, permit or attempt any destruction or modification of computing or communications equipment; including, but not limited to, reconfiguration of hubs, switches, routers, etc.

4. Users must not move or remove any CFSA-owned or administered computer equipment or documents from the computer network. This includes, but is not limited to, detaching any desktop computer or printer from an Ethernet, ISDN, ATM, Token Ring, etc., port.

5. Users must not physically or electronically attach any other device (such as an external disk, printer or video system) to a CFSA computer without prior approval. Any expense incurred in time, labor or parts from an incompatible or corrupting device will be charged to and is considered the responsibility of the user. Verification of compatibility should be coordinated through the CFSA help desk .

6. In accordance with the Software Management Standard, users must not install any software on any CFSA-owned or administered networked equipment, including, but not limited to operating systems, word-processing software, spreadsheets, games, wallpapers and screen savers.

7. For the purposes of software audits, systems backups or diagnosing systems problems, users must allow CFSA personnel access to all data files and software kept on the networked system.

8. CFSA network and system administrators, and information security personnel will remove any unauthorized or unlicensed software from any CFSA computer. The user is responsible for backing up any files and data under such circumstances.

9. CFSA computer facilities must not be used to threaten or harass any person. A user must cease sending messages or interfering in any way with another user's normal use of the computing or network facilities if the aggrieved user makes a reasonable request for such cessation.

Procedure D: Advanced Authentication Techniques

Considering that one of the most dangerous security threats is impersonation, in which someone uses the username and password of someone else. The identity of a user who has access to data and information classified as CFSA RESTRICTED and CFSA INTERNAL USE ONLY should be verified and authenticated not only by what he/she knows (e.g. password), but also by what he/she owns (e.g. smart card) or by his/her human characteristics (biometrics).

Procedure E: Roles and Responsibility

1. Acceptable Use
   a. Information Security Officer
      i. Establish and maintain an effective Access Control Standard on behalf of the Chief Information Officer.
      ii. Help agencies implement and comply with security standards contained herein.
      iii. Verify CFSA compliance with the minimum requirements of this standard.
   b. CFSA Managers/Supervisors/Users
      i. Comply with this standard.
      ii. Consult the Information Security Officer to obtain assistance.