DATABASE ACCESS REQUEST FORM

This form must be typed or completed on your computer and printed out for signatures in order to be processed
All information should be completed with the exception of Fax and DCF Log-on where not applicable.

1. REQUESTER INFORMATION:

Name: First: _____ MI: ___ Last: _____ User SSN: _____

Contractor ID: _____ Contractor Name: _____

Provider ID: _____ Provider Name: _____

Region:_____ Circuit: ___ County: _____ Phone: _____

Fax: _____ Email: _____

Mailing Address: _____

DCF Issued Log-on (If already assigned one): _____

2. AUTHORIZATION SIGNATURES:

Supervisor's Name: _____

Supervisor's Signature: _____ Signature Date: _____

SAMH Data Liaison or Regional Security Officer Name: _____

⇒ SAMH Data Liaison or Regional Security Officer Signature: _____ Signature Date: _____

⇒ SAMH HQ Security Officer Signature: _____ Signature Date: _____

3. DATABASE SYSTEM(S) TO BE ACCESSED BY THE REQUESTER

☐ **SAMH Database** (☐ **Query Facility,** ☐ **TANF,** ☐ **Data Visibility Reports)** ☐ **SALIS**

☐ **DC Aftercare Referral** ☐ **IRAS (Incident Reporting)** ☐ **Access To Recovery (ATR)**

4. LEVEL AND ROLE OF THE REQUESTER:

a. SAMHIS Roles: (Choose one)

	Administrator	Staff
State		
Region/Circuit		
Contractor		
Sub-Contractor		
DC Facility		

b. IRAS Roles: (Choose one)

☐ **Viewer** ☐ **Initiator** ☐ **Incident Coordinator** ☐ **Death Review Coordinator** ☐ **Child Fatality Prevention Specialist**

☐ **Communications Designee** ☐ **Leadership** ☐ **User Administrator** ☐ **Administrator**

5. ACTION REQUESTED:

☐ Add New User ☐ Deactivate User ☐ Reactivate User ☐ Update User Information

6. CONFIDENTIALITY AND SECURITY REQUIREMENTS/CERTIFICATIONS:

By my signature, I acknowledge that I am responsible for safeguarding the confidentiality and security of **all** information contained in **any** of the above data systems (# 3. above) to which I am granted access as required by the following state and federal laws:

42 Code of Federal Regulation Part 2 and Part 142;
Section 394.4615, Florida Statutes;
Section 916.107(8), Florida Statutes;
45 Code of Federal Regulation Parts 160 and 164;
Section 397.501(7), Florida Statutes;
Section 282.318, Florida Statute

I received: Security Awareness Training on: _____ (MMDDYYYY) HIPAA Training on: _____ (MMDDYYYY) ☐Certificates Attached

Requestor's Signature: _____ Signature Date: _____

SECURITY AGREEMENT FORM

The Department of Children and Families has authorized you:

_____

Employee's or Contractor's Name/Organization

to have access to sensitive data using computer-related media (e.g., printed reports, microfiche, system inquiry, on-line update, or any magnetic media).

Computer crimes are a violation of the department's Standards of Conduct. In addition to departmental discipline, committing computer crimes may result in Federal or State felony criminal charges.

I understand that a security violation may result in criminal prosecution according to the provisions of Federal and State statutes and may also result in disciplinary action against me according to the department's Standards of Conduct in the Employee Handbook.

By my signature below, I acknowledge that I have received, read, understand and agree to be bound by the following:

- The Computer Related Crimes Act, Chapter 815, F.S.
- Sections 7213, 7213A, and 7431 of the Internal Revenue Code, which provide civil and criminal penalties for unauthorized inspection or disclosure of Federal tax data.
- 6103(l)(7) of the Internal Revenue Code, which provides confidentiality and disclosure of returns and return information.
- CFOP 50-2.
- It is the policy of the Department of Children and Families that no contract employee shall have access to IRS tax information or FDLE information, unless approved in writing, by name and position to access specified information, as authorized by regulation and/or statute.
- It is the policy of the Department of Children and Families that I do not disclose personal passwords.
- It is the policy of the Department of Children and Families that I do not obtain information for my own or another person's personal use.
- I will only access or view information or data for which I am authorized and have a legitimate business reason to see when performing my duties. I shall maintain the integrity of all confidential and sensitive information accessed.
- "Casual viewing" of employee or client data, even data that is not confidential or otherwise exempt from disclosure as a public record, constitutes misuse of access and is not acceptable.
- The Department of Children and Families will perform regular database queries to identify misuse of access.
- Chapter 119.0712, Florida Statutes, and the Driver Privacy Protection Act (DPPA).

PRIVACY ACT STATEMENT: Disclosure of your social security number is voluntary, but must be provided in order to gain access to department systems. It is requested, however, pursuant to Section 282.318, Florida Statutes, the Security of Data and Information Technology Resources Act. The Department requests social security numbers to ensure secure access to data systems, prevent unauthorized access to confidential and sensitive information collected and stored by the Department, and provide a unique identifier in our systems.

Print Employee/Contractor Name	Signature of Employee/Contractor	Date
Print Supervisor Name	Signature of Supervisor	Date

CF 114, PDF 06/2010 Distribution of Copies: Original – Personnel File/Contract File; Copy – Employee/Contractor

CHAPTER 815: COMPUTER-RELATED CRIMES

815.01 Short title. The provisions of this act shall be known and may be cited as the "Florida Computer Crimes Act." (History: s. 1, ch. 78-92.)

815.02 Legislative intent. The Legislature finds and declares that:

(1) Computer-related crime is a growing problem in government as well as in the private sector.

(2) Computer-related crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime.

(3) The opportunities for computer-related crimes in financial institutions, government programs, government records, and other business enterprises through the introduction of fraudulent records into a computer system, the unauthorized use of computer facilities, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great.

(4) While various forms of computer crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which proscribes various forms of computer abuse.

(History: s. 1, ch. 78-92.)

815.03 Definitions. As used in this chapter, unless the context clearly indicates otherwise:

(1) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

(2) "Computer" means an internally programmed, automatic device that performs data processing.

(3) "Computer contaminant" means any set of computer instructions designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. The term includes, but is not limited to, a group of computer instructions commonly called viruses or worms which are self-replicating or self-propagating and which are designed to contaminant other computer programs or computer data; consume computer resources; modify, destroy, record, or transmit data; or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

(4) "Computer network" means any system that provides communications between one or more computer systems and its input or output devices, including, but not limited to, display terminals and printers that are connected by telecommunication facilities.

(5) "Computer program or computer software" means a set of instructions or statements and related data which, when executed in actual or modified form, cause a computer, computer system, or computer network to perform specified functions.

(6) "Computer services" include, but are not limited to, computer time; data processing or storage functions; or other uses of a computer, computer system, or computer network.

(7) "Computer system" means a device or collection of devices, including support devices, one or more of which contain computer programs, electronic instructions, or input data and output data, and which perform functions, including, but not limited to, logic, arithmetic, data storage, retrieval, communication, or control. The term does not include calculators that are not programmable and that are not capable of being used in conjunction with external files.

(8) "Data" means a representation of information, knowledge, facts, concepts, computer software, computer programs, or instructions. Data may be in any form, in storage media or stored in the memory of the computer, or in transit or presented on a display device.

(9) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.

(10) "Intellectual property" means data, including programs.

(11) "Property" means anything of value as defined in [Footnote 1] s. 812.011 and includes, but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in either machine-readable or human-readable form, and any other tangible or intangible item of value.

(History: s. 1, ch. 78-92; s. 9, ch. 2001-54.) ([Footnote 1] Note: Repealed by s. 16, ch. 77-342.)

815.04 Offenses against intellectual property; public records exemption.

(1) Whoever willfully, knowingly, and without authorization modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(2) Whoever willfully, knowingly, and without authorization destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(3) (a) Data, programs, or supporting documentation which is a trade secret as defined in s. 812.081 which resides or exists internal or external to a computer, computer system, or computer network which is held by an agency as defined in chapter 119 is confidential and exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution. (b) Whoever willfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation which is a trade secret as defined in s. 812.081 or is confidential as provided by law residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(4) (a) Except as otherwise provided in this subsection, an offense against intellectual property is a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084. (b) If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084. History: s. 1, ch. 78-92; s. 1, ch. 94-100; s. 431, ch. 96-406.)

815.045 Trade secret information. The Legislature finds that it is a public necessity that trade secret information as defined in s. 812.081, and as provided for in s. 815.04(3), be expressly made confidential and exempt from the public records law because it is a felony to disclose such records. Due to the legal uncertainty as to whether a public employee would be protected from a felony conviction if otherwise complying with chapter 119, and with s. 24(a), Art. I of the State Constitution, it is imperative that a public records exemption be created. The Legislature in making disclosure of trade secrets a crime has clearly established the importance attached to trade secret protection. Disclosing trade secrets in an agency's possession would negatively impact the business interests of those providing an agency such trade secrets by damaging them in the marketplace, and those entities and individuals disclosing such trade secrets would hesitate to cooperate with that agency, which would impair the effective and efficient administration of governmental functions. Thus, the public and private harm in disclosing trade secrets significantly outweighs any public benefit derived from disclosure, and the public's ability to scrutinize and monitor agency action is not diminished by nondisclosure of trade secrets. (History: s. 2, ch. 94-100.) (Note. Former s. 119.165)

815.06 Offenses against computer users.

(1) Whoever willfully, knowingly, and without authorization: (a) Accesses or causes to be accessed any computer, computer system, or computer network; (b) Disrupts or denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another; (c) Destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; (d) Destroys, injures, or damages any computer, computer system, or computer network; or (e) Introduces any computer contaminant into any computer, computer system, or computer network, commits an offense against computer users.

(2) (a) Except as provided in paragraphs (b) and (c), whoever violates subsection (1) commits a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084. (b) Whoever violates subsection (1) and: 1. Damages a computer, computer equipment, computer supplies, a computer system, or a computer network, and the monetary damage or loss incurred as a result of the violation is $5,000 or greater; 2. Commits the offense for the purpose of devising or executing any scheme or artifice to defraud or obtain property; or 3. Interrupts or impairs a governmental operation or public communication, transportation, or supply of water, gas, or other public service, commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084. (c) Whoever violates subsection (1) and the violation endangers human life commits a felony of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(3) Whoever willingly, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network commits a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.

(4) (a) In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, computer equipment, computer supplies, or computer data may bring a civil action against any person convicted under this section for compensatory damages. (b) In any action brought under this subsection, the court may award reasonable attorney fees to the prevailing party.

(5) Any computer, computer system, computer network, computer software, or computer data owned by a defendant which is used during the commission of any violation of this section or any computer owned by the defendant which is used as a repository for the storage of software or data obtained in violation of this section is subject to forfeiture as provided under ss. 932.701 – 932.704.

(6) This section does not apply to any person who accesses his or her employer's computer system, computer network, computer program, or computer data when acting within the scope of his or her lawful employment.

(7) For purposes of bringing a civil or criminal action under this section, a person who causes, by any means, the access to a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in both jurisdictions.

(History: s. 1, ch. 78-92; s. 11, ch. 2001-54.)

815.07 This chapter not exclusive. The provisions of this chapter shall not be construed to preclude the applicability of any other provision of the criminal law of this state which presently applies or may in the future apply to any transaction which violates this chapter, unless such provision is inconsistent with the terms of this chapter. (History: s. 1, ch. 78-92.)

SECTION 7213 – UNAUTHORIZED DISCLOSURE OF INFORMATION

(a) RETURNS AND RETURN INFORMATION -

(1) FEDERAL EMPLOYEES AND OTHER PERSONS – It shall be unlawful for any officer or employee of the United States or any person described in section 6103(n)(or an officer or employee of any such person),or any former officer or employee, willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)]. Any violation of this paragraph shall be a felony punishable upon conviction by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the costs of prosecution, and if such offense is committed by any officer or employee of the United States, he shall, in addition to any other punishment, be dismissed from office or discharged from employment upon conviction for such offense.

(2) STATE AND OTHER EMPLOYEES – It shall be unlawful for any person [not described in paragraph (1)] willfully to disclose to any person, except as authorized in this title, any return or return information [as defined in section 6103(b)] acquired by him or another person under subsection (d),(i)(3)(B)(i),(1)(6),(7),(8),(9),(10),(12),(15) or (16) or (m)(2),(4),(5),(6), or (7) of section 6103. Any violation of this paragraph shall be a felony punishable by a fine in any amount not exceeding $5,000, or imprisonment of not more than 5 years, or both, together with the cost of prosecution.

(3) OTHER PERSONS – It shall be unlawful for any person to whom any return or return information [as defined in section