



SECURITY AGREEMENT FORM

The Department of Children and Families has authorized you:

Employee's Name/Organization

to have access to sensitive data through the use of 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 and, in addition to departmental discipline, the commission of computer crimes may result in Federal and/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 and 50-6
- It is the policy of the Department of Children and Families that no contract employee shall be allowed access to IRS tax information or FDLE information, unless such contract employee is formally 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 is that personal passwords are not to be disclosed.
- It is the policy of the Department of Children and Families that information is not to be obtained for my own or another person's personal use.
- I will only access or view information or data that I am authorized, and have a legitimate business reason in the course of the performance of my duties. I shall maintain the integrity of all confidential and sensitive information accessed.
- The "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, is not acceptable, and will not be tolerated.
- It is the policy of the Department of Children and Families that database queries will be performed on a regular basis to identify misuse of access.

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

Print Employee Name

Signature of Employee

Date

Print Supervisor Name

Signature of Supervisor

Date

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 6103(b)] is disclosed in a manner unauthorized by this title thereafter willfully to print or publish in any manner not provided by law any such return or return information. 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.

(4) **SOLICITATION** – It shall be unlawful for any person willfully to offer any item of material value in exchange for any return or return information [as defined in 6103(b)] and to receive as a result of such solicitation any such return or return information. 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.

(5) **SHAREHOLDERS** – It shall be unlawful for any person to whom return or return information [as defined in 6103(b)] is disclosed pursuant to the provisions of 6103(e)(1)(D)(iii) willfully to disclose such return or return information in any manner not provided by law. 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.

SECTION 7213A – UNAUTHORIZED INSPECTION OF RETURNS OR RETURN INFORMATION

(a) PROHIBITIONS –

(1) **FEDERAL EMPLOYEES AND OTHER PERSONS** – It shall be unlawful for-

(A) any officer or employee of the United States, or

(B) any person described in section 6103(n) or an officer willfully to inspect, except as authorized in this title, any return or return information.

(2) **STATE AND OTHER EMPLOYEES** – It shall be unlawful for any person [not described in paragraph (1)] willfully to inspect, except as authorized by this title, any return information acquired by such person or another person under a provision of section 6103 referred to in section 7213(a)(2).

(b) PENALTY –

(1) **IN GENERAL** – Any violation of subsection (a) shall be punishable upon conviction by a fine in any amount not exceeding \$1000, or imprisonment of not more than 1 year, or both, together with the costs of prosecution.

(2) **FEDERAL OFFICERS OR EMPLOYEES** – An officer or employee of the United States who is convicted of any violation of subsection (a) shall, in addition to any other punishment, be dismissed from office or discharged from employment.

(c) **DEFINITIONS** – For purposes of this section, the terms "inspect", "return", and "return information" have respective meanings given such terms by section 6103(b).

SECTION 7431 – CIVIL DAMAGES FOR UNAUTHORIZED DISCLOSURE OF RETURNS AND RETURN INFORMATION

(a) IN GENERAL –

(1) **INSPECTION OR DISCLOSURE BY EMPLOYEE OF UNITED STATES** – If any officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against the United States in a district court of the United States.

(2) **INSPECTION OR DISCLOSURE BY A PERSON WHO IS NOT AN EMPLOYEE OF THE UNITED STATES** – If any person who is not an officer or employee of the United States knowingly, or by reason of negligence, inspects or discloses any return or return information with respect to a taxpayer in violation of any provision of section 6103, such taxpayer may bring a civil action for damages against such person in a district court of the United States.

(b) **EXCEPTIONS** – No liability shall arise under this section with respect to any inspection or disclosure -

(1) which results from good faith, but erroneous, interpretation of section 6103, or

(2) which is requested by the taxpayer.

(c) **DAMAGES** – In any action brought under subsection (a), upon a finding of liability on the part of the defendant, the defendant shall be liable to the plaintiff in an amount equal to the sum of-

(1) the greater of –

(A) \$1,000 for each act of unauthorized inspection or disclosure of a return or return information with respect to which such defendant is found liable, or

(B) the sum of:

(i) the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure, plus

(ii) in the case of a willful inspection or disclosure or an inspection or disclosure which is the result of gross negligence, punitive damages, plus

(2) the cost of the action.

(d) **PERIOD FOR BRINGING ACTION** – Notwithstanding any other provision of law, an action to enforce any liability created under this section may be brought, without regard to the amount in controversy, at any time within 2 years after the date of discovery by the plaintiff of the unauthorized inspection or disclosure.

SECTION 6103 – CONFIDENTIALITY AND DISCLOSURE OF RETURNS AND RETURN INFORMATION

(I) DISCLOSURE OF RETURNS AND RETURN INFORMATION FOR PURPOSES OTHER THAN TAX ADMINISTRATION

(7) Disclosure of return information to Federal, State, and local agencies administering certain programs under the Social Security Act, the Food Stamp Act of 1977, or title 38, United States Code, or certain housing assistance programs

(A) **Return information from Social Security Administration** – The Commissioner of Social Security shall, upon written request, disclose return information from returns with respect to net earnings from self-employment (as defined in section 1402), wages (as defined in section 3121 (a) or 3401 (a)), and payments of retirement income, which have been disclosed to the Social Security Administration as provided by paragraph (1) or (5) of this subsection, to any Federal, State, or local agency administering a program listed in subparagraph (D).

(B) **Return information from Internal Revenue Service** – The Secretary shall, upon written request, disclose current return information from returns with respect to unearned income from the Internal Revenue Service files to any Federal, State, or local agency administering a program listed in subparagraph (D).

(C) **Restriction on disclosure** – The Commissioner of Social Security and the Secretary shall disclose return information under subparagraphs (A) and (B) only for purposes of, and to the extent necessary in, determining eligibility for, or the correct amount of, benefits under a program listed in subparagraph (D).

(D) **Programs to which rule applies** – The programs to which this paragraph applies are:

(i) a State program funded under part A of title IV of the Social Security Act;

(ii) medical assistance provided under a State plan approved under title XIX of the Social Security Act or subsidies provided under section 1860D–14 of such Act;

(iii) supplemental security income benefits provided under title XVI of the Social Security Act, and federally administered supplementary payments of the type described in section 1616(a) of such Act (including payments pursuant to an agreement entered into under section 212(a) of Public Law 93–66);

(iv) any benefits provided under a State plan approved under title I, X, XIV, or XVI of the Social Security Act (as those titles apply to Puerto Rico, Guam, and the Virgin islands);

(v) unemployment compensation provided under a State law described in section 3304 of this title;

(vi) assistance provided under the Food Stamp Act of 1977;

(vii) State-administered supplementary payments of the type described in section 1616(a) of the Social Security Act (including payments pursuant to an agreement entered into under section 212(a) of Public Law 93–66);

(viii)

(I) any needs-based pension provided under chapter 15 of title 38, United States Code, or under any other law administered by the Secretary of Veterans Affairs;

(II) parents' dependency and indemnity compensation provided under section 1315 of title 38, United States Code;

(III) health-care services furnished under section 1710(a)(1)(I), 1710(a)(2), 1710(b), and 1712(a)(2)(B) of such title; and

(IV) compensation paid under chapter 11 of title 38, United States Code, at the 100 percent rate based solely on unemployability and without regard to the fact that the disability or disabilities are not rated as 100 percent disabling under the rating schedule; and

(ix) any housing assistance program administered by the Department of Housing and Urban Development that involves initial and periodic review of an applicant's or participant's income, except that return information may be disclosed under this clause only on written request by the Secretary of Housing and Urban Development and only for use by officers and employees of the Department of Housing and Urban Development with respect to applicants for and participants in such programs.

Only return information from returns with respect to net earnings from self-employment and wages may be disclosed under this paragraph for use with respect to any program described in clause (viii)(IV). Clause (viii) shall not apply after September 30, 2008.