

FLORIDA CROWN WORKFORCE BOARD, INC. POLICY

POLICY TITLE: Procedure for Reporting Breach of Security and Fraudulent Actions

POLICY NUMBER: ADM-011-08 DATE EFFECTIVE: March 13, 2008

DATE REVISED: July 20, 2010

APPLICATION

Florida Crown Workforce Board, Inc. (FCWB) Employees and Board of Directors, AWI Employees, and Service Provider Employees.

PURPOSE

This policy outlines the process in which personnel shall respond and report instances of security breaches, fraudulent practices and crimes, and provides guidance for staff members pursuant to 817.5681, Florida Statutes and Chapter 443 Florida Statutes.

POLICY

It is the policy of FCWB that in all instances where an employee suspects fraudulent practices, crime, and/or a breach of security concerning confidential personal information in third-party possession (personal information is defined in section 817.5681(5), Florida Statutes, as "an individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements when the data elements are not encrypted such as (a) social security number, (b) driver's license number or Florida Identification Card number, (c) account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account"), the following procedures must be followed:

Fraudulent Practices, Crime, and/or a Breach of Security:

1. Any employee who maintains computerized data in a system that includes personal information shall provide notice of any breach of the security of the system, following a determination of the breach, to their immediate supervisor, Project Manager, and FCWB management staff as well as to the individual and/or business entity of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notification shall be made without unreasonable delay, consistent with the legitimate needs of law

enforcement, or subject to any measures necessary to determine the presence, nature, and scope of the breach and restore the reasonable integrity of the system. Notification must be made no later than 45 days following the determination of the breach unless otherwise provided in this section.

2. The notification required by this section may be delayed upon a request by law enforcement if a law enforcement agency determines that the notification will impede a criminal investigation. The notification time period required by this section shall commence after the person receives notice from the law enforcement agency that the notification will not compromise the investigation.
3. For purposes of this section, the terms "breach" and "breach of the security of the system" mean unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person. Good faith acquisition of personal information by an employee or agent of the person is not a breach or breach of the security of the system, provided the information is not used for a purpose unrelated to the business or subject to further unauthorized use.
4. For purposes of this section, the term "personal information" means an individual's first name, first initial and last name, or any middle name and last name, in combination with any one or more of the following data elements when the data elements are not encrypted:
 - (a) Social security number.
 - (b) Driver's license number or Florida Identification Card number.
 - (c) Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
5. For purposes of this section, the term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.
6. For purposes of this section, notice may be provided by one of the following methods:
 - (a) Written notice;
 - (b) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. s. 7001 or if the person or business providing the notice has a valid e-mail address for the subject

person and the subject person has agreed to accept communications electronically; or

(c) Substitute notice, if the person demonstrates that the cost of providing notice would exceed \$250,000, the affected class of subject persons to be notified exceeds 500,000, or the person does not have sufficient contact information. Substitute notice shall consist of all of the following:

(1) Electronic mail or e-mail notice when the person has an electronic mail or e-mail address for the subject persons.

(2) Conspicuous posting of the notice on the web page of the person, if the person maintains a web page.

(3) Notification to major statewide media.

7. For purposes of this section, the term "unauthorized person" means any person who does not have permission from, or a password issued by, the person who stores the computerized data to acquire such data, but does not include any individual to whom the personal information pertains.
8. For purposes of this section, the term "person" means an individual or business entity. For purposes of this section, the State of Florida, as well as any of its agencies or political subdivisions, and any of the agencies of its political subdivisions constitutes a person.
9. The Department of Legal Affairs may institute proceedings to assess and collect the fines provided in this section.
10. If a person discovers circumstances requiring notification pursuant to this section of more than 1,000 persons at a single time, the person shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. s. 1681a(p), of the timing, distribution, and content of the notices.

Unemployment Insurance Confidentiality:

Pursuant to Florida's Unemployment Compensation Law (Chapter 443 Florida Statutes) Sections 443.171 (5) and 443.1715, F.S., it is prohibited to disclose unemployment insurance (UI) information except as authorized by law. The minimum security requirements are:

1. UI information is to be used only in an official capacity for valid administrative purposes;
2. UI information will not be disclosed except in accordance with the provision of ss. 443.171(5) and 443.1715, F.S. and Title 20 Part 603, Code of Federal Regulations.
3. The use of UI information is limited to only purposes authorized by law.
4. UI information will be stored in a place physically secure from access by unauthorized persons.
5. UI information stored and processed in electronic format, such as magnetic tapes or discs, will be maintained in such a way that unauthorized persons cannot retrieve the information by any means.
6. Precautions will be taken to ensure that only authorized individuals can access UI information stored in computer systems.
7. UI information and any copies that are not longer needed in the performance of official duties shall be disposed of in such a way that the data cannot be reconstructed, accessed or obtained by unauthorized means.
8. Individuals who violate the confidentiality provisions set forth in ss. 443.171(5) and 443.1715, F.S, commit a misdemeanor of the second degree, punishable as provided in s. 775.082 or 775.083, F.S.
9. An individual who makes a false representation in order to obtain a social security number is in violation of s. 119.0721 F.S. and commits a felony of the third degree, punishable as provided in s. 775.082 or 775.083, F.S.
10. Passwords authorizing access to UI information are not to be divulged to any other individual.

Computer Crimes:

Computer crimes are a violation of disciplinary standards and the commission of computer crimes may result in felony criminal charges. The Florida Computer Crimes Act, Chapter 815, Florida Statutes, addresses the unauthorized modification, destruction, disclosure or taking of information resources. The minimum security requirements are:

1. Personal passwords are not to be disclosed.

2. Information may not be obtained for personal use by an employee or other person's personal use.
3. Computer crimes such as the unauthorized modification, destruction and disclosure of computer data or computer systems are a violation of the Computer Crimes Act, Chapter 815. F.S. and the commission of computer crimes may result in felony criminal charges.

Whenever you change offices, change work locations, or leave FCWB, you do NOT, under ANY circumstances, have a right to delete or otherwise remove data from a FCWB computer. The IT staff reviews every computer after a change in staffing, and we know when something inappropriate has been done. Believe me when I tell you, it will be discovered, and appropriate actions will be taken.

ACTION:

FCWB Employees and Board of Directors, AWI Employees, and Service Provider Employees when suspecting security breaches, fraudulent practices and crimes will adhere to this policy.

Approved: *John Chastain*
John Chastain, Executive Director