

# FLORIDA CROWN WORKFORCE BOARD, INC. POLICY

**POLICY TITLE: Computer Use Policies**

**POLICY NUMBER: ADM-003-02**

**DATE EFFECTIVE: July 1, 2002**

**DATE REVISED: July 27, 2010**

---

## **APPLICATION**

Florida Crown Workforce Board, Inc. (FCWB) employee, contractor, provider and other users who accesses FCWB's network.

## **PURPOSE**

The purpose of this procedure is to delineate acceptable uses of computers, e-mail and the Internet/Intranet by employees and other authorized users of the FCWB Network Services and supersedes all past practices and policies related to topics defined below.

## **AUTHORITY**

Sections 119, 282.318, 282.3055 and 282.75, F.S.

## **EFFECTIVE DATE**

Upon issuance.

**Scope:** This is a list of general and specific computer use policies and security rules that apply to all users of FCWB computers or networks. Site supervisors/managers are responsible for implementing these policies and procedures in their organization and ensuring that users fulfill their responsibilities. **FCWB is to be provided a signed copy of this form to have a record on file for every user.**

## **Computer Usage**

Computers, software, and communications systems are provided by and property of FCWB and are intended for work-related activities. Use for non work-related functions while not specifically prohibited should be kept to a minimum and only during non-work time. Users are advised that ***all data files*** located on computers are public record and subject to inspection – **and shall not be removed from the system without review of the IT Department.**

## **Sensitive Processing and Data Protection**

Confidential (or sensitive) information is that information which is confidential by law, including information, which requires protection from unauthorized access by virtue of its legal exemption from the Public Records Act, Section 119, Florida Statutes. Information about persons who receive services may not be disclosed publicly in such a manner as

to identify such person, unless the person or their legal guardian provides written consent.

### **Data Retention**

When a user account is deleted, all permanent files (located on personal computer hard disks and located on file servers) are to be reviewed by the location supervisor **and IT Staff**. Data that is subject to the guidelines of Chapter 1B-26, F.A.C., 119, F.S., 257, F.S., shall be retained as public record all other data may be deleted.

### **Usernames and Passwords**

A user identifier known as a username and password are required of all users. Passwords must be at least six (6) characters long, not found in a dictionary, and should have at least two alphabetic and at least one numeric or special character. Passwords must be confidential. **Passwords will be set in user profiles for mandatory reset after 42 days**. The password must be changed as soon as possible after an unacceptable exposure or suspected compromise. Impersonating another user or other person to gain access to network systems is unauthorized. The sharing of a User ID and password is prohibited. Violations will be subject to disciplinary actions, **up to and including termination**.

### **Altering Authorized Access**

Users are prohibited from changing or circumventing access controls to allow themselves or others to perform actions outside their authorized privileges. **Violations will be subject to disciplinary actions, up to and including termination**.

### **Data Modification or Destruction**

Users are prohibited from taking unauthorized actions to intentionally modify or delete Information or programs. **Violations will be subject to disciplinary actions, up to and including termination**.

### **Software Use**

All software used on FCWB computers must be appropriately acquired and used according to the appropriate licensing. Possession or use of illegally copied software is prohibited. Likewise, users shall not copy copyrighted software, except as permitted by the owner of the copyright or licensing agreement. To prevent network problems which may be caused by certain types of software, the user will not install any software including but not limited to the following;

- a) Screensavers
- b) Games
- c) Utilities
- d) Applications-i.e., Instant messengers, Online weather, Music players, Browser toolbars, E-mail animations, etc.

Unauthorized software is any software **not** installed by the MIS Department.

Disciplinary action for unauthorized software is described on Page 7 of this Policy.

Note: If any software deemed by the user as necessary to perform daily job duties outside the scope of the FCWB installed software standard, a written request must be submitted, via e-mail, to the MIS Department by the appropriate supervisor. The MIS Department will then research and evaluate software, and if necessary, purchase software and appropriate licenses. Authorization for purchase will be reviewed and approved/declined by the MIS Director based upon recommendation from Executive Director for the Workforce Board.

### **Malicious Software**

Users must not introduce or use malicious software such as computer viruses, Trojan horses, or worms.

### **How viruses can infect Florida Crown's network**

There are actually three various types of computer viruses: true viruses, Trojan horses, and worms. True viruses actually hide themselves, often as macros, within other files, such as spreadsheets or Word documents. [*Note: Viruses can actually hide themselves in a variety of mediums: applications, boot sectors, partition sectors, and so forth.*] When an infected file is opened from a computer connected to Florida Crown's network, the virus can spread throughout the network and may do damage. A Trojan horse is an actual program file that, once executed, doesn't spread but can damage the computer on which the file was run. A worm is also a program file that, when executed, can both spread throughout a network and do damage to the computer from which it was run. Viruses can enter Florida Crown's network in a variety of ways:

- **E-mail** - By far, most viruses are **sent embedded in e-mail and email attachments**. These attachments could be working documents or spreadsheets, or they could be merely viruses disguised as pictures, jokes, etc. These attachments may have been knowingly sent by someone wanting to infect Florida Crown's network or by someone who does not know the attachment contains a virus. However, once some viruses are opened, they automatically e-mail themselves, and the sender may not know his or her computer is infected.
- **Disk, CD, Zip disk, USB drive, external hard disk or other media** - Viruses can also spread via various types of storage media. As with e-mail attachments, the virus could hide within a legitimate document or spreadsheet or simply be disguised as another type of file. All external storage media devices *MUST* be scanned by the anti-virus software before trying to access files stored on them.
- **Software downloaded from the Internet** - Downloading software via the Internet can also be a source of infection. As with other types of transmissions, the virus could hide within a legitimate document, spreadsheet, or other type of file. Seek direction from you IT department prior to downloading software from the Internet.
- **Instant messaging attachments** - Although less common than e-mail attachments, more viruses are taking advantage of instant messaging software. These attachments work the same as e-mail viruses, but they are transmitted via instant messaging software.

## **How Florida Crown's IT department prevents and minimizes virus infections**

Florida Crown's IT department fights viruses in several ways:

- 1. Scanning Internet traffic**— All Internet traffic coming to and going from our network must pass through company servers and other network devices. For example, an e-mail message that originates outside of the network must pass through the **Untangle Server, Cisco Pix/ASA Firewall, Cisco 3600 router, the X-Wall Server**, and finally the Exchange 2008 AVG anti-virus software before it is allowed to enter the e-mail server. The use of multiple layers of protection helps to minimize the risk of infection. Untangle also helps to fight Spy Ware, Phishing as well as defending the network from various unsecure protocols and files types.
- 2. Running server and workstation antivirus software**— **All servers and workstations run VIPRE anti-virus/anti-malware software.** This software scans our file-sharing data stores, looking for suspicious codes. This software scans all data written to or read from a workstation's hard drive. If it finds something suspicious, it isolates the dubious file on the computer and automatically notifies the help desk.
- 3. Routinely updating virus definitions**— Every morning, the firewall and server virus scanning programs check for updated virus definitions. These definition files allow the software to detect new viruses. If a new virus definition file is available, the virus scanning software is automatically updated, and then the system administrator is informed. When end users turn on their computers at the beginning of the workday, the workstation virus protection program checks with Florida Crown's server on the network for updates. The workstation program will then download and install the update automatically, if one exists.

## **How to respond to and report a virus**

Even though all Internet traffic is scanned for viruses and all files on the company's servers are scanned, the possibility still exists that a new or well-hidden virus could find its way to an employee's workstation, and if not properly handled, it could infect Florida Crown's network.

The IT staff will attempt to notify all users of credible virus threats via e-mail or telephone messages. Because this notification will automatically go to everyone in the organization, employees should not forward virus warning messages. On occasion, well-meaning people will distribute virus warnings that are actually virus hoaxes. These warnings are typically harmless; however, forwarding such messages unnecessarily increases network traffic. It is the responsibility of all Florida Crown's network users to

take reasonable steps to prevent virus outbreaks. Use the guidelines below to do your part:

- *Do not open unexpected e-mail attachments, even from co-workers.*
- *Never open an e-mail or instant messaging attachment from an unknown or suspicious source.*
- *Never open e-mail files with multiple extensions (e.g. text.zip.exe)*
- *Never download freeware or shareware from the Internet without express permission of the IT department.*
- *If a file you receive contains macros that you are unsure about, disable the macros.*

### **Notify the IT Department of suspicious files**

If you receive a suspicious file or e-mail attachment, DO NOT OPEN IT!! Submit an IT Support ticket to inform the IT Dept. that you have received a suspicious file. The IT Department will assist in determining the validity of or destroying that file. If the potentially infected file is on a disk that you have inserted into your computer, scan the disk with the anti-virus software installed on your workstation, format the disk, or eject the disk. Eject the disk and contact the IT Department at (386) 755-9026. They will instruct you on how to handle the disk.

After the IT Department has neutralized the file, send a note to the person who sent/gave you the file notifying them that they sent/gave you a virus. If the file is an infected spreadsheet or document that is of critical importance to Florida Crown, the IT department will attempt to scan and clean the file. The IT department, however, makes no guarantees as to whether any infected file can be totally cleaned and will not allow the infected file to be used on Florida Crown's computers.

### **Internet Usage**

**Purpose:** Internet access is provided as a business tool for reasons that are necessary for the accomplishment of an employee's job assignments. As is the case with other technology resources, Internet access services are shared among the entire Florida Crown Workforce Board staff and its partners. Everyone using Internet services should be considerate of the needs of others, and be certain that nothing is done to impede anyone else's ability to use this service.

A web-content filter has been installed to filter and report inappropriate internet use. Attempts to bypass the web-content filter are logged and violators will be subject to disciplinary action.

Internet usage is routinely monitored by the MIS Department.

## Procedures:

- Files downloaded from the Internet must be thoroughly scanned by anti-viral software maintained by the MIS Department. This anti-viral software is not to be disabled by the user.
- In accordance with departmental policy, executable files/software can only be downloaded by individuals whose job descriptions include the testing of software.
- Accessing, sending, storing, or displaying sensitive materials including, but not limited to, gambling or other illegal activities, sexually explicit materials, or materials that include profane, obscene, hate filled, racial or discriminatory content is prohibited and will result in the revocation of internet privileges. If you wouldn't want your children to see it, don't view it here.
- Data and files on the Internet must be considered copyrighted material and may not be distributed or published in any form without the written permission of the originator.
- In addition to work-related access, employees may briefly visit non-sensitive Internet sites during **non-working time**, such as break, lunch, or before or after work hours. Examples of acceptable sites are those dealing with health matters, on-line banking, weather, news, business topics, community activities, career advancement, and personal enrichment. It is imperative that common sense be used in viewing non-work related sites and they must not result in any additional cost to the Department or violate procedures defined below.

## Prohibited use of the Internet includes:

- Use for private or personal business such as cell phone home business.
- Use based on for-profit activities (sales, consulting for pay, etc., and specifically running an eBay business).
- Use involving illegal schemes or activities.
- To browse, create, display, transmit or make accessible threatening, racist, sexist (including nudity and pornographic content), obscene, offensive, annoying or harassing language and/or material.
- Sites containing nudity or pornographic material.
- Sites containing ethnic or racially offensive material.
- Sites depicting hate or hate crimes.
- Sites containing images of torture, death or disfigurement or violence of any type.
- Sites that are beyond what is generally considered morally acceptable and within the boundaries of good taste.
- Use of Chat rooms.
- Use of Instant Messenger (IM) services such as AOL Chat, Yahoo Messenger, MSN Messenger, Facebook Chat, etc.
- Use for dating and relationships.
- Use for retail shopping and or/purchases.
- Any use which adversely impacts the network communications of FCWB by overloading the network. Examples are playing streaming audio (music) via on-line radio stations, viewing streaming video (live news casts).

Note: Other categories may be added at the discretion of the Workforce Board.

## **FCWB E-mail Usage**

**Purpose:** E-mail is to be used for official business, which includes communications with customers, other workforce boards, state departments, governmental entities and private sector entities. Although FCWB does not prohibit all personal use of e-mail, a common sense approach should be applied.

Acceptable personal use of e-mail is where the communication is brief, does not interfere with work, does not subject the FCWB to any additional cost, and is consistent with the requirements contained in this policy.

**Confidentiality Notice:** The following notice is to appear on all e-mail communications:

“This message and any attachments are for the sole use of the intended recipient(s) and may contain confidential and privileged information that is exempt from public disclosure. Any unauthorized review, use, disclosure, or distribution is prohibited. If you have received this message in error please contact the sender (by phone or reply electronic mail) and then destroy all copies of the original message.”

### **Prohibited use of e-mail includes:**

- Non-board sponsored solicitations, including, but not limited to such things as advertising the sale of property or other commercial activities.
- Sending copies of documents in violation of copyright laws or licensing agreements.
- Sending messages prohibited or restricted by government security laws or regulations or any other communication that may adversely affect the Workforce Board's ability to carry out its mission.
- Sending messages which may reflect unfavorably on FCWB, or which may be perceived as representing the Workforce Board's official position on any matter when authority to disseminate such information has not been expressly granted are also prohibited.
- Sending confidential information or data to persons not authorized to receive it, either within or outside FCWB.
- Sending content that may constitute sexual harassment or be considered discriminatory, obscene, derogatory or excessively personal, whether intended to be serious or humorous.
- Sending communications reflecting or containing chain letters; illegal activity; harassment; sensitive information including but not limited to gambling, or materials that include profane, obscene, or inappropriate language, or racial, ethnic or other discriminatory content.
- Sending communications reflecting negatively on another employee.

FCWB reserves the right to routinely monitor the contents of e-mail messages. Users should expect that electronic mail messages may be accessed when duly authorized by the MIS Director without the permission of the employee.

Any requests for access to the contents of e-mail in order to respond to legal process, such as subpoenas and public records law requests, or for purposes involving litigation, investigation or claim must be immediately brought to the attention of the MIS Department for the Workforce Board.

Individual users are advised that all e-mails transmitted or received are public record and are archived for retention as required by Florida State laws.

**Disciplinary Actions to be taken for Violations**

If inappropriate usage of the Workforce Board's network, e-mail or the Internet is suspected, the MIS Department reserves the right to audit and/or monitor any user's activity. Failure to comply with aforementioned rules may result in the following disciplinary actions:

- 1) **First Offense:** User access will be suspended and the Partner/Immediate Supervisor will need to contact the Service Provider/Partner Executive manager at the corporate office. In turn, the Executive manager will have to call the Workforce Board MIS Department to re-activate user account. Also, the MIS Department will request that a written warning be placed in user's personnel file along with a copy sent to FCWB MIS Department.
- 2) **Second Offense:** User access will again be suspended and the Partner/immediate Supervisor will need to contact the Service Provider/Partner Executive manager at the corporate office. In turn, the Executive manager will have to submit a written request to the Workforce Board MIS Department to re-activate user account. The written request needs to describe the actions that will be taken to prevent user from violating these policies in the future. User reinstatement will have to be approved by the Workforce Board's MIS Director.
- 3) **Third Offense:** User access will again be suspended. Service Provider/Partner Executive manager will have to contact the FCWB MIS Director to set up a meeting to reinstate user and determine appropriate course of disciplinary action. FCWB MIS Director will then make recommendations to FCWB Executive Director. User access will not be reinstated without approval from FCWB Executive Director.

**Note:** With regards to user's negligence, it can be a very time consuming task to return a system to working order. The Workforce Board reserves the right to recover actual costs from the Service Provider/Partner for the MIS Department to return the FCWB network, e-mail, equipment loss/theft, or Internet to its normal operating state. During the repair process any and all files stored on the system are in danger of being damaged or deleted and no guarantees are made that this will not happen. In some instances a computer may need to be re-imaged. This will result in a loss of ALL data on this system.

I hereby acknowledge that I am being permitted by the Florida Crown Workforce Board (hereafter, FCWB) to use only software authorized and installed by the MIS Department

that is listed below. Also, I acknowledge that I have read the terms outlined in this "Computer Use Policies" form and understand that any use which I make of the Standard Software listed below will be made solely under such terms and conditions. I further agree that I will not install any other software on my workstation or on any other workstation connected to the FCWB network.

**Florida Crown Workforce Board Authorized Software Description**

- 1) Any software installed and evaluated by FCWB MIS Department
- 2) Operating System: *Windows XP, Vista, 7, and Linux*
- 3) Microsoft Office Suite: *Includes Office 2003 or 2007 (includes Word, Excel, PowerPoint, Outlook, Access (optional), Publisher (optional) and FrontPage (optional))*
- 4) Attachmate: *Extra! For SNA Server (State of Florida sessions) (where required)*
- 5) Internet Explorer, Mozilla Fire Fox, Apple Safari, Google Chrome
- 6) *Sunbelt VIPRE*
- 7) Adobe: *Acrobat Reader*
- 8) *VNC Viewer*
- 9) *SpyBot S&D*

**ACTION**

All FCWB employees, contractors and providers will adhere to this policy.

Approved: *John Chastain*  
John Chastain, Executive Director