Big Bend Community Based Care
Policy & Procedure

Series:	900: Data Collection, Records and Reporting	
Policy Name:	Use of Information System Resources	
Policy Number:	912	
Origination Date:	03/09/2009	**Revised:** Board Meeting of 12/13/2018

Policy

It is the policy of Big Bend Community Based Care, Inc. (BBCBC), to establish a standard for the acceptable use of computer resources for its employees and Case Management Organizations (CMOs).

Procedure

A. General Requirements.

1. This policy applies to all employees, contractors, consultants, temporary staff, and other workers at BBCBC and CMOs and pertains to all information resources that are owned or leased by BBCBC.

2. BBCBC reserves the right to audit networks and systems on a periodic basis to ensure compliance.

3. Users accessing the Internet are representing BBCBC.

a. All communications should be for professional reasons.

b. Users are responsible for seeing that the Internet is used in an effective, ethical and lawful manner.

c. Databases may be accessed for information as needed.

d. E-mail may be used for business contacts.

4. The installation of any personally owned electronic devices (i.e., PDAs, external storage media) is prohibited.

B. Security and Proprietary Information.

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies.

a. Examples of confidential information include, but are not limited to: company private or identifying client information.

b. Employees should take all necessary steps to prevent unauthorized access to this information.

2. Users need to keep passwords secure and not share accounts.

a. Authorized users are responsible for the security of their passwords and accounts.

b. System level and user level passwords should be changed quarterly.

3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at fifteen (15) minutes or less, or by logging off (control + alt + delete) when the host will be unattended.

4. All portable computers will be encrypted and equipped with tracking software.
5. Postings by employees from BBCBC email address to newsgroups is not permitted, unless posting is in the course of business duties.
6. All hosts used by the employee that are connected to the BBCBC Internet/Intranet/Extranet shall be continually executing approved virus-scanning software with a current virus database.
7. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

C. Unacceptable Use.

1. Under no circumstances is an employee of BBCBC authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing BBCBC-owned resources.
2. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.
   - **a.** Attempting to gain access or accessing another user's system files or messages.
   - **b.** Solicitation of non-BBCBC business, or any use of the Internet for personal gain
   - **c.** Internet use that results in disrupting the operation of the BBCBC network or the network(s) of other users (e.g., streaming video and/or audio).
   - **d.** Internet use for personal gain or advancement of individual views.
   - **e.** Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by BBCBC.
   - **f.** Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which BBCBC does not have an active license is strictly prohibited.
   - **g.** Unauthorized downloading of any software. All software downloads require prior approval of the Director of Information Services or his designee.
   - **h.** Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
   - **i.** Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
   - **j.** Using a BBCBC computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
   - **k.** Making fraudulent offers of products, items, or services originating from any BBCBC account.
   - **l.** Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
   - **m.** Effecting security breaches or disruptions of network communication.
     - **i.** Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not

expressly authorized to access, unless these duties are within the scope of regular duties.

ii. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

n. Port scanning or security scanning is expressly prohibited unless prior notification to BBCBC is made.

o. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

p. Circumventing user authentication or security of any host, network or account.

q. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

r. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

s. "Surfing" pornographic, gaming, warez, or any other web sites of a questionable nature is expressly prohibited.

D. Email and Communications Activities. The following activities are strictly prohibited:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within BBCBC's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by BBCBC or connected via BBCBC's network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

8. Email signature blocks that contain any information that is not strictly related to the conduct of official agency business

9. The use of email stationary.

E. Enforcement. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.