INTERNET / INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

3.11

Effective Date: 07/18

Purpose: To outline the responsibilities and requirements for employees when using the Internet, working on the BRDHD network, or utilizing and information technology belonging to BRDHD, including but not limited to flash drives, compact discs, or printers.

Failure to Comply: Employees who fail to comply with this policy will be subject to disciplinary procedures and could lose network privileges. Agency failure to comply could result in violation of federal, state or local regulations.

Policy: A signed P-19 Information Technology Security Agreement shall be required prior to being granted independent access to electronic media, specifically media that allows access to Electronic Protected Health Information. The security agreement indicates compliance with specified acceptable uses, rules of online behavior, access privileges and penalties for policy or procedural violations. Strict adherence to all standards, "acceptable uses" and "additional employee responsibilities" as stated in the signed security agreement is mandated.

For employee's whose positions require access to the BRDHD network and Intranet, the CDP Bridge system, a local or state email account or the state Intranet, an account with the appropriate permissions will be established. This account can include access to the Internet, electronic mail, the BRDHD Intranet, a directory to share files and a directory for personal files. Access to a BRDHD email account is conditional upon this signed agreement from the staff person that states the staff person's adherence and compliance to the policies and standards of BRDHD which also satisfy the Commonwealth's Office of Technology's (C.O.T.) guidelines.

BRDHD will not be responsible for any damages, including loss of data resulting from delays, nondeliveries, bad deliveries or service interruptions caused by its own negligence, user errors/omissions, and its service providers or for outages or email service interruptions caused by C.O.T. or other service providers.

Supervisors are encouraged to work with employees to determine the suitability of using the Internet and electronic communication for professional activities and career development during working hours while insuring employees do not violate the general provisions that prohibit use of BRDHD Internet for

personal gain or other policies. The employment of BRDHD internet access for personal use during breaks will be determined by the individual supervisor but is still subject to BRDHD policies.

The Internet gives each user unprecedented reach in propagating agency messages. Because of that power, employees must take special care to maintain clarity, consistency and the integrity of the BRDHD image and posture within the community. Monitoring tools are in place to observe employee's use of email, the Intranet and the Internet. **Employees shall have no expectation of privacy associated with email transmissions, Internet usage and the information they publish or store on the Internet or private network directories using the provided facilities.** BRDHD reserves the right to inspect any or all files stored in private areas on the network in order to assure compliance with policy.

Acceptable Uses for Electronic Media Access

1. Use of employee access should be in the support of education, communication, research, be consistent with BRDHD objectives and relate to specific job functions.

2. Employees have an obligation to use their access to the Internet and the various modes of electronic communication provided, i.e.; electronic mail, web blogs/forums/message boards, newsgroups, messaging etc., in a responsible and informed way while conforming to network etiquette, customs, courtesies and any applicable laws or regulations.

3. Professionalism in all electronic communication is of the utmost importance. Please see Best Practice Guidelines below**.**

4. Employees shall represent themselves and Barren River District Health Department accurately and honestly through electronic information and service content.

5. BRDHD retains the copyright to any material posted to any forum, blog, discussion board, newsgroup, email or Internet web-page by an employee in the course of his or her duties.

Unacceptable Uses for Electronic Media Access/ Additional Responsibilities

1. Sexually explicit or other material considered offensive, threatening, illegal or harassing may not be displayed, archived, stored, distributed, edited or recorded using the BRDHD network or computing resources.

2. Use of BRDHD resources for illegal activity is grounds for disciplinary action, including dismissal. BRDHD administration will cooperate with any legitimate law enforcement activity.

3. No employee may use BRDHD facilities to download, store or distribute pirated software and/or data.

4. Employees may not upload software licensed to BRDHD without specific authorization from a network administrator or the manager responsible for software or data.

5. No employee may use BRDHD facilities/resources to propagate any virus or other type of malicious code, to disable/overload any computer system or to circumvent any system intended to protect the privacy or security of another user.

6. Employees with Internet access must take particular care to understand the copyright, trademark, libel, slander and public speech control laws so our use of the Internet and electronic communication does not intentionally or inadvertently violate laws which might be enforceable against the perpetrator or the agency.

7. The use of electronic media; i.e., forums/email/blogs, etc., to promote or oppose any person campaigning for election to a political office, to advocate or oppose religious or political opinions or to promote or advertise a personal or commercial transaction.

8. Non-approved and non-business related activities which are not allowed and will cause congestion and disruption of networks include, but are not limited to: online gaming, unnecessary e-mail subscriptions and attachments, chat rooms, streaming online radio, instant messaging services and any other online services not sanctioned or authorized by a network administrator.

9. Sending or forwarding chain letters. This practice inundates co-workers and others with extraneous email that takes up work time to manage and uses BRDHD network transmission bandwidth that could be used in other, more productive ways.

10. Soliciting money for religious or political causes; advocating or opposing the like.

11. Use of music or file sharing applications such as BitTorrent and similar applications are expressly forbidden because they jeopardize security.

12. Use of vulgar, offensive, threatening, harassing or otherwise objectionable language in either public or private messages or web postings.

13. Misrepresentation of oneself or BRDHD.

14. Monopolizing the resources of the BRDHD network, i.e., storing unnecessary data on the network or sending/forwarding mass emails that are not work-related.

15. User ID's and passwords assist in maintaining individual accountability for Internet and network resource usage. Employees must keep passwords confidential. Sharing passwords is prohibited.

16. Loading of software of any type, downloading software or any shareware/freeware onto the hard drive of your workstation or storing this software on the network will be allowed only per the written authorization of a network administrator.

17. Using portable web browsers, hardware devices or software that inhibits or restricts the recording of all Internet viewing history to the user's host computer is a violation; i.e., the use of privacy or other features in any web browser that inhibits or restricts the recording of all Internet viewing history is not allowed.

18. Mobile equipment, i.e.; laptops, personal data assistants etc, must be locked with a password when not in use and staff members should be cognizant of the whereabouts of mobile equipment when it is taken outside the agency.

19. Staff members are required to protect documents/databases containing EPHI with passwords and store them in a secure area on the network server.

20. All agency laptops must be connected to the BRDHD network overnight to download virus protection and operating system updates **at least one time each week**.

21. Employees must not use non-agency or personal mobile equipment such as multimedia memory cards, laptops, camera/cell phones, personal data assistants, floppy discs or flash drives to store or transfer EPHI without specific written permission from a network administrator. Flash drives and other mobile equipment issued to agency staff will utilize password security; all flash drives and other mobile equipment must be purchased through the BRDHD IS department.

22. All agency computers, specifically mobile computers, must be locked (with software) or logged-off when not in use; user should be cognizant of its location and never leave it in a public place.

23. Any mobile device used by BRDHD staff to access BRDHD email or EPHI must be password protected. Employees utilizing a personal cell phone/PDA/laptop or other mobile device to access a work email account must password protect that device. ***It is not advised to access your work email account using a public device but if you do, you must verify you have logged out of your email account when your session is over.**

24. Flash drives and other removable media or devices (CD's, DVD's with EPHI) must be sent to the BRDHD IS department to be physically destroyed when they no longer function or the data on them is no longer needed.

25. To allow for data transference, EPHI may be put on agency-issued, password-protected or encrypted mobile devices, i.e.; laptops, PDA's, removable flash drives etc., for a maximum of twenty-four (24) hours. **Mobile/removable devices should be used only as a temporary method to store information and data should always be backed up in an alternate location such as a network server share *before* transferring it to a mobile device.**

26. Any breach of electronic security must be reported immediately to your supervisor and a network administrator. Notify a network administrator as soon as possible in the event a piece of mobile equipment has been lost or stolen.

27. Screensavers must be functioning on all agency computers, set to activate if the computer is idle for ten (10) minutes and require a password to unlock it from screensaver mode. This is to be the default setting and may ***not*** be changed by the individual network user.

28. EPHI must not be transmitted via email unless it has been password encrypted. Correspondence containing EPHI must be in a separate email than the password to unlock the data. Password correspondence must be deleted from both the receiver and the originator's email account.

29. An Information systems review, including a system activity audit, of up to five percent (5%) of authorized users on the BRDHD network may take place quarterly. This audit may include, but is not limited to, verifying the individual user's Internet history record, auditing system logs, verifying what files have been recently accessed, identifying any non-authorized programs that may have been installed and verifying network drive access.

30. Mobile equipment issued to staff must be included in the system activity audit and password policy adherence will also be verified during this audit.

31. In order to protect the availability and integrity of data should an individual workstation hard drive crash or become corrupt, all databases or electronic communication containing EPHI, that do not go through CDP, must be backed up on a specific drive share of the network server and not on individual hard drives or removable storage devices except for temporary transference. It is advisable to back up *all* sensitive or critical data on a drive share.

32. Staff members should be aware of what contacts outside of the BRDHD network should be trusted when allowing foreign media to be introduced onto the network, i.e.; downloading email attachments, loading removable discs or flash drives from an outside source.

33. Each user must submit a signed BRDHD P-19 Information Technology Security Agreement Form indicating compliance with this document. A signed P-19 Information Technology Security Agreement Form, which also signals compliance with Commonwealth Office of Technology (C.O.T.) policies and procedures, should be submitted if applicable.

34. Any questions or clarifications of this document should be directed to the HIPAA security officer in writing.

35. Users must observe basic online etiquette in all electronic correspondence or postings and in utilizing network resources by exhibiting the utmost professionalism.

36. Employees should always be vigilant in protecting patient information by not sharing network passwords with anyone (co-workers and supervisors included) and by keeping computer workstations secure from the public and co-workers who do not have the required "need to know" to access specific information.

37. Employees are mandated to change network passwords when prompted to do so by the system. The following parameters must be followed when choosing a network password:

    - Passwords must be a minimum of (8) eight characters.
    - Passwords must contain the following:
        - *At least one upper case character, one lower case character and one number.

Network users are required to change BRDHD network passwords, BRDHD e-mail passwords every thirty (30) days.

Passwords are case sensitive.

The network server will inform staff when it is time to change a user password on an account. The account will automatically be locked out if the password is not changed accordingly.

Network accounts are locked for a minimum of (30) thirty minutes if there are more than three unsuccessful login attempts within a fifteen-minute period.

A network administrator will be required to unlock the account after the system has locked it out.

Best Practice Guidelines for Electronic Communication, i.e.; email/forums etc.
Employees using BRDHD forums and email are expected to treat these "public" areas as they would any other public space. Please remember a forum may be viewed by any number of people and an email, while you think it may be between you and another person, can very easily be shared.

A. Be Respectful of Your Colleagues
Be thoughtful in your comments and cognizant of how your forum post or email could be interpreted. Remember that you are personally and ethically responsible for what you write. Be kind; emails or posts that are considered offensive, threatening, illegal or harassing are not allowed and can't be tolerated.

Don't share information that is not accurate or maliciously share information you know to be secret. Not everyone reading your post or email will feel comfortable sharing thoughts, concerns or ideas if they feel they may be misrepresented.

B. Be Factual
Respect any and all copyright laws. If you choose to share something you know is copyrighted, make sure you credit your source in your post or email. To provide accurate insights, take care to not misrepresent yourself, co-workers or the agency. You should exercise caution in regards to drawing legal conclusions, exaggeration, giving advice, using guesswork, making derogatory remarks or characterizations and using obscenity or other colorful language or humor. ***Any confidential or proprietary agency information is off-limits for posting!***

C. Engage in Respectful Feedback
To maintain an open dialogue make sure you have your facts straight and gracefully accept when someone else may have more knowledge of a topic than yourself.

D. Add Value and Context
Provide support for your argument so your position and reasoning will be understood. Most people value multiple perspectives and providing context to your opinion will help others understand yours. Develop thoughtful arguments whether you are posting/emailing in praise or criticism.

Forms: P-19 Information Technology Security Agreement Form

References: 902 KAR 8:160, Section 4; Policy 2.04 - Tuition Assistance Policy**;** KRS 434.845; KRS 434.850; KRS 434.855

Contact Persons: Human Resources Manager, Director of Information Systems

Procedure Origination, Revision, and Review Tracking

Procedure Version Number	Origination Date	Description of Revision or Reviewer Name
3.11	01.26.2018	HR Manager – Procedure Creation
3.11	10.16.2020	IT Manager-review