Salish Behavioral Health
Administrative Services Organization

Policy Name: WORKSTATION AND PORTABLE COMPUTER USE **Policy Number:** PS908

Effective Date: 1/1/2020

Revision Dates: 1/14/2021

Reviewed Date:

Executive Board Approval Dates: 7/30/2021

PURPOSE

The Salish Behavioral Health Administrative Services Organization (SBH-ASO) uses this and other policies to set limits on the use of email, PCs, cell phones, and telecommunications by employees. The requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 42 CFR Part 2 require that these policies be established, enforced, and audited.

POLICY

SBH-ASO staff must monitor the computer's (desktop, laptop, and/or mobile devices) operating environment and report potential threats to the computer and to the integrity and confidentiality of data contained in the computer system. SBH-ASO staff will take appropriate measures to protect computers and data from loss or destruction.

PROCEDURE

Workstation Use

Officers, agents, employees, contractors, and others using portable/laptop computers (users) must read, understand, and comply with this policy

- Personnel using SBH-ASO computers, needs to secure a safe area for their food and drinks to prevent damage to these devices.
- Any portable equipment and all related components, and data are the property of SBH-ASO and must be safeguarded and be returned upon request and upon termination of a workforce members employment. Staff are responsible for the equipment SBH-ASO issues during employment.
- Personnel logging onto the SBH-ASO network will ensure that no one observes the entry of their password.

- Personnel will neither log onto the system using another's password nor permit another to log on with their password. Nor will personnel enter data under another person's password. Please refer to the SBH-ASO Policy "Password Protection".
- Each person using SBH-ASO computers is responsible for the content of any data he or she inputs into the computer or transmits through or outside the SBH-ASO system. No person may hide his or her identity as the author of the entry or represent that someone else entered the data or sent the message. All personnel will familiarize themselves with and comply with Kitsap County e-mail policy.
- No personnel may access any confidential or other information that they do not have a need to know. No personnel may disclose confidential or other information unless properly authorized (SBH-ASO Confidentiality Use and Disclosure of Protected Health Information Policy).
- Personnel must not leave printers unattended when they are printing confidential information. This rule is especially important when two or more computers share a common printer or when the printer is in an area where unauthorized personnel have access to the printer.
- Personnel using the computer system will not write down their password and place it at or near the terminal.
- Each computer will be programmed to generate a screen saver when the computer receives no input for a specified period.
- Users must at a minimum lock their computer if leaving the computer terminal unattended.
- No personnel may download protected health information (PHI) from SBH-ASO system onto USB, CD, hard drive, fax, scanner, any network drive or any other hardware, software, or paper without the express permission of their manager with written notice to the SBH-ASO Privacy Officer.
- No personnel shall download any software without express written permission of the Kitsap County IS Manager. The Kitsap County IS Manager must approve any software than an employee wishes to download in order to protect against the transmission of computer viruses into the system.

The user agrees to use the equipment solely for SBH-ASO business purposes. The user further understands:

- The user understands that the hardware has been disabled from performing any functions other than those intended for business use and that the user may not attempt to enable such other functions.
- Computers, associated equipment, and software are for business use only, not for the personal use of the user or any other person or entity.
- Users must use only batteries and power cables provided by SBH-ASO and may not, for example, use their car's adaptor power sources.
- Users will not connect any non-SBH-ASO peripherals (keyboards, printers, modems, etc.) without the express authorization of the Kitsap County

Information Services department.

- Users are responsible for securing the unit, all associated equipment, and all data, within their homes, cars, and other locations.
- Users may not leave mobile computer units unattended unless they are in a secured location.
- Users should not leave mobile computer units in cars or car trunks for an extended period in extreme weather (heat or cold) or leave them exposed to direct sunlight.
- Users must place portable computers and associated equipment in their proper carrying cases when transporting them.
- Users must not alter the serial numbers and asset numbers of the equipment in any way.
- Users will not permit anyone else to use the computer for any purpose, including, but not limited to, the user's family and/or associates, clients, client families, or unauthorized officers, employees, and agents of SBH-ASO.
- Users must report in writing any breach of password security immediately to the SBH-ASO Privacy Officer and Kitsap County IS Department.
- Users must maintain confidentiality when using the computers. The screen must be protected from viewing by unauthorized personnel, and users must properly log out and turn off the computer when it is not in use.
- Users must immediately report in writing any lost, damaged, malfunctioning, or stolen equipment or any breach of security or confidentiality to the SBH-ASO Privacy Officer and Kitsap County IS Department.

Enforcement

All managers are responsible for enforcing this procedure. The SBH-ASO Privacy Officer is notified of any violations. Employees who violate this procedure are subject to personnel action.