SUBJECT Information System Security		**CHAPTER** 03	**SECTION** 01	**SUBJECT** 05
CHAPTER Information Management	**SECTION** Technology			
WRITTEN BY Kathy Tilley & Kelly VanWormer	**REVIEWED BY**		**AUTHORIZED BY** PIHP Board	

I. APPLICATION:

☐ PIHP Board ☒ CMH Providers ☒ SUD Providers
☒ PIHP Staff ☒ CMH Subcontractors

II. POLICY STATEMENT:

It shall be the policy of the Region 10 PIHP that the Agency computer users will follow standard procedures to maintain the security and integrity of the information system.

III. DEFINITIONS:

Agency: PIHP, CMH/Administrative Staff, CMH Providers/Sub-contractors & SUD Providers, Contractual Staff, Students, Volunteers.

Authorized Access: A security measure using a separate user identification (login) and password for each personnel which allows entry into programs and files necessary for the performance of assigned duties within the organization.

Computer Acceptable Use Agreement (CAUA): A document signed by any personnel who has access to the Information System which certifies that the personnel will keep their password secret, keep information confidential, and utilize Information System resources in accordance with all applicable policies and procedures.

Data: The complete set of information stored within the Information System or contained on disks, printouts, CDs or other media, regardless of current format.

EHR (Electronic Health Record): A systematic collection of patient electronic health information generated by one or more encounters in any care delivery setting and including various health-related, demographic and service information.

Information System: The network of computers and other hardware and software used to categorize, store, retrieve, copy, protect, and manipulate data on behalf of the Agency and its clinical and administrative operations.

SUBJECT	CHAPTER	SECTION	SUBJECT
Information System Security	03	01	05
CHAPTER	**SECTION**		
Information Management	Technology		

Password: The individual alphanumeric code used by each personnel to access an Information System.

Restricted Access: A security measure used to limit the number of personnel who can gain entry for the purpose of reading or writing to data files. Access is allowed on a need-to-know basis and is controlled, in part, through the use of individual user passwords.

Security: Methods used to protect the Information System and its contents from fraud, computer viruses, power failure, sabotage, destruction, and unauthorized access or alteration. Includes alarms, monitoring, firewalls, and restricted physical access by means of locked rooms and limited distribution of keys and access cards, which limits physical access to the main computer system, to other computer equipment and to data from the Information System and which otherwise protects the system from damage.

Security Measures: In addition to those noted above, mechanisms and processes established to maintain the integrity of the system and its contents such as back-up tapes, offsite storage of back-up tapes, secondary power sources, physical security of equipment, virus detection and protection software, *RAID* hard drive configuration, training, password security agreements, etc.

User: Individual who has access to an Information System as personnel, contractor, temporary employee, client, or other person who uses Agency computers.

IV. STANDARDS:

CMH/SUD Providers/Sub-contractors must have policies and procedures regarding the following standards.

A. PIHP must require passwords to be used to restrict access to Information Systems. Information Systems will be set up in such a way that each user who receives access does so by entering their user ID and personal password. The CIO and technical staff must ensure that operational guidelines exist to ensure that excessively simple passwords cannot be used, and to ensure that passwords be regularly changed. These guidelines will balance the risk from changing passwords frequently with the risks from changing passwords infrequently.

B. PIHP must require users not to share their password(s) with any other individuals, including administrative or technical personnel, and to report any suspected password breach.

C. PIHP must require all computer users to read and sign a Computer Acceptable Use Agreement (CAUA), indicating understanding and willingness to abide by its terms and conditions. The user's supervisor must request access in keeping with the individual's roles and responsibilities. A responsible administrator must sign the CAUA prior to granting requested access.

SUBJECT Information System Security		**CHAPTER** 03	**SECTION** 01	**SUBJECT** 05
CHAPTER Information Management	**SECTION** Technology			

D. PIHP must require notification to technical staff of Agency staff termination, voluntary or involuntary, and the process for termination of that user's access to the Information System.

E. PIHP must require education of all users in awareness of restrictions related to confidentiality and privacy of consumers and protection of consumer information from unauthorized use, access, revision, duplication, deletion or dissemination.

F. PIHP must ensure the security of computer servers which house Agency shared data systems, including that they must be stored in a secure location, must have proper hardware and software maintenance of these servers to ensure their ongoing accessibility and security, and a daily backup must be made and stored securely using industry standard methods.

G. PIHP must require Information Systems, including the electronic health records (EHRs) and operating system, to automatically terminate (e.g., log the user off and/or close the application) after a period of inactivity.

H. PIHP must require Agency computers to be protected from viruses and similar destructive programs.

I. PIHP must ensure that no individuals can install programs which can be used to obstruct or disrupt the use of any computing system or network. Users shall not by any means attempt to infiltrate (e.g., gain access without proper authorization) a computing system or network.

J. PIHP must require the Agency's technical staff to continuously review ways that unauthorized access might be gained to Agency networks and computers, and implement methods as necessary to thwart that access.

V. PROCEDURES: N/A

VI. EXHIBITS: N/A