

USER CONFIDENTIALITY AGREEMENT
User Policy and Responsibility Statement
KENTUCKY HOMELESS MANAGEMENT
INFORMATION SYSTEM (ServicePoint)

AGENCY/ORGANIZATION NAME: _____

ADDRESS: _____

CITY _____ STATE _____ ZIP _____

=====

I understand that I will be allowed access to confidential information and/or records in order that I may perform my specific job duties and none other. I further understand and agree that I am not to disclose confidential information, and/or client records without the prior consent of the Kentucky Housing Corporation, unless such disclosure is required by law.

I understand that all USERID/Passwords to access the *Kentucky Homeless Management Information System (ServicePoint)* are issued on an individual basis. I further understand that I am solely responsible for all information obtained, through system access, using my unique identification. At no time will I allow any other person to use my USERID/Password to logon to the *Kentucky Homeless Management Information System (ServicePoint)*. I understand that accessing or releasing confidential information and/or records, or causing confidential information and/or records to be accessed or released, on myself, other individuals, clients, relatives, etc., outside the scope of my assigned job duties would constitute a violation of this agreement.

By affixing my signature to this document I acknowledge that I have been apprised of the relevant laws, concerning access, use, maintenance and disclosure of confidential information and/or records which shall be made available to me through my use of the *Kentucky Homeless Management Information System (ServicePoint)*. I further agree that it is my responsibility to assure the confidentiality of all information, which has been issued to me in confidence, even after my access to the *Kentucky Homeless Management Information System (ServicePoint)* has ended.

Pursuant to this agreement I certify that I have read and understand the following laws concerning confidential information and/or records. Kentucky Revised Statute KRS 434.845, 434.850 and 434.855 – Unlawful Access to a Computer.

434.845 Unlawful access to a computer in the first degree.

(1) A person is guilty of unlawful access to a computer in the first degree when he or she, without the effective consent of the owner, knowingly and willfully, directly or indirectly access, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer systems, computer network, or any part thereof, for the purpose of:

- (a) Devising or executing any scheme of artifice to defraud, or
- (b) Obtaining money, property, or services for themselves or another by means of False or fraudulent pertenses, representations, or promises.

(2) Unlawful access to a computer in the first degree is a Class C felony.

Effective: July 15, 2002

History: Amended 2002 Ky. Acts ch. 350, sec. 2, effective July 15, 2002. - - Created 1984 Ky. Acts ch. 210, sec. 2, effective July 13, 1984

434.850 Unlawful access to a computer in the second degree.

(1) A person is guilty of unlawful access to a computer in the second degree when he or She, without the effective consent of the owner, knowingly and willfully, directly or indirectly accesses, causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network, or any part thereof, which results in the loss or damage of three hundred dollars (\$300) or more.

(3) Unlawful access to a computer in the second degree is a Class D felony.

Effective: July 15, 2002

History: Amended 2002 Ky. Acts ch. 350, sec. 3, effective July 15, 2002. - - Created 1984 Ky. Acts ch. 210, sec. 3, effective July 13, 1984

434.855 Misuse of computer information

(1) A person is guilty of misuse of computer information when he or she:

(a) Receives, conceals, or uses, or aids another in doing so, any proceeds of a violation of KRS 434.845; or

(b) Receives, conceals, or uses or aids another in doing so, any books, records, documents, property, financial instrument, computer software, computer program, or other material, or objects, knowing the same to have been used in or obtained from a violation of KRS 434.845.

(2) Misuse of computer information is a Class C felony.

Effective: July 15, 2002

History: Amended 2002 Ky. Acts ch. 350, sec. 6, effective July 15, 2002. - - Created 1984 Ky. Acts ch. 210, sec. 4, effective July 13, 1984

USER POLICY

Partner Agencies shall share information for provision of services to homeless persons through a network Infrastructure that establishes electronic communications among the Partner Agencies.

Partner Agencies shall at all times have rights to the data pertaining to their clients that was created or entered by them in the ServicePoint system. Partner Agencies shall be bound by all restrictions imposed by clients pertaining to the use of personal data that they to not formally release.

It is a Client's decision about which information, if any, entered into the ServicePoint system shall be shared and with which Partner Agencies. The ServicePoint Client Consent/Release of Information shall be signed anytime the Client agrees to have his/her information entered into the system or shared with Partner Agencies.

Data necessary for the development of aggregate reports of homeless services, including services needed, services provided, referrals and Client goals and outcomes should be entered to the greatest extent possible.

The ServicePoint system is a tool to assist agencies in focusing services and locating alternative resources to help homeless persons. Therefore, agency staff should use the Client information in the ServicePoint system to target services to the Client's needs.

USER RESPONSIBILITY

Your User ID and Password give you access to the statewide KHMIS ServicePoint system. Initial each item below to indicate your understanding and acceptance of the proper use of you User ID and password. Failure to uphold the confidentiality standards set forth below are grounds for immediate termination from the KYHMIS Service/Point system.

(Please Initial each line and sign at the bottom of the page)

_____ My User ID and Password are for my use only and must not be shared with anyone.

_____ I must take all responsible means to keep my Password physically secure.

_____ I understand that the only individual who can view information in the ServicePoint System are authorized users and the Clients to whom the information pertains.

_____ I may only view, obtain, disclose, or use the database information that is necessary to perform my job and none other.

_____ If I am logged into ServicePoint and must leave the work area where the computer is located, I must log-off of ServicePoint before leaving the work area.

_____ A computer that has ServicePoint open and running shall never be left unattended.

_____ Failure to log off ServicePoint appropriately may result in a breach in client Confidentiality and system security.

_____ Hard copies of ServicePoint information must be kept in a locked, secure file..

_____ Client release forms must be retained in a locked, secure location for five (5) years From date of last service to client and then destroyed by shredding or burning. When hard copies of other ServicePoint information are no longer needed, they must be destroyed by shredding or burning to maintain confidentiality.

_____ If I notice or suspect a security breach, I must immediately notify the Agency and the System Administrator (KHC).

User Signature: _____ Date: _____

Print or Type User Name: _____ Title: _____