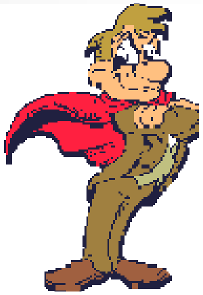
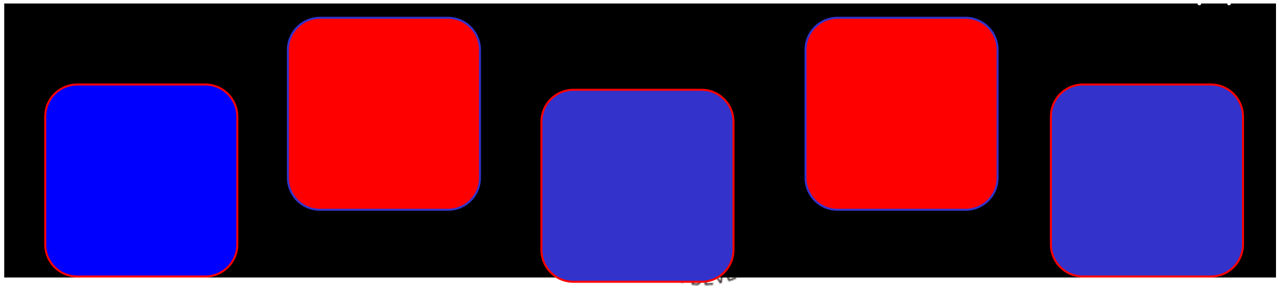
Alaska Homeless Management Information Systems (AKHMIS) Security Training Review





AKHMIS System Security

- ServicePoint (Bowman Systems) is a web-based software encrypted for secure transmittal and storage. Implementation of ServicePoint involves a centralized database where participating Agencies, with client consent, can enter and access Client information, and all data is encrypted at the database level.

- Every User of the AKHMIS system is authenticated with a unique User ID and password.

- A User will be locked out of the system after four consecutive bad logon attempts and will need to contact the System Administrator to regain access.

- All Users shall utilize the password protected screen savers on any computer accessing the HMIS database and the User shall log off of HMIS and shut down the browser when not using HMIS.

AKHMIS Program Responsibilities

- Your program must protect the AKHMIS system from viruses by using commercially available protection software and must regularly update virus definitions from the software vendor.

- You program must protect the AKHMIS system from malicious intrusion behind a secure firewall. Each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any other systems.

- For example, a workstation that accesses the Internet through a modem would need its own firewall. A workstation that accesses the server through a central server would not need a firewall as long as the server has a firewall

- Your program shall ensure that all their authorized Users are issued a unique User ID and password for AKHMIS and receive confidentiality training on the use of AKHMIS and applicable confidentiality laws.

Rules for Passwords and User IDs

- Each User will follow these Rules for Passwords and User IDs:

- Sharing of passwords and User IDs is forbidden. Every authorized User will be issued their own User ID and password. Keep your password secure and confidential.

- Never use the same password twice. When selecting a new password, choose one that is reasonably different from your previous password.

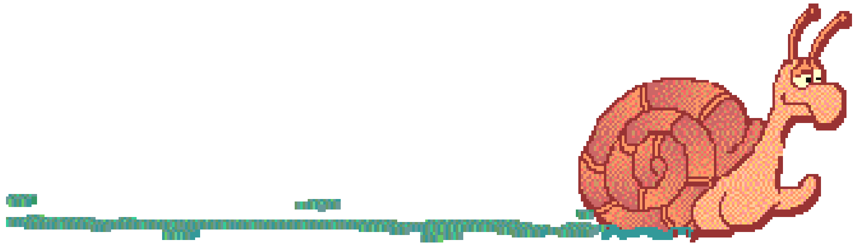
- ServicePoint will require a password change every 45 days. Passwords must be a minimum of 8 characters, and include 2 numeric values.

- Do not select a trivial, predictable or obvious password or a common word found in the dictionary or any of the below spelled backwards.

- Do NOT use someone else's or password or let anyone use your User ID. If you, or someone at your agency, needs more access, or if you are having problems with your access, contact your System Administrator for help.

- Beware of “shoulder surfers”. These are people who stand behind you and look over your shoulder while you are keying in your password or are working with confidential information.

- NEVER post your login or password on your terminal, under your keyboard or other obvious places.
- Always change the temporary password assigned to you by the System Administrator as soon as you receive it.



- LOG OFF or LOCK UP when you are finished using your terminal or workstation, or if you are stepping away from your desk, even momentarily.

- If you are going to be away from the office for an extended period (e.g. vacation or maternity leave), ask your administrator to temporarily suspend your access. Your ID will be reactivated when you notify the System Administrator or your return.

Let us review together the…

AKHMIS Licensed User Policy,

In regards to Security

- This agreement is signed by all users prior to accessing the AKHMIS databank aka: ServicePoint.

AKHMIS Licensed User Policy regarding Security User Responsibility Statement

A User ID and Password give a user access to the AKHMIS system. User must initial each item below indicating User understands and accepts the proper use of User's ID and password. Failure to uphold these confidentiality standards results in revocation of access to the AKHMIS.

1. My user ID and Password are for my use only.
2. My User ID and Password will not be shared with anyone.

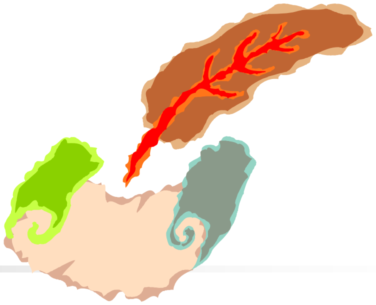
Continued…

3. I will keep my Password physically secure.
4. I understand that the only individuals who can view information in AKHMIS are authorized users who need the information for legitimate business purposes of this Agency and the Clients to whom the information pertains.
5. I will only view, obtain, disclose, or use the database information that is necessary to perform my job.
6. If I must leave my work area, I will log-off AKHMIS before leaving. (you may also lock your computer if leaving temporarily).

Continued…

5. A computer that has AKHMIS open and running will not be left unattended.
6. Hard copies of personally identifiable Client information printed from AKHMIS will be kept in a secure file, and destroyed when no longer needed.
7. If I notice or suspect a security breach, I will immediately notify the Agency’s executive director and the AKHMIS Administrator John Burger at 907-343-6593.

For Written Complaints



- For AKHMIS, users must permit clients to file a written complaint regarding the use of treatment of their information with AKHMIS. Client may file a written complaint with the Agency or the Municipality of Anchorage, AKHMIS (C/O MOA, Department of Health and Human Services, Human Services Division, AKHMIS Program), P.O. Box 196650, Anchorage, AK 99519-6650.

AKHMIS Team

- Sandra Olibrice-Program Coordinator: email- olibricesm@muni.org phone- (907)343-6592

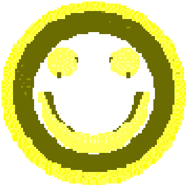
- John Burger-System Administrator: email- burgerjj@muni.org phone- (907)343-6593

- Melissa T. Anderson-AKHMIS Specialist-Trainer: email- andersonmt@muni.org phone- (907)343-6535

Additional Resources

- AKHMIS Team Joint Support Email address:

akhmissupport@muni.org



Thank you very much!