

RIHMIS Password Policy

Password Procedures:

The HMIS Lead Administrator generates an initial temporary password for new End Users automatically upon account creation. The System Administrator provides this password to the new End User. ServicePoint prompts the End User to reset the password immediately, and every 45 days in accordance with federal HMIS password regulations. If a user forgets their password, there is an option for users to reset their own password by entering their HMIS username. The temporary link will be sent to the users email address on file and will work for 15-minutes to reset their password immediately. It is the responsibility of the End Users to select passwords that meet password security guidelines set forth in the HMIS Password Policy and Federal HMIS regulations.

Password Requirements:

- All system-level passwords (e.g., root, enable, Windows Administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.
- HMIS Passwords change every 45 Days.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 60 days.
- All user-level and system-level passwords must conform to the guidelines described below.
- The same password must not be used for RI-HMIS more than once.

Creation of Passwords:

- Must contain at least 3 of the following characteristics:
 - Lower case characters;
 - Upper case characters;
 - Numbers;
 - Punctuation;
 - 'Special Characters' (e.g. @\$%^&*()-{}[]<>.,/?...etc.)
- Try to create easy to remember but hard to guess passwords. Some include song titles, affirmations or other phrases.
- AVOID creating weak passwords. Weak passwords have the following characteristics:
 - Under 8 characters;
 - Word found in a dictionary;
 - Common usage (names of pets, friends, computer terms, birthdays, address, phone numbers, patterns such as aaabbb or 123321);
 - Any of the above spelled backwards; and,
 - Any of the above preceded or followed by a digit.

RIHMIS Password Policy

Protection of HMIS Passwords:

- Use different passwords from other accounts.
- NEVER share HMIS passwords with ANYONE, including administrative assistance or secretaries; all HMIS passwords are to be treated as sensitive, confidential, HMIS information.
- Never store passwords anywhere written down or online without encryption.
- Never reveal a password in an email, chat or other electronic communication.
- Do not speak about a password in front of others.
- If someone demands a password, refer them to this document and direct them to the HMIS Administrator.
- Always decline "Remember Password" on browsers for all applications.
- If account or password compromise is suspected, report to the HMIS Administrator.

Violations:

- Should someone ask that your password is shared, please report them to the HMIS Administrator at the HMIS Lead organization within 24 hours.
- Should you become aware of sharing of passwords or any other breach, it must be reported to the HMIS Administrator at the HMIS Lead within 24 hours.
- All reports should go direct to the HMIS Administrator at the Rhode Island Coalition for the Homeless. Not sure who to contact? Email hmis@rihomeless.org!
- End Users found to have violated this policy may be subject to disciplinary action, up to and including the revocation of HMIS access and the potential termination from their agency.