Rhode Island Coalition for the Homeless

RIHMIS Password Policy

Password Procedures

The HMIS Lead Organization generates an initial temporary password for new End Users 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 or tries to log-in with 3 failed attempts, the HMIS staff at the Rhode Island Coalition for the Homeless must be contacted in order to request a new password. The temporary password will only work until the user signs in and is asked to reset the password immediately. It is the responsibility of the End Users to select passwords that meet password security guidelines set forth in this RIHMIS Password Policy.

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.
⇒ User accounts that have system-level privileges granted through group memberships or programs such as "Sudo" must have a unique password from all other accounts held by that user.
⇒ All user-level and system-level passwords must conform to the guidelines described below.

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 revel 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.
- Should you become aware of sharing of passwords or any other breach, it must be reported to the HMIS Administrator.
- All reports should go direct to the HMIS Administrator, Don Larsen, at the Rhode Island Coalition for the Homeless. 401-721-5685 ext. 25.
- 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.

Questions/Concerns?

Contact the RI-HMIS Lead at:
Rhode Island Coalition for the Homeless,
1070 Main St., Pawtucket, RI 02860
(401) 721-5685 info@rihomeless.org
HMIS Team:
Bob Maurice: ext. 26 bob@rihomeless.org
Shalissa Coutoulakis: ext. 25 shalissa@rihomeless.org