Blue Ridge Continuum of Care
A Place to Call Home

COUNCIL OF COMMUNITY SERVICES

BRCOC HMIS 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. HMIS prompts the End User to reset the password immediately, and every 60 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 for Agencies:

- ☐ All system-level passwords (e.g., Windows Administrator, root, enable, application administrator accounts, etc.) must be changed on at least a quarterly basis.
- ☐ HMIS Passwords change every 60 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 new HMIS password cannot be one of the last 3 passwords used.

Creation of HMIS Passwords:

- ☐ Requirements - An HMIS password must contain at least:
  - ○ Eight (8) characters or more.
  - ○ One uppercase letter (A to Z).
  - ○ One lowercase letter (a to z).
  - ○ One number (0 to 9).
  - ○ One non-alphanumeric character (! @ # $ ( ) % ^ & *).
  - ○ No spaces

- ☐ Restrictions – An HMIS password cannot contain:
  - ○ The name of our HMIS instance (“blueridge”).
  - ○ The word “clarity.”
  - ○ Your First Name, Last Name, or Username.
  - ○ “ABC” or “123”
  - ○ More than two consecutive characters.
  - ○ The same password as the three (3) prior passwords.

Protection of HMIS Passwords:

- ☐ A user's HMIS password should be different from other accounts they use.
- ☐ NEVER share HMIS passwords with ANYONE, including administrative assistants or secretaries, supervisors who do not have HMIS access, etc. All HMIS passwords should be treated as sensitive and confidential HMIS information.
- ☐ Never store passwords written down or online without encryption.
- ☐ Never reveal an HMIS password in an email, chat, or other electronic communication.
- ☐ Do not speak about your password in front of other staff or clients.
- ☐ If someone demands to know your HMIS password, refer them to this document and direct them to the Agency HMIS Captain who should report the issue to an HMIS System Administrator.
- ☐ If a user's HMIS account or password is compromised or suspected to be compromised, report the incident immediately to the Agency HMIS Captain and an HMIS System Administrator.

Violations of HMIS Password Policies:

- ☐ If someone asks that you share your password with them, please report them to your Agency HMIS Captain and the HMIS System Administrators within 24 hours.
- ☐ Should you become aware that a staff person with an HMIS user account has shared their password or committed any other breach of security or privacy, it must be reported to your Agency HMIS Captain and the HMIS System Administrators with 24 hours.
- ☐ All reports should be submitted to the HMIS System Administrators at the Council of Community Services as soon as possible (no later than 24 hours after the incident). If you are not sure who to contact, you can always email hmis@councilofcommunityservices.org.
- ☐ End users who violate these policies may be subject to disciplinary action, up to and including, the revocation of their HMIS access and potential termination from their agency.