Password Management Procedure:

<table>
<thead>
<tr>
<th>Version</th>
<th>Approval Date</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td>December 20, 2021</td>
<td>Chief Information Security Officer</td>
</tr>
</tbody>
</table>

I. **Purpose of Procedure**
To protect HealthShare Exchange (HSX) information assets by managing and enforcing password requirements.

II. **Procedure Scope**
This procedure applies to all employees, interns, contractors, members, participants, users, and third parties who use HSX information assets and related resources.

This procedure applies to centrally-administered and managed information asset technologies, personally-owned computing devices connected by wire or wireless to the HSX network, and to off-site computing devices that connect remotely to the HSX network.

This procedure applies to System Administrators and developers who manage or design systems that require passwords for authentication.

III. **Procedure**
The following controls shall be implemented to maintain the security of all passwords:

1. passwords shall be prohibited from being displayed when entered;
   - Where applicable, HSX will work with external parties to ensure that password settings are compliant with HSX password management policy and procedure
   - All systems, including new systems in development must hide passwords while they are entered
2. passwords shall be changed whenever there is any indication of possible system or password compromise; and
3. user identity shall be verified before performing password resets.
4. passwords shall be protected from unauthorized disclosure and modification when stored and transmitted;
5. passwords shall not be included in any automated log-on process (e.g., stored in a macro or function key);
6. all passwords shall be encrypted during transmission and storage on all system components;
7. users shall sign a statement to keep passwords confidential and to keep group passwords solely within the members of the group; and
8. temporary passwords shall be unique to an individual and shall not be guessable.
9. Users shall be provided with an initial or temporary strong password that is unique and random generated with the Mirth SSO. However, when a user requests a password reset, we will use LastPass Password Generator (to have at least 8 random characters including letters, numbers, and excluding any similar characters).
10. temporary passwords will be required to change at initial login
11. vendor supplied passwords will be required to change upon go-live
12. Passwords must be kept confidential and must not be written down or recorded electronically.
13. passwords must not be provided to anyone for any reason (to avoid compromising their user credentials through social engineering attacks)
14. passwords and accounts must not be shared.
15. personal and HSX (business) passwords must be different.
16. Passwords must be changed at least every 90 days or whenever there is any indication of possible system or password compromise.
17. Employees, interns, contractors, members, participants, users, and third parties shall utilize strong passwords that require at least 8 characters which are a combination of alphabetic, upper- and lower-case characters, numbers, and special characters (combination of any three [3] of the above four [4] listed is acceptable).
18. Passwords cannot be reused for at least six (6) generations. At least four changed characters must be used when new passwords are created.
19. Temporary passwords shall be changed at the first log-on

**Electronic Signature Passwords**
Consistent with HSX policies and procedures, passwords utilized for electronic signatures will only be provided to those authorized in the Contracting and
Signatory Authority policy and may not be shared. Documents electronically signed will have the meaning of “Approved”.

- Electronic signatures are the same as hand written signatures and are legally binding when used in accordance with the provisions of the Contracting and Signatory Authorization Policy.
- Authorized persons who use application based electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:
  o Identity verification of the individual is required prior to establishing, assigning, or certifying an individual’s electronic signature or any element of such signature.
  o Maintaining the uniqueness of each combined identification code and password, such that no two (2) individuals have the same combination of identification code and password.
  o Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging);
  o Following loss management procedures to electronically de-authorize lost, stolen, missing or otherwise potentially compromised tokens, cards and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls;
  o The use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organization management; and
  o Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.
  o Electronic signatures not based upon biometrics shall employ at least two distinct identification components that are administered and executed.
  o Electronic signatures, unique to one individual, cannot be reused by, or reassigned to, anyone else.

Electronic signatures based upon biometrics are designed to ensure that they cannot be used by any individual other than their genuine owners

**Password Reset Procedure**

When users call in or email the Help Desk to request a new password the following procedure must be followed:

1) The user’s e-mail linked to the account in reference shall be confirmed
The user will need to provide the Help Desk with the last successful log in date and time

The allocation of passwords shall be controlled through a formal management process:

1. the use of third parties or unprotected (clear text) electronic mail messages shall be avoided;
2. users shall acknowledge receipt of passwords;
3. default vendor passwords shall be altered following installation of systems or software;
4. when users are required to maintain their own passwords, they shall be provided initially with a secure temporary password, which they are forced to change immediately;
5. temporary passwords shall be changed at the first log-on;
6. temporary passwords shall be given to users in a secure manner;
7. passwords shall be changed at least every ninety (90) days or based on the number of accesses;
8. passwords for privileged accounts shall be changed at least every sixty (90) days;
9. passwords shall require at least eight (8) characters which are:
   i. easy to remember;
   ii. not based on anything somebody else could easily guess or obtain using person-related information (e.g., names, telephone numbers, and dates of birth etc.);
   iii. not vulnerable to dictionary attack (do not consist of words included in dictionaries);
   iv. free of consecutive identical characters; and
   v. a combination of alphabetic, upper and lower case characters, numbers, and special characters (combination of any three [3] of the above four [4] listed is acceptable).
10. passwords shall be prohibited from being reused for at least six (6) generations for all users; and
11. if the operating environment allows, at least four (4) changed characters are changed when new passwords are created.
12. Alternatively, passwords/phrases must have a strength (entropy) at least equivalent to the parameters specified above.

Process for setting password complexity requirements in admin interfaces (i.e. Mirth SSO)
1. Mirth SSO Required Settings

Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements. Under no circumstances can users change the requirements for their passwords on any device.

IV. Enforcement (If applicable)

HSX Technical Operations Lead will be responsible for doing a yearly check of all technical controls to ensure that all passwords through all systems, including external applications, are compliant with HSX's password management policy and procedure. Automatic software controls will also be used to enforce this policy.

Password requirements will be shared with users upon their initial credentialing process. These requirements will also be embedded in the user-facing interface when users will be prompted to create their unique password.
During the HSX onboarding process, external organizations are referred to the HSX website to ensure compliance with HSX’s publicly available policies. All parties will be required to sign an attestation to acknowledge notice of this procedure and the Password Management Policy.

<table>
<thead>
<tr>
<th>Responsible Owner:</th>
<th>HSX CISO</th>
<th>Contact: email</th>
<th><a href="mailto:Brian.Wells@healthshareexchange.org">Brian.Wells@healthshareexchange.org</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved By:</td>
<td>HSX CISO</td>
<td>Version #</td>
<td>1.2</td>
</tr>
<tr>
<td>Current Approval Date:</td>
<td>December 20, 2021</td>
<td>Prior review/Approval Dates:</td>
<td>October 28, 2023</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>December 5, 2022</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>October 9, 2021</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>October 19, 2020</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>December 15, 2019</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>April 1, 2017</td>
</tr>
<tr>
<td>Date Procedure to go into Effect:</td>
<td>December 20, 2021</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Related Documents:</td>
<td>Password Management Policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Glossary</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>