Every Heartland Community College employee and student is assigned a LOGIN NAME. This login name is based upon the person’s first name and last name. When necessary, numbers may be added to differentiate one person from another. Employees may contact IT to obtain their LOGIN NAME if they do not know what it is. Some examples of Login Names are shown below.

<table>
<thead>
<tr>
<th>Employee First Name</th>
<th>Employee Last Name</th>
<th>LOGIN NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carol</td>
<td>Boyer</td>
<td>CBOYER</td>
</tr>
<tr>
<td>George</td>
<td>Schneider</td>
<td>GSCHNEID</td>
</tr>
<tr>
<td>Shawn</td>
<td>Mitchell</td>
<td>SMITCHEL</td>
</tr>
<tr>
<td>Samantha</td>
<td>Mitchell</td>
<td>SMITCHE1</td>
</tr>
<tr>
<td>Sara</td>
<td>Mitchell</td>
<td>SMITCHE2</td>
</tr>
</tbody>
</table>

The password that is associated with the LOGIN NAME must meet the following requirements:

**LENGTH:**
Minimum of 8 characters.

**COMPLEXITY:**
- Passwords must include at least 1 letter and 1 number.
- Passwords may not match the Login Name.
- Passwords may not include spaces.
- Passwords are case sensitive.
- Passwords may not contain personal information (i.e., name and date of birth).

**HISTORY:**
Passwords may not be reused for 5 years.

**MAXIMUM AGE:**
Passwords must be reset every 120 days.

**GRACE LOGINS:**
6
A grace login is a login that is allowed AFTER a user’s password has expired. Once a password has expired (see dates above), the user will receive a message that the password has expired, and that he/she has 6 grace logins in which to change the password. Users are encouraged to change their passwords as soon as they expire to avoid being inadvertently locked out of the network once the grace logins are used.

**LOGIN ATTEMPTS:**
6
Each time a user tries to login with an incorrect password, a “login attempt” will be used. If a user tries to login 6 times and fails each time, the user account will be locked. When this occurs, the user will need to call IT to have the account unlocked.

**PROTECTION:**
A complex password is no longer secure if another person has access to it. Users may NEVER share a password with ANY other person, including supervisors and IT personnel. Users must never write down a password on a piece of paper or “post-it” note in an effort to keep from forgetting it.