SOP Attachment A – DC HMIS User Agreement

**DC Homeless Management Information System**

**User License Agreement**

**Version 5.0**

**Effective Date: June 1, 2011**

<table>
<thead>
<tr>
<th>User’s Full Name:</th>
<th>________________________________</th>
</tr>
</thead>
<tbody>
<tr>
<td>HMIS User ID:</td>
<td>________________________________</td>
</tr>
<tr>
<td>Agency Name:</td>
<td>________________________________</td>
</tr>
<tr>
<td>Program Name(s):</td>
<td>________________________________</td>
</tr>
<tr>
<td>License Effective Date:</td>
<td>__________________________________</td>
</tr>
</tbody>
</table>

**USER RESPONSIBILITY AND ETHICS STATEMENTS:**

Your User ID and Password give you access to the DC HMIS. Initial each item below to indicate your understanding and acceptance of the proper use of your User ID and Password. All users in the DC HMIS must abide by the *DC HMIS Policies and Standard Operating Procedures* that govern the use of the system and define security and confidentiality protocols. DC HMIS Users must treat clients and partner agencies with respect, fairness, and good faith and should maintain high standards of professional conduct in their capacity as a DC HMIS User. Failure to uphold the standards of the DC HMIS is grounds for immediate termination from the DC HMIS and may result in personnel action.

- I have read and understand the *DC HMIS Policies and Standard Operating Procedures* (or have been trained on them) and will abide by the protocols set forth in that document.
- My User ID and Password are for my use only and must not be shared with anyone including my Agency Administrator and Executives.
- I must take reasonable means to keep my Password physically secure.
- A computer that has the DC HMIS open and running shall never be left unattended.
- Failure to log off the DC HMIS appropriately may result in a breach in client confidentiality and system security, therefore, I will log off of the DC HMIS each time I use it.
- Hard copies of client information from the DC HMIS must be kept in a secure file.
- When hard copies are no longer needed, they must be properly destroyed to maintain confidentiality.
- Electronic files exported from the DC HMIS must be password protected to maintain confidentiality.
- If I notice or suspect a security breach, I must immediately notify the DC HMIS System Administrator.

**USER'S SIGNATURE** ___________________________ **DATE** __________

**AGENCY ADMINISTRATOR’S SIGNATURE** ___________________________ **DATE** __________

**PRINT AGENCY ADMINISTRATOR’S NAME**