AVEN HOME HEALTH SERVICES, INC.
INFORMATION SYSTEMS USER AGREEMENT

You must have an AHHS User ID and Password to login to the SOS Portal. If this is your first time logging in, please use the User ID and the one-time password that was emailed/given to you by Aven Home Health Services staff. You must change your password after your first log-in. Failure to do so will constitute a breach of contract and may lead to termination of system access privileges.

Your User ID will be the first letter of your first name, followed by your entire last name (ex.: Jane Doe = jdoe, Sally Nurse = snurse).

The default password for all new SOS Portal users is: change-me

Do not disclose or lend your User ID AND/OR PASSWORD to anyone else. They are for your use only and serve as your electronic signature. This means that you will be held responsible for the consequences of unauthorized or illegal transactions. Sharing of accounts may lead to termination of system access privileges and /or adverse action up to and including legal prosecution.

If you cannot remember your password, you may contact the AHHS Office to have your password reset to the one-time password. Call (818) 380-0853 for an immediate reset, or e-mail ilongomba@avengroup.com for a reset 24 hours after the request.

To change your password, first login and then select "Profile" in the top right corner of the screen.

Users shall:

- Immediately report all lost or stolen user ID/password information.
- Log-off the SOS Portal when leaving a computer unattended.
- Secure sensitive information (on paper and in electronic formats) when left unattended.
- Keep sensitive information out of sight when visitors are present.
- Only access sensitive information necessary to perform job functions (i.e., need to know).

Users shall not:

- Use another person's account or password.
- Exceed authorized access to sensitive information.
- Store sensitive information in public folders or other insecure physical or electronic storage locations.
- Share sensitive information, except as authorized.
- Transport, transfer, e-mail, remotely access, or download sensitive information, unless such action is explicitly permitted by the DOPCS/Administrator or owner of such information.
- Store sensitive information on portable devices such as laptops, personal digital assistants (PDA) and universal serial bus (USB) drives.
- Knowingly or willingly conceal, remove, mutilate, obliterate, falsify, or destroy information for personal use for self or others.
- Modify software without management approval.

Users shall ensure that passwords:

- Contain a minimum of six alphanumeric characters and at least one number or one special character.
- Avoid words found in a dictionary, names, and personal data (e.g., birth dates, addresses, social security numbers, and phone numbers).
- Are changed immediately in the event of known or suspected compromise, and immediately upon first log-in (e.g. default passwords).
- Are not reused until at least six other passwords have been used.
- Are committed to memory, or stored in a secure place.

I have read the AHHS Rules of Behavior and understand and agree to comply with these provisions. I understand that my use of the information system establishes my consent to any and all monitoring, recording and auditing of my activities. I understand that violations of the AHHS Rules or information security policies and standards may lead to disciplinary action, up to and including termination of employment; and/or revocation of access to SOS Portal information. I understand that exceptions to the AHHS Rules must be authorized in advance in writing by the Information Systems Manager.

_____ _____

Printed Name/Signature of Employee or Contractor Date