Grace House Services

*Nurturing Growth….Transforming Lives*

# CONFIDENTIALITY POLICY

Each employee of Grace House will be required to agree to and sign a confidentiality agreement. Strict confidentiality of any resident or visitor, including friends and family members, is required. All participants in any outreach program conducted on behalf of Grace House are also covered by confidentiality.

Grace House, Inc. is bound by terms of both medical and ethical confidentiality to keep health conditions and personal conditions known only to the affected person. Disclosure is the personal right of the protected person. Failure to maintain strict confidentiality may result in immediate termination of employment and legal actions.

This policy applies to written and oral communication. Files must be kept locked and not released without proper authorization and written consent for release of information.

When working on your computer on client-level data, each person must log off HMIS and close the file or window before leaving their computer unattended for any length of time.

If leaving your office unattended, the door must be locked.

Computers must be protected by password and set to lock within five minutes of non-use to protect confidential information contained within.

Grace House Services

*Nurturing Growth….Transforming Lives*

# HMIS SECURITY POLICY

Certain electronic security precautions are required for each agency:

- Install and maintain a firewall on the user's computer or the agency network
- Password-protected screensavers set at no more than 5-minute intervals
- Automatically updating antivirus software installed and maintained on every internet-accessible computer
- Keep the Operating System on each AWARDS access computer terminal up to date with the latest security devices

All users must attend a formal AWARDS training. The Director or Assistant Director will contact local HMIS staff to set up training for new hire employees within 14 days of beginning employment. The Executive Director or Assistant Director MUST contact the Data Systems Administrator within 24 hours of the end of employment so that the active user account can be disabled. This can be done in advance, so Directors and administrative staff are encouraged to alert the Data Systems Administrator as soon as it is known that a user account will no longer be needed.

All information placed into HMIS will be safeguarded, and no personal identifying information will be released to anyone beyond the system administration requirements. In addition, a privacy notice will be posted in areas where data is collected for HMIS, and every client will be made aware of the notice and sign a consent that identifies the level of data sharing agreed upon by the client.

All information contained within HMIS is subject to the confidentiality policies of the organization signed by all staff members at the time of hire. Inappropriate handling of the information in HMIS is subject to disciplinary actions, including termination, and may result in legal actions taken against the violator on behalf of the client.