****

**HOMELESS MANAGEMENT INFORMATION SYSTEM**

**SECURITY PLAN**

**Introduction**

Security refers to protecting the HMIS system and its data (electronic or printouts) from unauthorized access, loss, or corruption.

The HMIS Lead agency and the HMIS Participating agencies will adhere to the baseline security standards and requirements for system application and hardcopy security as outlined in the Federal Register HMIS Notice dated July 30, 2004. The HMIS Lead agency and the HMIS Participating agencies will:

* Apply system security provisions to all systems where personal protected information is stored, including, but not limited to networks, desktops, laptops, mini-computers, mainframes and servers;
* Protect ShareLink HMIS from viruses by using commercially available virus protection software. Virus protection must include automated scanning and must be regularly updated to maintain optimum protection;
* Protect ShareLink HMIS from malicious intrusion behind a secure firewall
* Ensure that when a workstation is not in use, the ShareLink HMIS Technical staff log off before leaving their workstation;
* Hard copies of client information will be secured

The HMIS Lead will adhere to the baseline security standards and requirements for system application and hardcopy security as outlined in the Federal Register HMIS Notice dated July 30, 2004. The HMIS Lead will:

* Provide to each participating Agency a User Authentication System consisting of a unique User name and a password for each authorized User;
* Provide ShareLink HMIS ServicePoint administration and user access to the ServicePoint software application for organizations using the ShareLink HMIS;
* Coordinate ShareLink HMIS software upgrades and updates with the software provider;
* Provide initial and on-going user training and technical support to maintain the security of the ShareLink HMIS system;
* Oversee the use of Public Key Infrastructure use further secure access to the HMIS system to previously approved computers;
* Complete a background check on the ShareLink HMIS administrators

The HMIS software provider and system host will

* Ensure that all ShareLink HMIS data is encrypted to meet current industry standards prior to electronically transmitting it over the Internet, public accessible networks or phone lines;
* Ensure that data is stored in binary, not text, format;
* Ensure that a copy of all ShareLink HMIS data is made daily to another medium and stored in a secured off-site location where the required privacy and security standards are met;
* Provide for the physical security of the system
* Ensure that the system enables reporting on user activity and access of client records.

HMIS users will receive training in Security Policies and acknowledge their responsibilities by signing the ShareLink HMIS User Policy and Responsibility Statement prior to being granted HMIS access. Each user will renew their Policy and Responsibility Statement yearly in order to maintain HMIS access.

The CoC, HMIS Committee, Agencies, and HMIS lead will share the responsibility of reviewing compliance with these standards at least annually. Any security policy compliance issue arising from review or from incident will be promptly addressed by the HMIS, Agency and HMIS Committee with CoC oversight.

Failure to comply with security policies can result in a user’s or agency’s access to HMIS being discontinued in accordance with HMIS Standard Operating Policies and Procedures.