Stanislaus County HMIS

HMIS Security Standards

Purpose: This document is designed to establish security standards for the Stanislaus County Homeless Management Information System (Stanislaus County HMIS) participating agencies within the Stanislaus Community System of Care Collaborative (StanCSOC). The following requirements and recommendations are based on the Security Standards as defined in the HUD HMIS Data and Technical Standards Final Notice of July 30, 2004, and the presentation of these standards in the HUD HMIS Data and Technical Standards National Broadcast of October 18, 2004. A goal of the Stanislaus County HMIS Project is to support and assist agencies in meeting these requirements.

Security Standards: The Stanislaus County HMIS Security Standards are divided into two sections. Security Requirements are minimum standards with which all HMIS participating agencies must comply. Additional Security Recommendations are best practices recommended by the Stanislaus County HMIS Project Team. The security standards include both technology solutions and protocols for staff use of technology.

Security Audit: Stanislaus County HMIS staff will conduct an initial and periodic security audit of each participating agency to document compliance with the security requirements; the audit can be performed in conjunction with designated agency staff. Each requirement section below includes specific instructions for auditing and documenting compliance with the requirement. The Stanislaus County HMIS staff will work with agencies to assess and overcome any identified barriers to security compliance.

Security Requirements

1.	**Applicability**	HMIS Security Requirements apply to all networked computers at HMIS participating agencies as well as all non-networked computers that are used by HMIS participating agencies to access HMIS software. The Security Requirements specifically apply to:
a.		All other computers, such as employee or volunteer owned computers, used to access HMIS over the Internet
e.	**Audit**	Visit all applicable sites. List all applicable sites and the number of applicable computers at each site.
2.	**Passwords**	Computers must be secured by a user password at computer login. Computer passwords and HMIS software passwords must meet the following minimum criteria:
a.		Passwords must contain at least one number, one special character (ie. $#@), and at least one capital letter.
b.		Passwords must not be based on the users name, organization, or software.
c.		Passwords must not be based on common words in any language. (ie. Food, Car, Run).
d.		Written information pertaining to passwords must not be displayed in any publicly accessible location.
e.	**Audit**	Does the agency have a written password policy that complies? Does the agency have a computer enforced password policy? List any additional applicable information.
3.	**Anti-virus**	All computers must have anti-virus software installed.

a.		Anti-virus software must be updated regularly.
b.	**Audit**	List manufacturer of anti-virus software installed. If multiple manufacturers of anti-virus software are in use then list the manufacturer and the name of the computer that coincides with the software. Also note the date or version of the anti-virus definition files that are installed on each computer.
4.	**Firewall**	All computers must be protected by a firewall.
a.	**Audit**	If a hardware firewall in employed, list the manufacturer, model, revision number, and firmware version. If a software firewall in employed list manufacturer and version number.
5.	**Digital Certificates**	All computers must be identified by HMIS through the use of a locally installed digital certificate employing standard Public Key Infrastructure technology. Computers without digital certification will not be able to access HMIS.
a.		Each Internet Browser software package installed on a computer must have its own separate digital certificate in order to access HMIS through that browser software.
b.	**Audit**	Visually verify installation of digital certificates by viewing the Internet Options under the View menu in Internet Explorer. Locate the Content tab and then click the certificates button. Verify that the HMIS certificate is installed.
6.	**Wireless Access Points (WAP)**	Wireless is not to be used with any computers that are being used with HMIS.
7.	**Operating System**	All computers must run Microsoft Windows 2000 or later operating systems.
a.	**Audit**	Verify Operating System Service Pack version by running Winver and recording the output below. To run Winver click on start, select Run, and then type Winver. Click on OK.
8.	**System Updates**	All computers must be regularly updated for protection against security threats and must have the latest service packs installed.
a.	**Audit**	Verify Operating System Service Pack version by running Winver and recording the output below. To run Winver click on start, select Run, and then type Winver. Click on OK. For networks that do not have their own Windows Update server, navigate to windowsupdate.microsoft.com, and check for new updates. If applicable, view the installation history to determine if all updates have been installed.
9.	**Computer Locking**	Computers must be locked when on but unstaffed to prevent unauthorized access to HMIS. Computers must be locked via 1) "ctrl-alt-del" and "lock computer," or 2) logging off. Computer will also automatically lock when the screen saver begins.
a.	**Audit**	List any HMIS applicable computers that are unstaffed and unlocked upon arrival at the site. Observe staff ability to lock and unlock the workstations. List names of staff observed and document whether they are able to perform the action.
10.	**Anti-spyware**	All computers must have anti-spyware/anti-malware software installed.
a.		Anti-spyware/anti-malware software must be updated regularly.
b.	**Audit**	Visually verify that suggested anti-spyware software is installed in Add/Remove programs. Launch each anti-spyware application and check it for updates. List

		computer names of workstations not current.
10.	**Security Audit**	HMIS participating agencies will be subject to a security audit prior to implementing HMIS and on an annual basis to document compliance with security requirements
a.		The security audit will be conducted by the Stanislaus County HMIS staff in conjunction with designated agency staff.

Additional Security Recommendations

1.	**Computer and HMIS Passwords**	Computer and HMIS passwords should routinely change at a rate of no less then three times a year.
a.		Computer and HMIS passwords within an agency department should be changed immediately upon personnel changes within that department.
b.		HMIS software user passwords should be different from users' passwords for other non-HMIS accounts.
c.		HMIS software passwords should not be disclosed to anyone else. All passwords should be treated as sensitive, confidential information. Follow these precautions: • Do not reveal a password over the phone to anyone • Do not reveal a password in an email message • Do not reveal a password to your supervisor or manager • Do not talk about a password in front of others • Do not hint at the format of a password (e.g., "my family name") • Do not reveal a password on questionnaires or security forms • Do not share a password with family members • Do not reveal a password to co-workers while on vacation • If someone demands a password, refer them to this document or have them contact the HMIS Project Team
d.		Do not use the "Remember Password" feature of applications.
2.	**Avoid Unsafe Behavior**	Computers used to access HMIS should never be used for 1) recreational web surfing or 2) downloading files offered through various file sharing services such as music sharing services, as such behavior increases the risk of contracting viruses or spyware/malware.
a.		All implementations should support a hardware address that can be registered and tracked, i.e., a Media Access Control (MAC) address.