

# ShelterLink HMIS Security Standards

**Purpose:** This document is designed to establish security standards for participating agencies within the ShelterLink HMIS system. 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. A goal of ShelterLink is to support and assist agencies in meeting these requirements.

**Security Standards:** The ShelterLink 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 ShelterLink Project Team. The security standards include both technology solutions and protocols for staff use of technology.

**Security Audit:** The ShelterLink Systems Administrator will conduct a security audit to document compliance with the security requirements. The ShelterLink Systems Administrator will work with agencies to assess and overcome any identified barriers to security compliance.

## Security Requirements

|           |                             |  |
|-----------|-----------------------------|--|
| <b>1.</b> | <b>Applicability</b>        | 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 computers connected to the agency's network  |
| b.        |                             | All computers that access the agency's network via Virtual Private Network (VPN)   |
| c.        |                             | All other computers, such as employee or volunteer owned computers, used to access HMIS over the Internet  |
| <b>2.</b> | <b>Passwords</b>            | 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 1 number and 1 letter.   |
| b.        |                             | Written information pertaining to passwords must not be displayed in any publicly accessible location. Password recording must be disabled at each computer. (Do not use the "Remember Password" feature of applications.)                               |
| <b>3.</b> | <b>Anti-virus</b>           | All computers must have anti-virus software installed.   |
| a.        |                             | Anti-virus software must be updated regularly.   |
| <b>4.</b> | <b>Firewall</b>             | All computers must be protected by a firewall.   |
| <b>5.</b> | <b>System Updates</b>       | All computers must be regularly updated for protection against security threats and must have the latest service packs installed.  |
| <b>6.</b> | <b>Computer Locking</b>     | Computers must be locked when unstaffed to prevent unauthorized access to the HMIS. Computers must be secured via locking screensavers or by logging off.  |
| <b>7.</b> | <b>Anti-spyware</b>         | All computers must have anti-spyware/anti-malware software installed.  |
| a.        |                             | Anti-spyware/anti-malware software must be updated regularly.  |
| <b>8.</b> | <b>Digital Certificates</b> | All computers must be identified by HMIS through the use of a locally installed digital certificate employing standard Public Key Infrastructure technology.   |

|            |                                     |   |
|------------|-------------------------------------|---|
| <b>9.</b>  | <b>Wireless Access Points (WAP)</b> | All wireless LAN devices must utilize WPA or WPA2 security protocols and strong passwords of at least 14 random characters or must utilize a corporate-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. |
| <b>10.</b> | <b>Electronic Data Storage</b>      | All HMIS data is classified as confidential and must be handled discreetly.   |
| a.         |                                     | Electronic copies shall be stored only on an encrypted device where a password is required to access the data.  |
| b.         |                                     | Electronic copies shall be stored only where the appropriate staff can access the data.   |

### **Additional Security Recommendations**

|           |                                    |   |
|-----------|------------------------------------|---|
| <b>1.</b> | <b>Computer and HMIS Passwords</b> | Computer passwords should routinely change at a rate of no less than 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: <ul style="list-style-type: none"> <li>• Do not reveal a password over the phone to anyone</li> <li>• Do not reveal a password in an email message</li> <li>• Do not reveal a password to the boss</li> <li>• Do not talk about a password in front of others</li> <li>• Do not hint at the format of a password (e.g., "my family name")</li> <li>• Do not reveal a password on questionnaires or security forms</li> <li>• Do not share a password with family members</li> <li>• Do not reveal a password to co-workers while on vacation</li> <li>• If someone demands a password, refer them to this document or have them contact the ShelterLink Systems Administrator.</li> </ul> |
| <b>2.</b> | <b>Avoid Unsafe Behavior</b>       | Computers used to access HMIS should never be used for 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.   |