Homeless Management System (HMIS) Security Checklist

WORKSTATION REQUIREMENTS			
REQUIREMENT	YES	DOES NOT	FOLLOW UP ACTION
Written Communication uses HMIS ClientID (not name)			
Hard copies of client information kept in locked cabinet (or in locked room with staff members responsible to monitor these files)			
Loose papers with client information (outside of client file) disposed of			
Monitor is turned away from a door or window, and away from client seats or outside viewing			
Documents containing passwords are physically locked or secure			
Servers housing HMIS information kept at a secured and monitored facility			

AGENCY REQUIREMENTS			
REQUIREMENT	YES	DOES NOT	FOLLOW UP ACTION
Notify TVCH within 24 hours of a user deactivation for user no longer employed/needing access			
Display HMIS Consent Poster near where Intake is performed			
All current users participate in HMIS Orientation Training			
Agency reports security incidents within 2 business days of occurrence			

TECHNICAL SAFEGUARDS REQUIREMENTS

REQUIREMENT	YES	DOES NOT	FOLLOW UP ACTION
Terminal uses lock screen and password			
Browser accessing HMIS does not save or auto fill password			
User closes HMIS when terminal is unattended			
Electronic documents with user information uses password protection			

COMPUTER REQUIREMENTS

REQUIREMENT	YES	DOES NOT	FOLLOW UP ACTION
Browser: Chrome or IE7/IE8 **			
Virus Protection			

** Firefox is not recommended by CaseWorthy, but still works for the time being.

- o Chrome for MAC/PC can be downloaded here: https://www.google.com/chrome/browser/desktop/.
- o Internet Explorer for PC here: http://www.microsoft.com/en-us/download/internet-explorer.aspx

HMIS Department Signature   **Date**

PLEASE HAVE FOLLOW UP ACTIONS COMPLETED BY: _____

Date