KING COUNTY HMIS SECURITY OFFICER COMPLIANCE CERTIFICATION CHECKLIST

HMIS Partner Agency Name:		Security Officer Name:
Semi-Annual: Sept 30 □	Semi-Annual: March 31 □	Date:

Workstation Security Standards

In partnership with King County Regional Homelessness Authority (KCRHA), Bitfocus, Inc., administers the Homeless Management Information System ("HMIS"), a shared database software application which confidentially collects, uses, and releases client-level information related to homelessness. Client information is collected in the HMIS and released to nonprofit housing and services providers (each, a "Partner Agency," and collectively, the "Partner Agencies"), which use the information to improve housing and services quality. Partner Agencies may also use client information to identify patterns and monitor trends over time; to conduct needs assessments and prioritize services for certain homeless and low-income subpopulations; to enhance inter-agency coordination; and to monitor and report on the quality of housing and services. This Compliance Certification Checklist is to be completed and certified semi-annually by the Partner Agency Security Officer for the HMIS Partner Agency named above. Each Agency workstation used for HMIS data collection, data entry, or reporting must be certified compliant. Any identified compliance issues must be resolved within thirty (30) days. Upon completion, the original signed copy of this checklist should be retained in the records of the HMIS Partner Agency named above for a minimum of seven (7) years.

For the purposes of the following Workstation Security Standards, "Authorized Person" means a Partner Agency authorized agent or representative (each, an "HMIS End User," or simply an "End User") who has completed HMIS Privacy and Security training within the past twelve (12) months. Please use the table below to confirm that each End User is in compliance with the following Standards:

1. An HMIS Privacy Statement is visibly posted at each HMIS workstation and authorized portable electronic device
2. Each HMIS workstation computer and authorized portable electronic device is in a secure location where only Authorized Persons have access.
3. Each HMIS workstation computer and authorized portable electronic device is password-protected and locked when not in use. (Changing passwords on a regular basis is recommended)
4. Documents printed from HMIS are sent to a printer in a secure location where only Authorized Persons have access.
5. Non-authorized persons are unable to view any HMIS workstation computer monitor.
6. Each HMIS workstation computer and authorized portable electronic device has antivirus software with current virus definitions (i.e., within the past twenty-four (24) hours), and each HMIS workstation computer and authorized portable electronic device has had a full system scan within the past week.

7. Each HMIS workstation computer has and uses a hardware or software firewall. Authorized portable electronic devices are for work purposes only and have a password protected lock screen. Unencrypted personally identifying information ("PII") – defined as client-level identifying information, including, without limitation, information about names, birth dates, gender, race, social security number, phone number, residence address, photographic likeness, employment status, income verification, public assistance payments or allowances, food stamp allotments, or other similar information – has not been electronically stored or transmitted in any fashion (including, without limitation, by hard drive, flash drive, email, etc.). (Encrypted hard drives are recommended)
8. Hard copies of PII (including, without limitation, client files, intake forms, printed reports, etc.) are stored in a physically secure location.
9. Each HMIS workstation computer and authorized portable electronic device password information, including each Authorized Person's user identification information, is kept electronically and physically secure.

		Standards									
	Workstation/Portable Device Location or End User Name	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**Notes/Comments**
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

Workstation/Portable Device security compliance issues identified		**Steps taken to resolve workstation / portable device security compliance**

Security Officer Certifications

(Initials) **I have verified that:**

__________ Each End User workstation / portable device has completed the Workstation Security Standards review.

__________ End User requires access to HMIS to perform her or his assigned duties.

__________ Each End User is using the most current versions of the King County HMIS Client Consent to Data Collection and ROI and the Partner Agency list.

__________ Each End User completed the King County HMIS Privacy and Security Training annually.

__________ Each End User accounts are up to date and actively being used.

__________ No unauthorized access to HMIS or confidential legally protected client data was divulged to unauthorized third parties[1].

__________ Incidents of unauthorized access has been reported to King County and impacted clients have been notified.
Date of Incident:______________ County Staff informed: _____________________________________

____ ____ ______________________________

Partner Agency Security Officer Name *Partner Agency Security Officer Signature* *Date*

____ ____ ______________________________

Partner Agency Executive Director Name *Partner Agency Executive Director Signature* *Date*

[1] As needed see the Incidents of Unauthorized Access section of the HMIS Security Plan.