KCRHA Homeless Management and Information System (HMIS) SECURITY PLAN

The Department of Housing and Urban Development (HUD), in its Proposed Rule for HMIS Requirements, requires implementation of specified security standards. These security standards are designed to ensure the confidentiality, integrity, and availability of all HMIS information; protect against any reasonably anticipated threats or hazards; and ensure compliance with all applicable standards by end users.

The King County Security Plan includes the following elements:

(1) Designated security officers;
(2) Security Audits;
(3) Physical and Technical safeguards;
(4) Incidents of Unauthorized Access;
(4) Establishing HMIS User IDs and Access Levels***;***
(5) Rescinding user and/or HMIS Partner Agency access;
(6) Implementation requirements;
(7) Computers and Electronic Devices;
(8) Encryption Management;
(9) Records; and
(10) Monitoring and Audits
Appendix 1. King County HMIS Partner Agency Technical Administrator and Security Officer Agreement
Appendix 2. Security Officer Compliance Certification Checklist

Each portion of this plan is detailed below.

Designated Security Officers

Pursuant to the HMIS Partner Agency Privacy and Data Sharing Agreement, each HMIS Partner Agency must designate a technical administrator, also referred to as the HMIS Agency Lead, (the "Partner Agency Technical Administrator") and a security officer (the "Partner Agency Security Officer") to fulfill the responsibilities enumerated below and detailed in the Partner Agency Technical Administrator and Security Officer Agreement (See Appendix 1).

King County Lead Security Officer:

1. Bitfocus, Inc., in its role as HMIS System Administrator, is the Lead Security Officer.
2. Bitfocus, Inc. will review and maintain files of Partner Agency annual compliance certification checklists.

3. Bitfocus, Inc. may conduct security audits of Partner Agencies.

Partner Agency Security Officer:

1. May be the HMIS Partner Agency Technical Administrator or another Partner Agency employee, volunteer or contractor who has completed HMIS Privacy and Security training and is adequately skilled to assess HMIS security compliance
2. Conducts security audit for any workstation or portable electronic device that will be used for HMIS data collection or entry
    a. Prior to issuing a User ID to a new HMIS End User, AND
    b. Any time an existing user moves to a new workstation or accesses a portable electronic device as part of accessing HMIS.
3. Completes the Semi-Annual Compliance Certification Checklist (see Appendix 2), and forwards the Checklist to the Lead Security Officer.
4. Assures physical and technical safeguards are in place.

Security Audits

New HMIS Partner Agency Site Security Assessment

Prior to establishing access to HMIS for any new Partner Agency, the Lead Security Officer may assess the security measures in place at the Partner Agency to protect client data. The Lead Security Officer may ask to meet with the Partner Agency Executive Director (or executive-level designee), HMIS Partner Agency Technical Administrator and Partner Agency Security Officer to review the Partner Agency's information security protocols prior to recommending that KCRHA cosign the HMIS MOU. This security review shall in no way reduce the Partner Agency's responsibility for information security, which is the full and complete responsibility of the Partner Agency, its Executive Director, and its HMIS Partner Agency Technical Administrator/Security Officer.

Semi-Annual Partner Agency Self-Audits

1. The Partner Agency Security Officer will use the HMIS Semi-Annual Compliance Certification Checklist to conduct semi-annual security audits of all Partner Agency HMIS End User workstations and portable electronic devices.
2. If areas are identified that require action due to noncompliance with these SOPs, the Partner Agency Security Officer will note these on the Compliance Certification Checklist, and the Partner Agency Security Officer and/or HMIS Agency Technical Administrator will work to resolve the action item(s) within 15 days.
3. Any Compliance Certification Checklist that includes 1 or more findings of noncompliance and/or action items will not be considered complete until all action items have been resolved. The Checklist findings, action items, and resolution summary must be reviewed and signed by the Partner Agency Executive Director or other empowered officer prior to being forwarded to the Lead Security Officer.
4. The Partner Agency Security Officer must turn in a copy of the Compliance Certification Checklist to the Lead Security Officer on a semi-annual basis.

Security Audits

1. The Lead Security Officer may schedule security audits in advance with selected Partner Agency Security Officers.
2. The Lead Security Officer will use the Semi-Annual Compliance Certification Checklist to conduct such security audits.

3. During such audits, the Lead Security Officer will randomly audit at least 10% of the workstations and/or portable electronic devices for the HMIS Partner Agency selected for review. In the event that an agency has more than 1 project site, at least 1 workstation or portable electronic devices affiliated with each project site will be audited.
4. If areas are identified that require action due to noncompliance with these standards or any element of these SOPs, the Lead Security Officer will note these on the Compliance Certification Checklist, and the Partner Agency Security Officer and/or HMIS Partner Agency Technical Administrator will work to resolve the action item(s) within 15 days.
5. Any Compliance Certification Checklist that includes 1 or more findings of noncompliance and/or action items will not be considered complete until all action items have been resolved and the Checklist findings, action items, and resolution summary has been reviewed and signed by the Partner Agency Executive Director or other empowered officer and forwarded to the HMIS Lead Security Officer.

Physical Safeguards

In order to protect client privacy it is important that the following physical safeguards be put in place. For the purpose of this section, authorized persons will be considered only those individuals who have completed Privacy and Security training within the past 12 months

1. Computer Location – A computer or portable electronic device used as an HMIS workstation must be in a secure location where only authorized persons have access. The HMIS workstation must not be accessible to clients or the public. HMIS-trained and non-HMIS trained staff may use the same computers and portable electronic devices. The Partner Agency must insure that non-HMIS trained staff receive training that incorporates all of the privacy and confidentiality requirements in this SOP document.
2. Printer location – Documents printed from HMIS must be sent to a printer in a secure location where only authorized persons have access. HMIS-trained and non-HMIS trained staff may use the same printers. The Partner Agency must insure that non-HMIS trained staff receive training that incorporates all of the privacy and confidentiality requirements in this SOP document
3. Line of Sight – Non-authorized persons should not be able to see an HMIS workstation screen. Monitors should be turned away from the public or clients in order to protect client privacy.

Technical Safeguards

<u>Workstation and Portable Electronic Device Security</u>

1. To promote the security of HMIS and the confidentiality of the data contained therein, access to HMIS will be available only through approved workstations and portable electronic devices.
2. Partner Agency Security Officer will confirm that any workstation accessing HMIS shall have antivirus software with current virus definitions (updated at minimum every 24 hours) and frequent full system scans (at minimum weekly).
3. Partner Agency Security Officer will confirm that any workstation accessing HMIS has and uses a hardware or software firewalls.

<u>Other Technical Safeguards</u>

1. The HMIS Partner Agency Security Officer shall develop and implement procedures that will prevent unauthorized users from connecting to private agency networks, whether or not they are used to access HMIS.
2. Unencrypted PII may not be stored or transmitted in any fashion—including sending file attachments by email or downloading reports including PII to a flash drive, to the End User's desktop, or to an agency shared drive. All downloaded files containing PII must be deleted from the workstation temporary files and the "Recycling Bin" emptied before the End User leaves the workstation or finishes using the portable electronic device for the day.
3. Encrypted hard drives are recommended

Incidents of unauthorized access

Should confidential and/or legally protected client data be divulged to unauthorized third parties, Agency shall be responsible for complying with all applicable federal and state laws and regulations and shall be solely responsible for the costs associated with any and all activities and actions required. Agency shall take appropriate action to address any incident of unauthorized access to HMIS. These actions must include:

1. Immediately working to remedying or mitigating the issue that resulted in such unauthorized access;
2. Notifying County within 24 hours of any incident of unauthorized access to HMIS data, or any other breach in the Agency's security that materially affects County or HMIS;
3. Upon request from County, Agency shall provide a corrective action plan that addresses the incident and is designed to ensure compliance by its officers, employees, agents, and subcontractors with the confidentiality provisions in this Agreement; and
4. Agency will be responsible for notifying all impacted clients.

Establishing HMIS User IDs and Access Levels

Agency will maintain security and confidentiality of HMIS information and is responsible for the actions of its users and for their training and supervision. Among the steps the Agency will take to maintain security and confidentiality are:

1. **Access:** Agency will permit access to HMIS or information obtained from it only to authorized Agency staff who need access to HMIS for legitimate business purposes (such as to provide services to the Client, to conduct evaluation, to administer the program, or to comply with regulatory requirements). Agency will limit the access of such staff to only those records that are immediately relevant to their work assignments.
    a. The HMIS Partner Agency Technical Administrator will ensure that any prospective End User reads, understands and signs the HMIS User Policy, Responsibility Statement and Code of Ethics.
    b. The HMIS Partner Agency Technical Administrator is responsible for ensuring that all agency End Users have completed mandatory trainings prior to being provided with a User ID to access HMIS.

c. The HMIS Partner Agency Technical Agency Administrator will always attempt to approve the most restrictive access that allows the End User to efficiently and effectively perform his/her assigned duties.
d. The HMIS Partner Agency Technical Administrator will notify Bitfocus when new users are approved for usernames and passwords.
e. The HMIS Partner Agency Technical Administrator will notify Bitfocus which access level to assign to each authorized user. Access levels may vary across HMIS Partner Agencies, depending upon their involvement with coordinated entry, contract monitoring, program and system evaluation, and other factors.
f. When the HMIS Partner Agency Technical Administrator determines that it is necessary to change a user's access level, the Partner Agency HMIS Partner Agency Technical Administrator will notify Bitfocus as soon as possible.

2. **User Policy:** Prior to permitting any user to access HMIS, user will be prompted upon logging into HMIS to sign a User Policy, Responsibility Statement & Code of Ethics Form ("User Policy"), which is found on the HMIS login page and may be amended from time to time by WA Department of Commerce.

    a. Agency will comply with, and enforce the User Policy and will inform the KCRHA immediately in writing of any breaches of the User Policy.

    b. Agency will be provided with a monthly report of their user activity so they can keep their End User accounts up to date.

    c. End User accounts are monitored at least semi-annually to assure any inactive accounts have been deactivated.

    d. Upon request, the Agency may be required to submit a written report to Bitfocus or the County with up-to-date information on all current End Users, as well as the names of former End Users who no longer have access to the HMIS.

3. **Passwords:** Agency will permit access to HMIS only with use of a User ID and password, which the user may not share with others. Written information pertaining to user access (e.g. username and password) shall not be stored or displayed in any publicly accessible location.

    a. Passwords shall be at least eight characters long and meet industry standard complexity requirements, including, but not limited to, the use of at least one of each of the following kinds of characters in the passwords: Upper and lower-case letters, and numbers and symbols. Passwords shall not be, or include, the username, or the HMIS name. In addition, passwords should not consist entirely of any word found in the common dictionary or any of the above spelled backwards. The use of default passwords on initial entry into the HMIS application is allowed so long as the default password is changed on first use. Passwords and usernames shall be consistent with guidelines issued from time to time by HUD and/or WA Department of Commerce.

    b. All user IDs are individual and passwords are confidential. No individual should ever use or allow use of a User ID that is not assigned to that individual, and user-specified passwords should never be shared or communicated in any format.

c. Temporary passwords must be changed on first use. User-specified passwords must be a minimum of 8 characters long and must contain a combination of numbers, lowercase letters, capital letters; and/or special characters (e.g. ~ ! @ # $ % ^ & * ( ) _).
d. End users may be prompted by the software to change their password from time to time.
e. End Users must immediately notify their HMIS Partner Agency Technical Administrator and/or Security Officer if they have reason to believe that someone else has gained access to their password.
f. Three consecutive unsuccessful attempts to login will disable the User ID until the account is locked for a period of time determined by the Lead Security Officer.
g. All user passwords may only be reset by Bitfocus.
h. Agency shall not give or share assigned passwords and access codes for HMIS with any other Agency, business, or individual. Each user shall request their own login and password.
i. Agency shall take due diligence not to cause in any manner, or way, corruption of the HMIS database, and Agency agrees to be responsible for any damage it may cause.

Rescinding User Access

1. End User access should be terminated within 24 hours if an End User no longer requires HMIS access to perform his or her assigned duties due to a change of job function or termination of employment. The HMIS Partner Agency Technical Administrator is responsible for notifying Bitfocus so that access can be terminated within the specified timeframe.
2. Bitfocus reserves the right to terminate End User licenses that are inactive for 90 days or more. The HMIS System Administrator will attempt to contact the HMIS Partner Agency Technical Administrator for the End User in question prior to termination of the inactive user license.
3. In the event of suspected or demonstrated noncompliance by an End User with the HMIS User Policy, Responsibility Statement and Code of Ethics or any other HMIS plans, forms, standards, policies, or governance documents, Bitfocus will deactivate the User ID for the End User in question until an internal agency investigation has been completed. The HMIS Partner Agency Technical Administrator or Security Officer will notify the County within 24 hours of any substantiated incidents that may have resulted in a breach of HMIS system security and/or client confidentiality, whether or not a breach is definitively known to have occurred.
4. In the event the HMIS Partner Agency Technical Administrator is unable or unwilling to conduct an internal investigation as described above, Bitfocus is empowered to deactivate any End User licenses pending its own investigation of an End User's suspected noncompliance with the HMIS User Policy, Responsibility Statement and Code of Ethics or any other HMIS plans, forms, standards, policies, or governance documents. King County is empowered to permanently revoke a Partner Agency's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the King County HMIS Standard Operating Procedures, or the King County HMIS Partner Agency Privacy and Data Sharing Agreement

Implementation Requirements

Partner Agencies must generate or obtain documents that cover each of the following areas in order for implementation to begin.

1. *Written Client Consent for Data Entry:* Partner Agencies must obtain a client's informed written consent prior to entering information concerning the client into the system, using the approved King County *HMIS Client Consent for Data Collection and Release of Information.* If a client does not consent, services should not be denied to the client. The agency can use the client consent refused protocol as outlined in the Partner Agency Privacy and Data Sharing Agreement in appropriate cases.

2. *Background Check Procedures*: Each Partner Agency is responsible for conducting its standard employment background check for the HMIS designated Lead(s) and Security Officer(s).

3. *Staff Confidentiality Agreements*: Each Partner Agency must develop a procedure for informing staff of client confidentiality. All users of the system must complete general Clarity Human Services user training prior to being authorized to use the system. In addition, all users of the system are required to attend confidentiality and privacy training.

4. *Information Security Protocols*: Internal policies must be developed at each Partner Agency to establish a process for the detection and prevention of a violation of any HMIS information security protocols. This includes adopting written policies concerning data security procedures, and data breach procedures.

5. *Virus Prevention, Detection, and Disinfection Protocols*: Participation in the HMIS requires that Partner Agencies develop procedures intended to assure that computers with access to the HMIS run updated anti-virus software.

6. *Data Collection Commitment*: Participation in the HMIS requires that all Partner Agencies collect minimum data elements on all consenting clients in accordance with HUD requirements, unless an exception has been granted by King County.

7. *Connectivity*: Once implementation has begun, each Partner Agency agrees to use its reasonable best efforts to maintain appropriate internet connectivity in order to continue participation.

8. *Maintenance of Onsite Computer Equipment and/or Portable Electronic Devices.* Each Partner Agency agrees to use its reasonable best efforts to maintain computer equipment and/or portable electronic devices to the extent required to continue participation.

9. *Conversion of Legacy Data or Links to Other Systems*: Partner Agencies using other systems or desiring to have legacy data converted must provide resources and processes that enable conversion without cost to Bitfocus or King County.

Computers and Electronic Devices

Security for data maintained in HMIS depends on a secure computing environment. Computer and device security is adopted from relevant provisions of the Department of Housing and Urban Development's (HUD) "Homeless Management Information Systems (HMIS) Data and Technical Standards Notice" (Docket No. FR 4848-N-01; see https://www.hudexchange.info/resource/1318/2004-hmis-data-and-technical-standards-final-notice/) until the HMIS Proposed Rule is finalized and replaces the current Standards: https://www.hudexchange.info/resource/1967/hearth-proposed-rule-for-hmis-requirements/. Agencies are encouraged to directly consult that document for complete documentation of HUD's standards relating to HMIS.

Agency agrees to allow access to HMIS only from computers and Electronic Devices which are:

1. Owned by the Agency for the purpose of accessing and working with HMIS (no personal devices);
2. Secured and use of such device complies with all parts of this Agreement;
3. Protected from viruses by commercially available virus protection software;
4. Protected with a software or hardware firewall;
5. Maintained to insure that the operating system running the computer or electronic device used for the HMIS is kept up to date in terms of security and other operating system patches, updates, and fixes;
6. Accessed through web browsers with 256-bit encryption (e.g., Internet Explorer, version 11.0). Some browsers have the capacity to remember passwords, so that the user does not need to type in the password when returning to password-protected sites. This default shall ***not*** be used with respect to WA Department of Commerce' HMIS; the end-user is expected to physically enter the password each time he or she logs on to the system; and
7. Staffed at all times when in public areas. When computers and electronic devices are not in use and staff is not present, steps should be taken to ensure that the computers, electronic devices, and data are secure and not publicly accessible. These steps should minimally include: Logging off the data entry system, physically locking the computer or electronic device in a secure area, or shutting down the computer or electronic device entirely.

Encryption Management

Encryption General: All information should be encrypted in the database per HUD standards. All connections to the HMIS should be encrypted to HUD standards or higher. Encryption should be sufficient to prevent unauthorized personnel from accessing confidential information for any reason.

Encryption Management: In the event that system-wide data decryption becomes necessary, the System Performance Committee must obtain the written authorization of every Partner Agency's Executive Director.

Records

Agency and County will maintain records of any unauthorized disclosures (aka data breach) of Client identifying information either of them makes of HMIS information for a period of **seven** years after such disclosure. On written request of a Client, Agency and County will provide an accounting of all such disclosures within the prior **seven**-year period.

Monitoring and Audits

County reserves the right to monitor agency privacy practices and compliance with the provisions of this agreement through document review and site visits. Monitoring and audit visits may be performed by County staff or by Bitfocus.

Appendix 1. Partner Agency Technical Administrator and Security Officer Agreement

King County Homeless Management and Information System (HMIS)

PARTNER AGENCY TECHNICAL ADMINISTRATOR AND SECURITY OFFICER AGREEMENT

This Agreement is entered into by and between King County Regional Authority on Homelessness ("KCRHA") and the undersigned parties in order to establish the responsibilities described herein and to confirm compliance with required background check requirements as set forth below. KCRHA reserves the right to request access to the Partner Agency records and place of business for monitoring compliance with this Agreement.

The King County Homeless Management Information System ("HMIS") is a shared database and software application which confidentially collects, uses, and shares client-level information related to homelessness in King County. On behalf of the King County Continuum of Care ("CoC"), HMIS is administered by the County and Bitfocus, Inc. ("Bitfocus") in a software application called Clarity Human Services ("Clarity").

Clients must consent to the collection, use, and release of their information, which helps the CoC to provide quality housing and services to homeless and low-income people. Client information is collected in HMIS and released to housing and services providers (each, a "Partner Agency," and collectively, the "Partner Agencies"), which include community-based organizations and government agencies. Partner Agencies use the information in HMIS: to improve housing and services quality; coordinate referral and placements for housing and services; 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 delivery, impact, and quality of housing and services.

Pursuant to the HMIS Standard Operating Policies and the HMIS Security Plan, each HMIS Partner Agency must designate a technical administrator, also referred to as the HMIS Agency Lead, (the "Partner Agency Technical Administrator") and a security officer (the "Partner Agency Security Officer") to fulfill the responsibilities enumerated below. Furthermore, the Partner Agency Technical Administrator and the Security Officer may be the same person.

The **Partner Agency Technical Administrator** is responsible for:

- Overseeing the Partner Agency's compliance with the most recent versions of the Partner Agency Privacy and Data Sharing Agreement and Memorandum of Understanding and all other applicable plans, forms, manuals, standards, agreements, policies, and governance documents;
- Detecting and responding to violations of any applicable HMIS plans, forms, manuals, standards, agreements, policies, and governance documents;
- Serving as the primary contact for all communication related to the HMIS at the Partner Agency and forwarding such information to all Partner Agency authorized agents and representatives ("HMIS End Users," or simply "End Users") as she or he deems

appropriate;

- Ensuring complete and accurate data collection by Partner Agency End Users as established by HMIS plans, forms, manuals, standards, agreements, policies, and governance documents;
- Providing first-level End User support;
- Requesting End User account access;
- Ensuring the Partner Agency maintains adequate internet connectivity;
- Maintaining complete and accurate Partner Agency and program descriptor data in HMIS;
- Working with Bitfocus to configure provider preferences (including assessments, referrals, services, etc.) in HMIS;
- Completing agency-level reporting and/or supporting agency programs according to applicable reporting standards established by the U.S. Department of Housing and Urban Development ("HUD") and local funders; and
- Performing authorized imports of client-level data.

The **Partner Agency Security Officer** is responsible for:

- Conducting a complete and accurate semi-annual review of the Partner Agency's compliance with all applicable plans, forms, manuals, standards, agreements, policies, and governance documents;
- Completing the HMIS Semi-Annual Compliance Certification Checklist (the "Checklist"), and forwarding the Checklist to the HMIS System Administrator, as defined therein;
- Continually monitoring and maintaining security of all staff workstations and devices used for HMIS data entry which includes, but is not limited to, ensuring workstation computers are password-protected and locked when not in use, ensuring that non-authorized persons are unable to view any HMIS workstation computer monitor, and ensuring that documents printed from HMIS are sent to a printer in a secure location where only Authorized Persons have access;
- Safeguarding client privacy by ensuring Partner Agency and Partner Agency End User compliance with all HUD Rules;
- If the Agency agrees to allow access to HMIS from agency computers and Portable Electronic Devices, assure compliance with the HMIS Partner Agency Privacy and Data Sharing Agreement standards.
- Investigating potential and actual breaches of either HMIS system security or client confidentiality and security policies, and immediately notifying the County and the System Administrator, as defined in the Checklist, of substantiated incidents;
- Developing and implementing procedures for managing new, retired, and compromised local system account credentials;
- Developing and implementing procedures that will prevent unauthorized users from connecting to any private Partner Agency networks;
- Ensuring all Partner Agency End Users sign and execute the HMIS End User Agreement;

and

- Ensuring all Partner Agency End Users complete the required New User General Training, and Annual Security and Privacy Training, as well as all other mandatory trainings; retaining documentation of training completion; and forwarding such documentation to the HMIS System Administrator.

As required by HUD, the Partner Agency shall perform a background check on any End User who is:

- Designated as a Partner Agency Technical Administrator,
- Designated as a Partner Agency Security Officer, or
- Granted agency manager-level access in HMIS.

The Partner Agency Executive Director shall ensure that such background checks are completed and shall approve the results before the End User is (i) granted a Technical Administrator or Security Officer title, or both, as applicable, or (ii) granted agency manager- level access in HMIS. The results of the background check shall be retained by the Partner Agency in the End User's personnel file. A background check may be conducted once for each End User unless otherwise required.

King County Homeless Management and Information System (HMIS)

PARTNER AGENCY TECHNICAL ADMINISTRATOR AND SECURITY OFFICER AGREEMENT

Partner Agency Name: _____

On behalf of the Partner Agency, I will be fulfilling the role of (check all that apply):

- ❑ Partner Agency Technical Administrator
- ❑ Partner Agency Security Officer

By signing, I agree to fulfill all of the responsibilities enumerated above for my role.

_____

HMIS End User Printed Name

_____ _____

HMIS End User Signature Date

I certify that a background check has been completed on the End User named above, that I approve the results, and that a copy of the results is filed with the End User's personnel file.

Further, I certify that Partner Agency will ensure the End User named above performs each of these functions.

_____

Partner Agency Executive Director Printed Name

_____ _____

Partner Agency Executive Director Signature Date

Appendix 2. Security Officer Compliance Certification Checklist

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, 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 KCRHA 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 KCRHA 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.