One Appendix D form must be completed, signed and submitted to DSS annually by each Contributing HMIS Organization (CHO). It provides DSS with information on information on key CHO contacts and CHO HMIS software and certifies CHO compliance with administrative, technical, and security responsibilities and requirements.

Appendix D: NYC HMIS Administrative, Software Certification and Security Checklists

Contributing HMIS Organization (CHO) Name: _____

A. Identification and Contact Information

You are required to notify DSS within 15 business days if one of these contacts changes.

Executing Officer (Executive Director or Chief Executive Officer)

a. Name _____
b. Title _____
c. Phone _____
d. Email _____

CHO HMIS Administrator (may be the same as the Executing Officer)

a. Name _____
b. Title _____
c. Phone _____
d. Email _____

Backup CHO HMIS Administrator

a. Name _____
b. Title _____
c. Phone _____
d. Email _____

CHO Security Contact

a. Name _____
b. Title _____
c. Phone _____
d. Email _____

B. Is AWARDS software used as the CHO's project-level HMIS-compliant database?

☐ Yes
☐ No. If no, identify the software and version in use for collecting HMIS information:

_____

You are required to notify DSS and Foothold Technology in advance of any changes in this software.

C. Key Responsibilities

CHO HMIS Administrator's duties include:

- Providing a single point of communication between the CHO End Users and the HMIS Lead around HMIS issues;
- Ensuring the stability of the CHO connection to the Internet and the data warehouse, either directly or in communication with other technical professionals;
- Maintaining awareness of industry standards;
- Training CHO End-Users in data collection, security and privacy policies and procedures, and assuring End Users receive any requisite training provided by HMIS Lead for End Users;
- Providing support for generating organization reports;
- Managing CHO user names and passwords for project level HMIS compliant system;
- Monitoring compliance with standards of client confidentiality and data collection, entry, and retrieval; and
- Participating in CHO HMIS training.

Security Contact duties include, but are not limited to:

- Annually review the Section E of this appendix, Assurances of Consistency with Security Plan
- Security Certification Checklist document, test the CHO security practices for compliance, and work with appropriate vendors (where applicable) to confirm security compliance of the project-level HMIS-compliant system;
- Using this Security Certification Checklist document, certify that the CHO adheres to the Security Plan or provide a plan for remediation of non-compliant systems, including milestones to demonstrate elimination of the shortfall over time;
- Communicate any security questions, requests, or security breaches to the DSS System Administrator and/or DSS Security Officer;
- Communicate security-related HMIS information to the CHO's End Users;
- Complete any CoC-mandated security training offered by the HMIS Lead; and
- Additional duties as specified in the HMIS Participation Agreement.

D. Assurances of Consistency with Policies and Procedures

Each CHO is required to establish and follow the following policies and practices. If the requirement cannot be met at the time of execution of the Participation Agreement, you must indicate a date not later than three months execution date by which you will have met the requirement. At that time, you will be required to submit an updated version of this form demonstrating your compliance**. <u>If you achieved full compliance last year and maintain such compliance to date, you may skip this checklist and sign below.</u>**

Administrative and Software Certification Checklist			
#	Required Policy	Meets Requirement (Yes/No)	If no, date by which compliance will be met
I	**Administrative Requirements**		
1	CHO has a policy detailing its internal communication practices for HMIS matters consistent with **Section 3.2.4 CHO Communications** of the NYC HMIS policies and procedures.		
2	CHO has a policy for granting access to its project-level HMIS-compliant system's End Users consistent with **Section 3.6.1 User Levels and Activation** of the policies and procedures.		
3	The CHO has adopted the minimal End User Agreement provided by the NYC HMIS Lead		
3.1	If not, CHO's End User Agreement otherwise meets the minimum requirements established in **Section 3.6.2 CHO User Agreement** of the policies and procedures.		
4	CHO End User Agreements are signed and on file for all staff who access the project-level HMIS-compliant system. See Appendix G.		
5	CHO has a policy for managing the breach of End User Agreement that meets the minimum standards outlined in **Section 3.6.3 User Agreement Breach** of the policies and procedures.		
6	Each CHO End User has been trained on system use, privacy, security, and data collection requirements consistent with training sessions provided by the HMIS lead and the NYC HMIS policies and procedures, consistent with **Section 3.7 Training Requirements** of the policies and procedures.		
7	The CHO has adopted the minimal standard Privacy Policy provided by the NYC HMIS Lead		
7.1	If not, CHO's Privacy Policy otherwise meets the minimum requirements established in **Section 6. Privacy Policy** of the policies and procedures.		
8	The CHO's Privacy Policy is posted on the CHO's website.		
9	A sign including the required language described in **Section 6.6.2 Informed Client Consent** of the policies and procedures is posted at all intake desks or other location where data collection occurs.		

Administrative and Software Certification Checklist			
#	Required Policy	Meets Requirement (Yes/No)	If no, date by which compliance will be met
10	The CHO has a policy requiring that all client data is entered into the system as per the requirements of the data collection point, and for "update " within, at most, three business days of a client interaction, consistent with **Section 7.4.1 Timeliness.**		
10.1	The CHO has a policy for conducting logic checks to validate the accuracy of the data in its project-level HMIS-compliant system and regularly comparing universal and program specific data elements to available paper records and updating/correcting missing or inaccurate data, consistent with **Section 7.4.3 Accuracy** of the policies and procedures.		
II	**Software and Technical Requirements**		
1	CHO's project-level HMIS compliant client data collection system is a relational database capable of recording client data from a limitless number of service transactions and preserving all required historical data as outlined in **Section 7. Data Quality Plan** of the NYC HMIS policies and procedures and the current HUD HMIS Data Standards.		
2	System has the capacity to collect data on system use for the purposes of data quality and security, including login attempts, search parameters, and incidents of changes made to records.		
3	System has the capacity to collect all project descriptor, universal, program-specific, and metadata elements as specified in **Section 7. Data Quality Plan** of the policies and procedures.		
4	System has the capacity to meet technical security requirements specified in **Section 4. HMIS Security Plan** of the policies and procedures and technical privacy requirements specified in **Section 6. Privacy Policy** of the policies and procedures.		
5	System has the capacity to transfer data directly to the Data Warehouse or export a CSV file of all required data elements consistent with current HUD HMIS CSV Format documentation for the purposes of upload to the Data Warehouse.		

If the software used for data collection changes, DSS and Foothold Technology must be notified in advance.

E. Assurances of Consistency with Security Plan

Each CHO is required to meet the following security requirements. If the requirement cannot be met at the time of execution of the Participation Agreement, you must indicate a date not later than three months execution date by which you will have met the requirement. At that time, you will be required to submit an updated version of this form demonstrating your compliance. **If you achieved full compliance last year and maintain such compliance to date, you may skip this checklist and sign below.**

Security Checklist			
#	Required policy	Meets Requirement (Yes/No)	If no, date by which compliance will be met
1	CHO has a policy regarding conducting background checks and hiring individuals with criminal justice histories consistent with **Section 4.4.1 Criminal Background Verification** of the HMIS policies and procedures.		
2	Documentation is on file that each End User has completed security training prior to gaining system access consistent with **Section 4.4.2 Annual Security Training** of the HMIS policies and procedures.		
3	CHO has established procedures protecting the physical security of the facilities and media in which the data is stored or has provisions in its contract with the provider of the project-level HMIS-compliant system to meet the minimum standards established in **Section 4.6.1 Physical Security** of the policies and procedures (including temperature control and surge suppressors).		
4	All HMIS data is copied to another medium and stored in a secure off-site location at least weekly or the CHO has included provisions in its contract with the provider of the project-level HMIS-compliant system to meet the minimum standards established in **Section 4.6.2 Backup** of the policies and procedures.		
5	Restoration of backed-up data has been tested within the last 12 months.		
6	CHO has policies and procedures that specify how the software provider or system operator will address all reported bugs within three business days and specify that, if customer intervention is required, the CHO is responsible for ensuring that all enhancements, upgrades and bug fixes are applied promptly upon release by the software provider, consistent with **Section 4.6.3 Software Security** of the policies and procedures.		

Security Checklist			
#	Required policy	Meets Requirement (Yes/No)	If no, date by which compliance will be met
7	CHO maintains and follows procedures to install, update and use anti-virus software on all CHO-owned devices used to access the project-level HMIS-compliant system, consistent with **Section 4.6.3 Software Security** of the policies and procedures.		
7.1	Identify the anti-virus software in use		
7.2	Specify the frequency with which the software is updated and the frequency with which the devices will be scanned. At minimum, update of the software and scan the relevant devices for viruses and malware must be done monthly		
8	CHO has established procedures for protecting HMIS data behind a firewall or has provisions in its contract with the provider of the project-level HMIS-compliant system to meet the minimum standards established in **Section 4.6.4 Boundary Protection** of the policies and procedures.		
9	The project-level HMIS-compliant system's password requirements have been tested within the last 12 months and meet the minimum standards established in **Section 4.6.5 System Access User Authentication and Passwords** of the policies and procedures.		
10	The following username protections have been formalized in a written procedure and tested within the last 12 months:		
10.1	Defines a period of inactivity after which the user's workstation must be automatically logged out of the system and/or locked out of the computer, requiring a username and password to resume use of the project-level HMIS-compliant system.		
10.2	Requires that any default passwords provided for initial entry into the application be changed on first use.		
10.3	Defines how individual users' forgotten passwords will be reset and communicated to the user.		
10.4	Specifies how unsuccessful login attempts will be handled and confirm that the project-level HMIS-compliant system will maintain an auditable record of all attempted logins. At maximum, 5 consecutive unsuccessful login attempts must lock a user out of the system for at least 30 minutes.		
11	CHO has a procedure for accessing its project-level HMIS-compliant system through networks and devices not owned or managed by the CHO consistent with **Section 4.6.5 System Access User Authentication and Passwords** of the policies and procedures.		
12	CHO's project-level HMIS-compliant system maintains audit records of user activity, including attempted logins, searches conducted by each user, records altered by each user, and records added by each user.		
13	CHO has a policy to monitor audit records regularly for security breaches at least monthly, consistent with **Section 4.6.6 Audit Controls** of the policies and procedures.		

Security Checklist			
#	Required policy	Meets Requirement (Yes/No)	If no, date by which compliance will be met
14	CHO has a policy specifying that End Users may not electronically transmit any unencrypted client-level data across a public network, consistent with requirements associated with Personally Identifying Information (PII) described in **Section 4.7 PII Management and Disposal** of the policies and procedures.		
15	CHO has a policy specifying any hard drives or removable media on which PII is stored will be encrypted and that users are prohibited from storing client-level data on any personally owned media, consistent with **Section 4.7 PII Management and Disposal** of the policies and procedures.		
16	CHO has a policy describing how hard-copy and electronic client-level data will be protected and disposed of, consistent with **Section 4.7 PII Management and Disposal** of the policies and procedures and industry standards for digital media disposal.		
17	CHO has a policy specifying the thresholds and process for security incident reporting, consistent with **Section 4.8 Security Incidents** of the policies and procedures.		
18	CHO maintains records of any and all security breaches to the project-level HMIS-compliant system.		
19	Each CHO will have a plan in place for maintaining and recovering access to its own data, consistent with **Section 5** Disaster Recovery of the policies and procedures.		

We affirm and certify that this organization, _____ _____, achieved full compliance last year (and has a completed checklist on file with DSS) for all requirements listed as "CHO" (Contributing HMIS Organization) responsibilities in the U.S. Department of Housing and Urban Development Homeless Management Information System (HMIS) Data and Technical Standards Final Notice and with the NYC CCoC HMIS Policies and Procedures. This certification is incorporated into the HMIS Participation Agreement. Any misrepresentation of the foregoing may result in termination of the Participation Agreement.

OR

We affirm and certify the above information is true and that this organization, _____ _____, is in full compliance with all requirements listed as "CHO" (Contributing HMIS Organization) responsibilities in the U.S. Department of Housing and Urban Development Homeless Management Information System (HMIS) Data and Technical Standards Final Notice and with the NYC CCoC HMIS Policies and Procedures or will be in compliance within the timeframes stated above. This certification is incorporated into the HMIS Participation Agreement. Any misrepresentation of the foregoing may result in termination of the Participation Agreement.

CHO HMIS System Administrator

Signature _____

Date _____

Printed Name _____

Title _____

CHO HMIS Security Contact

Signature _____

Date _____

Printed Name _____

Title _____

Executing Officer (Executive Director or Chief Executive Officer)

Signature _____

Date _____

Printed Name _____

Title _____