E.5

HOMELESS CONTINUUM OF CARE OF STARK COUNTY SYSTEM SECURITY PLAN

I. Background

A. The Department of Housing and Urban Development (HUD)'s Interim Rule requires implementation of security standards. Security standards are directed to ensure the confidentiality, integrity, and availability of all HMIS and Coordinated Entry System (CES) or System information; protect against any reasonably anticipated threats or hazards to security; and ensure compliance by end users.

B. Written policies and procedures must comply with all applicable Federal law and regulations, and applicable state or local governmental requirements.

II. Policy

A. HCCSC HMIS Committee shall annually review and revise policies and agreements that protect and control access to electronic HMIS information.

III. Administrative Safeguards

A. Security Officer:

1. HCCSC HMIS and each Participating Agency must designate an HMIS Security Officer to be responsible for ensuring compliance with applicable security standards. For HCCSC HMIS, this person shall be the System Administrator from the Lead HMIS Agency.

B. Workforce Security

1. Each Participating Agency shall conduct background checks on all Users. Unless otherwise required by HUD, all background checks may be conducted only once for all Users.

C. Security Training and Follow-Up:

1. HCCSC HMIS shall ensure that all Users receive security training prior to being given access to the HMIS, and that the training curriculum reflects the policies of the CoC and the requirements of this plan. HMIS security training is required annually.

D. Reporting Security Incidents:

1. All Participating Agency security breaches involving access to HMIS data must be documented, logged, and reported to HCCSC HMIS within one business day.

E. Disaster Recovery Plan:

1. The HMIS Software Vendor and Lead HMIS Agency must develop, maintain, and make available the Disaster Recovery Plan for all HMIS data.

F. Annual Security Review:

1. HCCSC HMIS shall complete an annual security review to ensure the implementation of the security requirements for itself and Participating Agencies.

G. Contracts and Other Arrangements:

1. HCCSC HMIS shall retain copies of all contracts and agreements executed as part of the administration and management of the HMIS or required to comply with the requirements of the HMIS security standards.

IV. Physical Safeguards

A. Access to areas containing equipment, data, and software will be secured. All identifying information will be strictly safeguarded in accordance with the latest technology available provided by the HMIS Software Vendor. All data will be securely protected to the maximum extent possible. Ongoing security assessments to include penetration testing will be conducted on a regular basis.

B. Scope:

1. Server hardware physical security (Locked office)
2. Server software security (Location Access Controls and Username accounts)
3. Network software security (Firewall protection)
4. Network hardware physical security (Locked office)
5. Wire security (SSL and VPN Encryption)
6. Client data security (SSL and VPN Encryption)
7. 7. Remote data storage

C. HCCSC HMIS shall annually review and revise all physical measures, policies and procedures to protect the HMIS.

V. Technical Safeguards

A. All computing resources that will be used to access the HMIS will satisfy the following measures:

1. Anti-virus and malware protection shall be installed on each workstation used to access the HMIS, whether accessed from the Participating Agency or remotely.

2. Devices will be protected at all times by a firewall.

3. User access through the internet will be controlled at all times. Participating Agency or User access may be suspended or revoked for suspected or actual violation of the security protocols.

B. All potential violations of any security protocols will be investigated by the HMIS Security Officer.

C. Any User found to be in violation of security protocols will be sanctioned accordingly. Sanctions may include but are not limited to: a formal letter of reprimand, suspension of system privileges, revocation of system privileges, termination of employment and criminal prosecution.

D. Any agency that is found to have consistently and/or flagrantly violated security protocols may have their access privileges suspended or revoked.

E. All sanctions can be appealed to the HCCSC Board of Directors.