



Safe Harbors HMIS: Security Policy

Effective 08/26/2005

Table of Contents Page

- Purpose 3
- Policy Statement 4
- Governing Principles 4
 - To Protect Data Integrity 4
 - To Protect Access to Client Records 4
 - To meet HIPAA and HUD Requirements 4
 - To Avoid Computer Crime 5
- Roles and Responsibilities 5
 - Safe Harbors System Owner/Operator — System Management 5
 - Safe Harbors Security Officer 5
 - Agency System Management 5
 - Agency Data Custodians 6
 - Agency Users 6
- Security Areas 7
 - Systems and Network Security 7
 - Web Based System Security 7
- Policy Requirements for Services 7
 - Authentication 7
 - Authorization 8
 - Confidentiality 8
 - Integrity 8
 - Availability 8
 - Non-repudiation (attribution) 8
 - OS Maintenance 8
 - Firewalls and Virus Protection 8
 - Physical Security 8
 - Personnel Security Measures 9
 - Data Security and Data Integrity 9
- Technical Guidelines 10
- Data Sharing 10
- Defaults & Policies 10
- Policy Enforcement 10
 - Audits 11
 - Applicability 11
- APPENDIX A 12
 - Sign-on Warning 12
 - Report Print Warning 12
 - Printed Document Top of Page Warning 12
 - Screen Watermark & Screen Print Warning 13

Security Policy

Purpose

The purpose of this policy is to help ensure the security and availability of information technology systems and networks. It also helps ensure confidentiality, integrity and availability of electronic information captured, maintained, and used by the City of Seattle. It provides direction for compliance to federal and state regulations, specifies appropriate practices, and defines custodial responsibilities for records associated with City operations. This policy should be used as a foundation document for all standards, procedures, and guidelines that are developed and implemented by the City related to information systems security.

Definitions

Agency: An organization working with Safe Harbors signing an Agency Partner Agreement thereby agreeing to follow Safe Harbors policies and procedures. The Agency Partner Agreement is in effect for all related programs within an agency.

Client: A person who applies for or receives services from a Safe Harbors partner agency.

Client-identifying Confidential Information: Personal information that identifies a client, including protected health information, and that state or federal laws protect from improper disclosure or use.

Confidential Information: Information that is protected by state or federal laws, including information about clients that is not available to the public without legal authority.

Disclosure: The release, transfer or provision for access to information outside Safe Harbors.

HIPAA: The Health Insurance Portability and Accountability Act of 1996, 42 USC 1320d et. seq.

HMIS: Homeless Management Information System — a web based computer system managed by Safe Harbors staff that collects client identified confidential information with services received and outcomes achieved by the clients.

HUD: Federal Department of Housing and Urban Development.

Privacy Policy: Safe Harbors policy developed to comply with federal and state privacy requirements. The individuals responsible for implementing and managing this policy are Safe Harbors staff, Safe Harbors partner agencies, and partner agency staff using the Safe Harbors HMIS.

Safe Harbors: A project jointly funded by City of Seattle, King County and United Way of King County to implement HMIS required by Congressional directive.

Safe Harbors Partner Agency: An agency that signs the Safe Harbors Partner Agency Agreement thereby agreeing to abide by all conditions required of any

agency using the HMIS and providing services to homeless people, referred to as clients.

Policy

Policy Statement

It is the policy of the City of Seattle, under whose jurisdiction the HMIS System resides, to ensure the security, availability, and integrity of its information systems, networks and data. All Users of City computing services, resources and data are required to support this effort by complying with all established policies, guidelines, and procedures. This includes compliance with all related federal and state statutes and regulations as required.

Prominent among these requirements is the City's commitment to ensure that its treatment, custodial practices, and uses of client-identifying confidential information are in full compliance with all related statutes and regulations, and the City's core values of maximizing trust, integrity and respect for privacy.

It also is critically important to secure systems and networks from unauthorized access, to prevent their misuse, disruption and destruction.

This general policy is the foundation for all other policy statements, guidelines, and procedures that are developed and implemented within City computing environments.

Governing Principles

To Protect Data Integrity

Data is the most valuable and most sensitive asset of the Safe Harbors system. It is our policy to protect this asset from accidental or intentional modification, disclosure or destruction. Our data security program must be a well organized and cost effective plan, which formulates the safeguards to protect client, agency and policy level interests. Safe Harbors System Administrator is responsible for controlling access to the system and will use access controls to carry out this responsibility.

To Protect Access to Client Records

The Client Privacy policy is designed to protect against recording information in unauthorized locations or systems. Only staff who work directly with clients or who have administrative responsibilities will receive authorization to look at, enter, print or edit client records.

To meet HIPAA and HUD Requirements

The data collected by this system may be considered personally identifiable information covered by HIPAA. Because of this, every effort must be made to protect this information and treat it as confidential to the extent of the law.

To Avoid Computer Crime

The Safe Harbors Policy is to minimize any computer crime and prosecute wherever possible. Computer crimes violate state and federal law as well as the Safe Harbors system Security Policy. They include but are not limited to: unauthorized disclosure, modification or destruction of data, programs or hardware; theft of computer services; illegal copying of software; invasion of privacy; theft of hardware, software, peripherals, data or printouts; misuse of communication networks; promulgation of malicious software such as viruses; and breach of contract. Perpetrators may be prosecuted under state or federal law, held criminally or civilly liable for their actions, or both. Safe Harbors staff and authorized agencies must comply with license agreements for copyrighted software and documentation. Licensed software must not be copied unless the license agreement specifically provides for it or with written permission from the vendor. Copyrighted software must not be loaded or used on systems for which it is not licensed. Pirated software (i.e. unauthorized copies) may not be loaded onto any Safe Harbors computer.

Roles and Responsibilities

Safe Harbors System Owner/Operator — System Management

Safe Harbors, as a system, will be 'owned' by the Safe Harbors Partners (City of Seattle, King County and United Way of King County). There are responsibilities associated with that 'ownership' as defined in the City of Seattle Information Systems Security Policy (Section 5.3). The responsibilities will be acted out by overall System Managers in charge of system-wide functions including:

- System auditing
- System-wide data integrity
- Enforcing policies and standards
- Implementing backup, recovery and data retention

Safe Harbors Management

Safe Harbors Management is ultimately responsible for establishing security policy, and auditing compliance.

Agency System Management

Agency Administrator plays a critical role in the protection of Safe Harbors data. Their responsibilities for systems and information security are included in the City of Seattle Information Systems Security Policy in Section 5.3.

Some agencies in our Continuum of Care have Information Department Staff who could also serve as Agency Administrator. Roles and responsibilities for the Agency Administrator include the following:

- There will be multiple levels of access to the Safe Harbors system. The appropriate access to the Safe Harbors system will be determined for each user by the Agency Administrator. This determination should be based on each user's job function as it will relate to the Safe Harbors system data entry and retrieval (i.e. role based security).
- The Safe Harbors Agency Administrator will be responsible for detecting and responding to violations of the Safe Harbors Policies or Agency Policies and Procedures.
- The Agency Administrator will develop strict procedures for issuing, altering and revoking access privileges.
- The Agency Administrator will perform system auditing (within Agency) and ensure Agency-wide data integrity.
- The Administrator will enforce agency information system policies and standards.
- The Agency Administrator will implement backup, recovery and data retention procedures (within their agency).
- The Agency Administrator will provide direct authority and control over the management and use of specific information in accordance with procedures as documented in the City of Seattle Information Systems Security Policy.

The Executive Director of each Safe Harbors Agency will be accountable for all agency staff that generate, have access to, or release/transmit client-level data stored in the system software to ensure adherence to the operating policies outlined in this document.

Agency Users

Users are bound by the City of Seattle Information Systems Security Policy Section 5.5 and shall comply with same. All Users have a critical role in the effort to protect and maintain City information systems and data. Users of City computing resources and data have the following responsibilities:

- All users must change their Safe Harbors passwords at a pre-set interval of 180 days.
- Users **must** log off the Safe Harbors system or lock their workstation when leaving their work station **AND** close the Internet browser to prevent someone from viewing the last client screen.
- All users of the Safe Harbors system must read and sign the User Code of Ethics prior to applying for access to Safe Harbors. Partner Agencies must maintain copies of these signed forms for all their Safe Harbors system Users and send copies of all signed forms to Safe Harbors.
- Support compliance with all federal and state statutes and regulations.
- Comply with all City and departmental policies and guidelines
- Protect and never share access accounts, privileges, and associated passwords.

- Maintain the confidentiality of sensitive information to which they are given access privileges.
- Accept accountability for all activities associated with the use of their user accounts and related access privileges.
- Ensure that use of City computers, email, Internet access, computer accounts, networks, and information stored, or used on any of these systems is restricted to authorized purposes and defined use limitations.
- Report all suspected security and/or policy violations to an appropriate authority (e.g. manager, supervisor, system administrator or the CISO) and the Safe Harbors System Administrator.

Users are also required to follow all specific policies, guidelines and procedures established by their agencies with which they are associated and that have provided them access privileges.

Security Areas

Systems and Network Security

To protect the availability and integrity of the Safe Harbors system, all computing systems accessing the Safe Harbors system shall comply with the minimum security measures and practices outlined in the City of Seattle Information Systems Security Policy Section 6.5.1. Also, the servers used to store the data as well as the application will be protected in terms of physical and system access control, firewalls and virus protection, as well as a backup and disaster recovery plan.

Web Based System Security

Safe Harbors HMIS is an application accessed via a web browser. Therefore, in order to protect the security, availability and integrity of the system and data, it is important to abide by the Minimum Network Security Measures and Practice outlined in the City of Seattle Information Systems Security Policy Section 6.5.2

Policy Requirements for Services

Authentication

Authentication is proof of identity. All system access accounts for Users must be based on a unique identifier and no shared accounts are allowed except where authorized as an exception by the Safe Harbors System Administrator.

Username and password are required to access the HMIS. Passwords should be at least 8 characters long & meet industry standard complexity requirements. Passwords must be changed at pre-set intervals, and usernames and passwords must not be shared.

Authentication must be 2 tier minimum. A PKI issued certificate coupled with user account and password is a two-layered authentication scheme.

Authorization

Authorization is the provision of specific permissions or authority to have access. Access control measures required for establishing Users' access to any City computing resources shall be commensurate with the functional nature and degree of criticality of the computer systems, network resources, and data involved.

All Users' system access will be based on the "principle of least privilege" and the "principle of separation of duties."

Confidentiality

Confidentiality ensures the level of privacy of specific information. The HMIS application provides for this by encrypting the data sent over the internet. In addition, every effort must be made through policies to ensure that any personal identifiable data entered remains so, especially at the intake point.

Integrity

Integrity provides assurance of an unaltered or unmodified state of information. Integrity is provided by using digital certificates, signatures, and other safeguards to ensure that the data arrives where it is supposed to unaltered.

Availability

Availability ensures that there is no delay or denial of authorized services or loss of data processing capabilities. This takes into account things such as virus protection, firewalls, intrusion detection, management of operating system updates, backup and recovery, and physical security to make sure that the application and database are available for the agencies to use.

Non-repudiation (attribution)

Non-repudiation provides for proof of receipt. This is accomplished through digital certificates.

OS Maintenance

Plans must be in place to keep the PCs used to access the application updated with the latest security and other updates for the operating system.

Firewalls and Virus Protection

Each agency will have firewall protection on their networks or PCs accessing the internet and the application. Virus protection must also be in place on each PC, as well as an update subscription to maintain the virus code base.

Physical Security

In order to ensure that unauthorized persons cannot physically access servers, physical security measures and objectives will be implemented where applicable and

appropriate to protect Safe Harbors computing and network assets as outlined in the City of Seattle Information Systems Security Policy Section 6.6.

As with logical security measures at the City, physical security measures required for protecting City computing resources shall be commensurate with the nature and degree of criticality of the computer systems, network resources, and data involved. The more sensitive and critical the computing environment, the more control measures are likely to be needed. Because the system will be collecting and storing sensitive information, physical access control measures sufficient to prevent the HMIS system from unnecessary and unauthorized access, use, misuse, vandalism, or theft will be implemented. All specific tools, systems, or procedures implemented to meet physical security requirements should be selected on the basis of its cost-effectiveness and common sense.

The Hosting Entity, where the application and data will reside, provides:

- Physical security guarded and electronically monitored
- Rack mounted computer systems
- Environmental controls and monitoring of Data Center physical environment
- Fire detection and suppression systems
- Conditioned power
- Un-interruptible power supply
- Raised floor

Personnel Security Measures

Comprehensive pre-employment screening (i.e. background check, policy record check) is recommended for all potential candidates for key Safe Harbors' technical positions that include an actual or potential span of systems control, and/or access to sensitive information. In addition, such employees must sign a confidentiality agreement. Both the results of the background check and the confidentiality agreement must be maintained in the staff personnel files.

All Safe Harbors agencies and partners will establish and maintain all necessary processes and procedures to properly and immediately close and remove all system and network privileges and resources when an employee is terminated (return tokens, notify Safe Harbors staff to revoke certificates, disable the account, etc.)

Data Security and Data Integrity

- Safe Harbors' software will automatically log off after a pre-set interval of inactivity.
- There will be multiple levels of access to the Safe Harbors system. The appropriate access to the Safe Harbors system should be determined for each user. This determination should be based on each user's job function as it will relate to the Safe Harbors' system data entry and retrieval and will be officially designated by the Agency Executive Director.

- Each client record in the Safe Harbors system will be assigned a unique identifier that enables the software to count unduplicated records for aggregate reporting purposes. The unique identifier cannot be used to identify a specific individual.
- Each user of the HMIS will be required to obtain a security certificate and token in order to access the system.

Technical Guidelines

The City of Seattle Information Systems Security Policy contains Guidelines for technical measures, operating practices and methods that could be applied for the proper protection of the Safe Harbors Computer System and related data. Further, the Safe Harbors Security Requirements document will spell out specifics about how to implement the policy described herein.

Data Sharing

As a part of the implementation strategy of the system software, a participating agency program must have client consent procedures and completed forms in place when electronic sharing of identified data is to take place.

- Agency program policies for data sharing with other agencies should be reviewed periodically.
- Agencies programs shall determine when and if agency program data is shared with another agency program. Appropriate safeguards will be negotiated between and among agencies if sharing data.
- No identified client records will be shared electronically with another agency program without written client consent.

Defaults & Policies

Partner Agencies must have policies in place regarding the appropriate access to client data in the Safe Harbors system.

- The policies must include when, where and under what circumstances it is deemed appropriate for agency staff to access Safe Harbors' data outside the office. The policies must also indicate the consequences for staff failure to abide by the policies.

Policy Enforcement

Violators of this policy may be denied access to Safe Harbors' computing and network resources and may be subject to other penalties and disciplinary action within and outside of their agency.

Documented procedures should be in place for issuing, altering, and revoking access privileges on shared systems.

Audits

Agency sites and personnel are subject to periodic security audits. This is to make sure that the recommendations in this policy document are being implemented and that the agency is in compliance with the City of Seattle Security Policy.

Applicability

This Policy is applicable to all users (employees, contractors, and others) of City computing systems, networks, digital information, and any other electronic processing or communications related resources or services provided through the City.

APPENDIX A

Sign-on Warning

WARNING

This is a proprietary system of the City of Seattle and is for use by authorized individuals only.

The information in this system is confidential. Confidential information is sensitive or secret information, or information whose unauthorized disclosure could be harmful or prejudicial. Only those who have been explicitly granted their own userid and password by Safe Harbors may access this system beyond this point of entry. Any printed information obtained from this system must also be treated as confidential.

Use of this system constitutes an express consent to monitoring at all times. If monitoring reveals possible violations of criminal statutes, all relevant information will be provided to law enforcement officials. Anyone using this computer system or related information without proper authorization or in violation of the *Safe Harbors Security Policy* may be subject to possible internal disciplinary actions, civil and/or criminal prosecution.

By proceeding beyond this screen you are acknowledging that you understand and accept the content of this notice.

Report Print Warning

WARNING: reports may contain personal identifiable information. This information must be treated as **CONFIDENTIAL**.

Printed Document Top of Page Warning

WARNING: This printed page may contain personal identifiable information. This information must be treated as **CONFIDENTIAL**. You are personally responsible for protecting this document while it is needed and destroying it once is not needed, unless it is required to be retained in accordance with applicable law.

Screen Watermark & Screen Print Warning

WARNING: The above web page may contain personal identifiable information. This information must be treated as **CONFIDENTIAL**.