

**HMIS SECURITY PLAN  
of the  
PHILADELPHIA CONTINUUM OF CARE**

This plan describes the standards for the security of all data contained in the Philadelphia Continuum of Care Homeless Management Information System (HMIS). This plan outlines the security measures currently implemented by the HMIS Lead Agency, the City of Philadelphia Office of Supportive Housing (OSH) and details the baseline security requirements for all HMIS Participating Agencies.

**Applicability**

OSH and HMIS Participating Agencies must apply system security provisions to all the systems where personal protected information (PPI) is stored, including, but not limited to, its networks, desktops, laptops, mini-computers, mainframes and servers.

In addition to the Philadelphia Continuum of Care Security Plan, OSH must also adhere to the City of Philadelphia's Information Security Policy - Access Control (See Appendix A) and the Information Security Policy – Physical and Environmental Security (See Appendix B).

**User Authentication**

Upon successful completion of training and subject to approval by OSH, each HMIS user will be provided with a unique personal User Identification Code (User ID) and initial password to access the HMIS.

While the User ID provided will not change, HUD standards require that the initial password only be valid for the user's first access to the HMIS. Upon access with the initial password, the user will see a screen that will prompt the user to change the initial password to a personal password created by the user.

- A. Only the user will know the personal password he or she creates. It is the user's responsibility to remember the password.
- B. The password created by the user must be meet the following Federal and application-enforced guidelines:
  - The password must be at least eight characters long.
  - The password must contain at least one letter.
  - The first character of the password must be a letter.
  - The password must contain at least one number.
  - The password must contain at least one symbol or punctuation character.
  - The password may not contain your User ID.
  - The password may not contain the consecutive upper- or lower-case letters "HMIS" or "hmis."
- C. The password may not be stored in a publicly accessible location and written information pertaining to the User ID, password, or how to access the HMIS may not be displayed in any publicly accessible location.
- D. The user is not permitted to divulge this password or to share this password with anyone.

Before logging in to the HMIS, the user must check a box agreeing to the HMIS User Agreement which was established by OSH in cooperation with the City of Philadelphia Solicitor's Office. See Appendix C.

Providers are responsible for communicating all staff departures to the OSH Information Technology

Staff in a timely manner to ensure user profiles for departed staff are inactivated.

### **Application Security**

All computers connecting to HMIS must run a current version of anti-virus software. This is enforced through an Active Directory network policy, and applies to both devices directly attached to the City of Philadelphia's Wide Area Network as well as those at service provider locations that connect through the public Internet via a Secure Socket Layer (SSL) Virtual Private Network (VPN) tunnel connection. Individual computers are scanned and only allowed to connect to the network when the presence of updated anti/virus software from an approved list has been verified. This appliance also provides protection against phishing, malware, bot attacks and provides access control to limit users to appropriate resources.

HMIS Participating Agencies must maintain anti-virus software on all PC's on their network. PC's that access the Internet must be configured to automatically download updated virus definitions. Steps should also be taken to prevent the intrusion of "adware" and "spyware" programs.

OSH maintains hardware, software and PPI in a secure environment, protected by a Firewall.

### **Public Access**

End users connect to the Philadelphia CoC HMIS through the public Internet via a Secure Socket Layer (SSL) Virtual Private Network (VPN) tunnel connection.

Users may connect to one of several Terminal Servers which have been set up to assure redundancy and load balancing. All servers are monitored continuously for availability by the product What's Up Gold, and OSH IT staff are notified by email when they are not responding.

### **Physical Access to Systems With Access to HMIS Data**

HMIS Participating Agencies must staff computers at all times that are stationed in public areas and used to collect and HMIS data. Every computer that is used to access the HMIS must have a password-protected screen saver that automatically turns on when the computer is temporarily not in use. If an HMIS user will be away from the computer for an extended period of time, he or she is required to log off from HMIS before leaving the work area in which the computer is located.

### **Disaster Protection and Recovery**

HMIS data is contained on SQL 2005 databases which are run on a Windows Server clustered environment so that there will failover if the primary server becomes unavailable. The physical data storage is on multiple disc drives in a RAID array for redundancy so that no data will be lost or downtime incurred if a physical disk drive becomes inoperable. Additional hardware redundancy exists in the form of dual power supplies, disc controllers and network interface cards. OSH maintains service coverage through original and extended warranties from the original equipment manufacturer and assures that the systems are kept up to date in terms of patches and updates issued by both the software and hardware vendors. The SQL databases are automatically backed up nightly and stored on another secure server.

The HMIS database server itself is located in a controlled, physically secured environment at the City of Philadelphia Office of Innovation Technology (OIT) and is protected by modern systems for HVAC and Fire Suppression which are monitored 24/7. A diesel generator is maintained for backup power, and redundant Internet connections exist on opposite sides of the building. The Terminal Servers are distributed between OIT and OSH's office location where they are also behind a locked door in a

building that has 24/7 security.

### **Disposal**

The City of Philadelphia contracts with a certified specialist for destruction of physical disk drives who can be utilized as required.

### **System Monitoring**

HMIS produces reports based on log files that are reviewed and inactive user accounts are consequently disabled. In addition to the HMIS database itself, access to HMIS is also controlled, monitored and logged by the Active Directory (AD) and Checkpoint security systems.

### **Electronic Data Storage**

HMIS data is contained on SQL 2005 databases which are run on a Windows Server clustered environment; and therefore, is stored in binary format.

### **Hard Copy Security**

The guidelines regarding the security of paper or other hard copy containing PPI that is either generated by or for the HMIS, including, but not limited to reports, data entry forms, and signed consent forms are:

1. HMIS Participating Agency staff must supervise at all times any paper or other hard copy generated by or for the HMIS that contains PPI when the hard copy is in a public area.
2. When HMIS Participating Agency staff is not present, the information must be secured in areas that are not publicly accessible.
3. Written information specifically pertaining to user access (e.g., User ID and password) must not be stored or displayed in any publicly accessible location.

### **Duration**

This plan must be reviewed annually and updated as needed by the Philadelphia Continuum of Care.

This plan was originally approved by the Philadelphia CoC Strategic Planning Committee on January 30, 2014.

### **ATTACHMENTS:**

City of Philadelphia Information Security Policy - Access Control

City of Philadelphia Information Security Policy – Physical and Environmental Security

HMIS User Agreement



# CITY OF PHILADELPHIA

Issued:	<b>Information Security Policy Access Control</b>	Policy Number: 10.00
Effective:		Approved By:
Revised:		
Revision #: 1.0		

## 1 PURPOSE

The purpose of this *policy* is to establish *general standards* for securing access to City of Philadelphia (City) *information systems* and *information*, for assigning *access rights* and *credentials* (user ID and passwords) based on job functions, and for limiting individual *users'* access in accordance with their *access rights*. These *general standards* are intended to ensure the *security of information* accessed, stored or processed by any City *information system*, including *portable devices* and *portable media*, and by *information systems* that are not owned or furnished by the City.

*Portable device* means any portable electronic computing device including but not limited to, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, *messaging systems*, smartphones (e.g., BlackBerrys) or any other *portable device* that may be used to store City *information*.

*Portable media* means any portable material or device (other than an electronic computing device) that stores *information*, including, but not limited to floppy disks, CD-ROMS, DVDs, magnetic tape, external hard drives, memory devices, and microfilm or microfiche and USB external flash drives (e.g., pen drives, thumb drives or memory sticks).

*Access rights* means the privileges that a particular *user* has to access a City *information system* and/or the *information* on it, such as the right to read, write, modify or delete *information*, the right to use certain system commands, or the right to access certain file folders.

## 2 POLICY SCOPE

This *policy* applies to all City *information users*, *information systems*, and *information*; to *information systems* not owned or furnished by the City that are used to access, store or process City *information* (including *user-provided information systems*); to *users* who have access to City *information systems* or *information* and to the activities related to all stages in the *user access lifecycle*, from initial *user request* for access through final termination of access to *users* who no longer require it.

*Information systems* include, but are not limited to, mainframes, servers, desktop computers, notebook computers, hand-held computers, *portable devices*, *portable media*, pagers, *messaging systems*, distributed processing systems, *network* attached and computer controlled medical and laboratory equipment (i.e., embedded technology), telecommunication resources, *network equipment*, telephones, fax machines and printers. *Information systems* also include *operating system software*, *software applications* and *service bureaus* and *software applications* that are hosted by third parties and accessed through the *Internet*.

*User access lifecycle* means the activities related to requesting, authorizing, granting, establishing, documenting, reviewing and/or modifying and terminating a *user's* right to access City *information systems* and *information*.

### 3 USERS

The *users* to whom this *policy* applies are all City personnel, including but not limited to, *agency heads* and *information technology (IT) administrators*, who request, authorize, grant, establish, document, review, modify and/or terminate a *user's* right to access City *information systems* and *information*, and all *information users* who have access to City *information systems* or *information*.

*Agency head* means the person who is responsible for the supervision and operation of a City *agency*.

*Information technology administrators* means and includes all City *employees*, *contractors*, *third party users*, consultants, vendors and any other City *information users* who provide support and management to City *information systems* and the *information* created, received, transmitted, stored or deleted within.

*Information users* or *users* means and includes City *employees*; *information technology administrators* (or *information technology administrators* or *administrators*); officers and elected officials; City divisions, *agencies*, departments, boards and commissions; *City-related agencies*; *City contractors*; and *third party users* who use or have access to City *information systems* and *information*.

### 4 DEFINITIONS

Italicized terms defined in this *policy* shall have the meanings in this *policy* that are here provided.

Italicized terms not defined in this *policy* shall have the meanings contained in City Information Security Policy No. 13.00: *Glossary of Information Security Terms*.

### 5 POLICY

This *policy* sets forth the *general standards* for securing access to City of Philadelphia (City) *information systems* and *information*, for assigning *access rights* and *credentials* (User ID and passwords) based on job functions, and for limiting the individual *user's* access in accordance with the *user's access rights*. The *general standards* set forth in this *policy* are intended to ensure the *security* of *information* accessed, stored or processed by any City *information system*, including *portable devices* and *portable media*, and by *information systems* that are not owned or furnished by the City. The *Information Security Group (ISG)* shall develop *specific standards*, as required, to implement the *general standards* in this *policy*.

The *general standards* in this *policy* shall apply to all City *agencies* and all *information systems* containing City *information*, whether or not they are owned or furnished by the City, including *user-provided information systems*. *Agency heads*, in consultation with the Division of Technology (DOT), shall develop and implement detailed *procedures* in accordance with this *policy* and specific *access standards* issued by the *Information Security Group* to control access to the City *information systems* and *information* for which they are responsible.

## 5.1 Standards of Compliance

### 5.1.1 User Access Lifecycle

The *access rights* available to the *user* shall be controlled by the *specific standards* established by the *Information Security Group* and the *general standards* contained in this *policy* governing each stage of the *user access lifecycle*. The *standards* for each stage shall be sufficient to prevent unauthorized access to *City information systems* and *information*. Authorization of *user access rights* and modification or removal of *access rights* are normally the responsibility of the *users' agency head* or designee, but the *Information Security Group* may assume this responsibility, with notice to the *agency head*, if the *Information Security Group* determines it is necessary to do so in order to protect the *security* of *City information systems* or *information*.

### 5.1.2 User Responsibilities

In accordance with City Information Security Policy No. 02.00: *Acceptable Use* and the *general standards* contained in this *policy*, *information users* are permitted to access and use *City information systems* and *information* only as required to carry out their specific job responsibilities, as determined by the head of the *users' agency*, and to conduct *City business*. *Users* are responsible for the following:

- a) Protecting their *user IDs* and passwords, and maintaining the *security* of *City information systems* and *information* they use and have access to. *Users* should avoid keeping a record (e.g., paper record, or electronic file) of passwords unless they can be stored securely and the method of storage has been approved by the *Information Security Group*;
- b) Not sharing computer accounts, passwords and other access *credentials* assigned to them;
- c) Selecting passwords in accordance with the *Information Security Group's specific standard* governing *user IDs* and passwords;
- d) Changing temporary passwords at the first logon;
- e) Terminating active sessions when finished, unless the session can be secured by a locking mechanism approved by the *Information Security Group* (e.g., the Windows computer locking feature) when unattended; and
- f) Protecting *information systems* and *information* under their control by using passwords or other security controls as required by the *Information Security Group* when not in use.

### 5.1.3 Network Access Control

The Division of Technology shall implement *security controls* sufficient to prevent unauthorized access and otherwise ensure the *security* of *City networks*, including at a minimum the following types of *security controls*:

- a) Network Controls

At a minimum, access to *City networks* shall be governed by *security controls* that:

- i) Ensure the *security* of *information* passing to and from *City networks* over public *networks* or wireless *networks*, such as, but not limited to, *data encryption*;

- ii) Provide prevention and detection controls such as, but not limited to, firewalls and intrusion detection and prevention systems;
- iii) Require redundancy for *networks* that support *critical information systems*;
- iv) Restrict physical *network* connections (i.e., *network* board, jack and cable) and other *network* ports allowing connectivity to City *networks* to only authorized *users*; and
- v) Ensure that all *networks* and *network equipment*, including but not limited to routers and switches, require *user* authentication in accordance with Section 5.1.3(b) and (c) of this *policy* as a condition of access.

b) User Identification and Authentication

The *Information Security Group* shall establish a *specific standard* for creating *user* identification (*user* ID), and *user* accounts, including the method of authentication to be used on City *network equipment*. At a minimum, this *specific standard* shall include the following:

- i) The requirement that a unique *user* ID be established for each *user* that is sufficient to provide an audit trail and permit accountability for the *user's* actions performed on *networks* and *network equipment*; and
- ii) Criteria for password creation, including temporary passwords, such as, but not limited to, number and type of characters required in a password.

c) Secure Logon Standard

The *Information Security Group* shall establish a *specific standard* for logging onto City *networks* and *network equipment* sufficient to limit access to authorized *users*. The logon shall disclose no more *information* about the *network equipment* than is necessary to complete a secure logon. At a minimum, the logon *standard* shall:

- i) Prevent display of system or application identifiers until the logon process has been successfully completed;
- ii) Prohibit help messages during logon procedures that would aid an unauthorized *user* to access the *network* or *network equipment*, such as messages identifying the incorrect credential(s) during failed logon attempts;
- iii) Limit the number of unsuccessful logon attempts allowed before the *user* is shut out (e.g., three attempts);
- iv) Hide or disguise passwords as they are entered; and
- v) Prevent transmission of passwords in clear text over the *network*.

d) Remote Access Controls

The Division of Technology and *agency heads* shall implement *security controls* to protect City *information systems* and *information* accessed remotely. *Information users* who remotely access City *networks*, *information systems* or *information* are responsible for preventing unauthorized access by means they control. *Remote access* means the ability to access a City *network*, *information system* or *information* from outside the City's *networks*, or to access and control or manage an *information system* from another *information system* within the City's *networks*, using protocols that include, but are not limited to, virtual network computing (VNC), remote desktop protocol (RDP) or Citrix independent computing architecture (ICA).

- i) The Division of Technology shall develop *specific standards* specifying approved methods for *remote access*.
- ii) *Remote access* shall be authorized only for *users* whose job functions and specific City business needs require *remote access*.
- iii) Only *information technology administrators* and other *users* authorized by the *Information Security Group* may have *remote access* to maintenance and *diagnostic paths* into City *information systems*. *Contractors* shall not have such *remote access* unless authorized by the *Information Security Group*.
- iv) All *user accounts* for *remote access* shall be created and maintained in accordance with Sections 5.1.2 and 5.1.5 of this *policy*.

e) Wireless Access

No *user* may access any City *network*, *information system* or *information* by any wireless communications system or wireless equipment unless authorized by the Division of Technology. Wireless connections to City *networks*, *information systems* and *information* shall comply with *specific standards* developed by the *Information Security Group*, which shall at a minimum specify encryption and user authentication protocols.

f) Segregation of Networks

City *networks* shall be segregated into *logical network segments* by means of *network security controls* that restrict access between and among City *networks* and *information systems*. The controls shall permit such access only to the extent necessary for *users* to carry out their job functions and conduct City business, and shall restrict access based on the criticality and classification of the *information* resident on the *networks* and *information system(s)*.

- i) City *networks* shall be segregated into *logical network segments* based upon the criticality and classification of *information* stored or processed on the *network*, the degree of verification (or trust) needed for *users* to perform transactions using that *information* and business requirements. *Logical network segments* shall be protected by *network controls* sufficient to minimize or eliminate the impact of service disruptions in any segment to any other segment. *Logical network segments* shall be protected by routing, filtering and blocking *controls* sufficient to restrict access among segments except as authorized by the *Information Security Group*.
- ii) City *networks*, accessed through the *Internet*, the City's *intranet*, or a City or non-City *extranet* shall be protected by *network access controls* that establish *logical network segments* (such as, but not limited to, segregation into an internal *logical network segment* and an external *logical network segment*), each protected by a defined *security zone* or perimeter that controls access to and from the segment. The Division of Technology shall establish *security controls* within *security zones* and perimeters that are sufficient to provide, at a minimum, positive source and destination address verification, and filtering and blocking mechanisms to prevent access among *logical network segments* except as authorized by the *Information Security Group*.

g) Security of Network Devices

The *Information Security Group* and *agency information technology administrators* shall ensure that access to all City *network devices*, including, but not limited to, routers, switches, firewalls and access control servers, is controlled by means of *user IDs* and passwords for authentication,

and that such IDs and passwords are different from the IDs and passwords used for access to other City *information systems*.

#### 5.1.4 Portable Devices and Portable Media

All *agencies* shall follow the *specific standards* established by the *Information Security Group* for implementing *security controls* to protect *information* accessed, transmitted and stored on *portable devices* and *portable media*, whether or not issued by the City. Special care shall be taken to ensure the *security* of *portable devices* and *portable media* containing *confidential* or *for official use only information*.

#### 5.1.5 Information System Access Control

The Division of Technology and City *agency heads* shall implement *security controls* in City *information systems* to restrict access to authorized *users*. *Security controls* shall include at least the following:

a) Information Access Restriction

*Information* stored or processed on *information systems* shall have *security controls* that restrict the access of each *user* to only the *information* required to perform the *user's* job functions.

b) User Identification and Authentication

The *Information Security Group* shall establish a *specific standard* for creating *user* IDs and the method of authentication to be employed on City *information systems*. At a minimum, this *specific standard* shall:

- i) Require unique *user* identification for each *user* that is sufficient to provide an audit trail and permit accountability for the *user's* actions performed on *networks* and *network equipment*;
- ii) Specify criteria for password creation, including temporary passwords, such as, but not limited to, number and type of characters required in a password; and
- iii) Require a separate *user* ID and password for each *information system* accessed by the *user*.

c) Secure Logon Standard

The Division of Technology shall establish *specific standards* for logging onto *information systems* that are sufficient to prevent unauthorized access. The logon shall disclose no more *information* about the *information system* than is necessary to complete a secure logon. At a minimum, the logon standard shall:

- i) Prevent display of *system* or application identifiers until the logon process has been successfully completed;
- ii) Prohibit help messages during logon *procedures* that would aid an unauthorized *user* to access the *information system*, such as identifying incorrect *credential(s)* during failed logon attempts;
- iii) Limit the number of unsuccessful logon attempts allowed before the *user* is shut out (e.g., three attempts);
- iv) Hide or disguise passwords as they are entered; and
- v) Prevent transmission of passwords in clear text over any *network*.

d) Use of System Utilities

Access to and use of *system* utilities that can override authentication or other *information systems'* controls shall be restricted to *users* authorized by the *Information Security Group*.

e) Computer Timeout

The Division of Technology and *agency heads* shall ensure that *information systems* are configured to log off or lock a *user* or shut down after waiting a certain period of time without receiving expected input. The timeout period shall be determined by the *security* risks related to the *information system*, the criticality and classification of the *information* on the system, and the criticality of the *software applications* being used.

**5.1.6 Monitoring System Access, Use and Risk**

The Division of Technology and *agency heads* shall ensure *security controls* are implemented and maintained to detect unauthorized or suspicious system events and identify and record *security* incidents. Such controls shall include, at a minimum, the following:

a) Event Logging

Audit logs shall record relevant *security* events and exceptions to provide for regular access control *monitoring* and to support any investigations of *security* incidents.

b) Assessment of Risk

The *Information Security Group* shall establish *specific standards* for *monitoring information systems* to ensure that *users* are carrying out only authorized activities.

*Agencies* and the *Information Security Group* shall regularly review every City *information system* to identify and assess risks specific to the *software applications* resident on the *information system*. The review shall take into account the criticality of the *information system* and the *information* it processes, as well as the criticality of the *software applications*, the history of misuse of the *information system* (including *security* incidents), and the accessibility of the *information system* from other City *networks* and *information systems*.

c) Logging and Reviewing Events

The *information technology administrators* shall ensure that a regular review of system logs is performed in accordance with the *Information Security Group's specific standard* for such review to identify *system* events and exceptions that are suspicious and warrant further investigation. Such system log reviews shall not be performed by the *information technology administrators* who are responsible for the *information systems* being reviewed.

d) Time Synchronization

Time synchronization with the City's authorized time source shall be maintained for all City *information systems* in order to ensure the accuracy of audit logs.

**5.1.7 Exception Management**

This *policy* is not intended to preclude the use and access of City *information systems* and *information* to meet any legitimate business need of the *user* or the *user's agency*. If an *agency* needs to transmit or access materials prohibited by this *policy* or otherwise to act contrary to the *policy* in order to conduct its

business and carry out its responsibilities, the *agency* is responsible for first obtaining approval for an exception to the *policy* from the *Information Security Group*.

## **6 ENFORCEMENT; DISCIPLINARY ACTION**

Each City *agency head* shall be responsible for enforcing compliance with this *policy* by *agency information users*.

*Information users* that violate this *policy* may be subject to disciplinary action, up to and including, termination of employment, in accordance with the disciplinary *policies* of the *information user's agency* and, for *information users* represented by the Fraternal Order of Police, International Association of Firefighters, District Council 47 or District Council 33, the terms of the applicable collective bargaining agreement.

If a City *contractor* or *third party user* knowingly or negligently commits or permits a material violation of this *policy*, the City may terminate the contract in accordance with its terms, and/or terminate the *contractor's* or *third party user's* access to City *information processing facilities, information systems* and *information*, in addition to any legal or remedial actions the City may take to enforce and protect its interests.

## **7 GETTING MORE INFORMATION**

Questions about this *policy* and other *information security* matters should be addressed to the *Information Security Group* (Email: [ISG@phila.gov](mailto:ISG@phila.gov) Phone: (215) 686-8180).



# CITY OF PHILADELPHIA

Issued:	<b>Information Security Policy Physical and Environmental Security</b>	Policy Number: 09.00
Effective:		Approved By:
Revised:		
Revision #: 1.0		

## 1 PURPOSE

The purpose of this *policy* is to define the minimum physical and environmental *security controls* required by the City of Philadelphia (City), including City *general standards* to be applied in the implementation of such *security controls*, to protect the *confidentiality, integrity and availability* of City *information processing facilities, information systems and information*. *Security controls* means and includes the safeguards or countermeasures to avoid, counteract or minimize *security risks*. *Security controls* may include, but are not limited to, identification badges; *information backup procedures; policy and procedures for employee separation from the City; and controls on physical network access*. Such controls are intended to prevent unauthorized disclosure of, access to, destruction or theft of, damage to and interference with City *information processing facilities, information systems and information*, including *information systems* that present special *security risks*, such as, but not limited to, *portable devices, portable media, and network equipment*.

## 2 POLICY SCOPE

This *policy* applies to all *information processing facilities* owned, leased, controlled, or used by the City; to all *information systems* owned, controlled, or used by the City; and to all *information* created, received, transmitted, stored and/or deleted by means of City *information systems*.

*Information systems* include, but are not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, *portable devices, portable media*, distributed processing systems, *network* attached and computer controlled medical and laboratory equipment (i.e., embedded technology), telecommunication *resources* and systems, *network equipment*, telephones, fax machines and printers. *Information systems* also include *operating system software, software applications and service bureaus and software applications* that are hosted by third parties and accessed through the *Internet*.

*Portable devices* include, but are not limited to, notebook computers, hand-held computers, *personal digital assistants (PDA)*, pagers, *messaging systems*, smartphones (e.g., Blackberry) or any other *portable device* that may be used to store City *information*.

*Portable media* include, but are not limited to, floppy disks, CD-ROMs, DVDs, magnetic tape, external hard drives, external memory devices, microfilm or microfiche, and USB external flash drives (pen drives, thumb drives, flash drives or memory sticks).

*Network equipment* includes, but is not limited to, switches, *firewalls*, wireless access points, routers and cabling.

### 3 USERS

The *users* to whom this *policy* applies include all City *information users* who use and/or have access to City *information processing facilities*, *information systems* and *information*. *Information users* or *users* mean and include City *employees*; *information technology (IT) administrators* (or *information technology administrators* or *administrators*); officers and elected officials; City divisions, *agencies*, departments, boards and commissions; *City-related agencies*; City *contractors*; and *third party users* who use or have access to City *information processing facilities*, *information systems*, and *information*.

### 4 DEFINITIONS

Italicized terms defined in this *policy* shall have the meanings in this *policy* that are here provided. Italicized terms not defined in this *policy* shall have the meanings contained in City Information Security Policy No. 13.00: *Glossary of Information Security Terms*.

### 5 POLICY

City *Information processing facilities*, *information systems* and *information* shall at all times be protected by *security controls* sufficient to ensure their *confidentiality*, *integrity*, and *availability* and prevent unauthorized disclosure or access, damage, destruction, theft or interference. *Information users* are responsible for applying such *security controls* to the *information processing facilities*, *information systems* and *information* to which they control or have access.

#### 5.1 Standards for Compliance

##### 5.1.1 Secure Areas

Access to City *information processing facilities*, *information systems* and *network equipment* shall be secured with sufficient controls to protect them from unauthorized access, damage, destruction, theft and interference.

a) Physical Security Perimeter

A clearly defined *security* perimeter shall be established for each City *information processing facility*. The *security* perimeter shall provide a secure area within each City *information processing facility* to house *information systems* and *network equipment*.

b) Physical Access Control

Offices and rooms containing *confidential information* or *for official use only information* shall have effective access controls sufficient to ensure that only authorized persons may enter the *information processing facility* and/or access the *information systems* or *information* maintained in the facility. Such *security controls* may include, but are not limited to, electronic or mechanical locks, gates or doors controlled by electronic badges and security guards.

c) Identification Badges

All persons accessing a City *information processing facility*, including, but not limited to, City *employees*, *contractors* and visitors, shall be required to wear, in plain view, an identification badge.

## d) Facility Access

Access to City *information processing facilities* and to any restricted area in the facilities shall be controlled in accordance with each facility's access management *procedures*. Access to a secure area shall be granted only to *information users* who require access to perform job duties, and shall be no greater in scope than is necessary for the performance of these duties.

The Department of Public Property (DPP) shall ensure that records of all persons obtaining access to any City *information processing facility*, including, but not limited to, visitors, *contractors* and *third party users*, are created and maintained. Reports summarizing such records shall be made available to *users' agency head* or designee, the Inspector General, Police Department, Internal Affairs Division, the Law Department, the Ethics Board, the District Attorney's Office and the *Information Security Group (ISG)*. Access reports may be used to investigate unauthorized access to or use of *information processing facilities* or *information systems*, and may be the basis for modifying or rescinding *access rights* or disciplinary action.

## e) Facility Surveillance

Entrances and exits to City *information processing facilities* shall be equipped with surveillance devices placed and configured in accordance with City *standards* established by the Department of Public Property.

### 5.1.2 Information System Security

*Information systems* and *network equipment* shall be installed and maintained with *security controls* sufficient to protect the *confidentiality*, *integrity*, and *availability* of information systems and *network equipment*, and the *information* stored and/or processed on them, from unauthorized disclosure or access, damage, destruction, theft and interference.

## a) Network Equipment

A secure area for *network equipment* shall be established in each *information processing facility* in accordance with City physical and environmental *security standards* established by the Department of Public Property and the Division of Technology (DOT).

## b) Portable Devices and Media

*Users* are responsible for protecting all *portable devices* and *portable media* that contain City *information*, whether or not they were issued by the City. Such *portable devices* and *portable media* shall be stored securely when not in use to prevent theft, damage and unauthorized access, in accordance with *standards* established by the Division of Technology.

## c) Information System Re-Use

Re-use of equipment and other *information systems* by another *user* or *agency* or sale or other transfer of used equipment to non-City persons or entities may be permitted only if all City *information* is first removed from the equipment in accordance with City *standards* established by the Division of Technology.

## d) Power Supplies

*Agency heads*, in coordination with the Division of Technology, shall determine which *information systems*, *network equipment*, telecommunications equipment and other *critical systems* shall be equipped with an uninterruptable power supply (UPS) sufficient to ensure

system *availability* in accordance with the *service level agreement (SLA)* defined for the *information system*.

e) Cabling

*Network* and communication cables to and from *information systems* shall comply with the Institute of Electrical and Electronics Engineers (IEEE) 802.3 -2006 domestic cabling *standard* and with any additional cabling *standards* established by the Department of Public Property and the Division of Technology to ensure the *availability* of *City information systems* and *network equipment*.

f) Environmental Damage

In accordance with *City standards* established by the Department of Public Property and the Division of Technology, *agency heads* shall ensure *information systems* and *network equipment* are installed, operated, maintained and stored in a manner that will protect against environmental risks, including, but not limited to, damage or destruction by fire, water, heat, humidity, electrical surges and static electric discharge. *Security controls* shall include, but are not limited to, fire detection and suppression equipment, electrical power conditioning, climate controls and other measures designed to protect against environmental damage.

A preventive maintenance program shall be established in accordance with *City standards* established by the Department of Public Property and the Division of Technology to ensure the proper function and adequate environmental quality of *City information processing facilities, information systems* and *network equipment*.

### 5.1.3 Securing Third Party Access to City Information Processing Facilities, Information Systems and Information

The Division of Technology and the Department of Public Property shall develop *procedures* and protocols for ensuring the *security* of *City information processing facilities, information systems* and *information* accessed and/or used by persons and entities that are not *employees* or *agencies* of the City, including, but not limited to, *City contractors* and *third party users* (collectively, third parties). Such *procedures* and protocols shall include at least the following:

- a) No third party may have access to *City information processing facilities, information systems, network equipment* or *information* unless it has first fully executed a City contract for goods or services or *security agreement* containing terms and conditions approved by the *Information Security Group* and the City's Law Department.
- b) All third party access shall be controlled in accordance with Sections 5.1.1 (b), (c) and (d) of this *policy*.
- c) Contracts with third parties that manage or maintain *City information systems, network equipment* and/or *information* on an *outsourcing* basis shall include terms and conditions that require the third party to maintain the *integrity* and *security* of *City information*.
- d) Third parties that perform *outsourcing* functions for the City outside City premises shall be subject to a *security audit* by the City. No contract may be entered into with such a third party, and no access to any *City information processing facilities, information systems, network equipment* or *information* may be granted to such a third party, unless or until the Chief Information Security Officer reviews and approves the results of the *security audit*.

#### **5.1.4 Securing Visitor Access to City Information Processing Facilities, Information Systems, Network Equipment and Information**

The Department of Public Property and the Division of Technology shall develop *procedures* and protocols for ensuring the *security* of *City information processing facilities* and the *information systems* and *information* located in them from unauthorized access by visitors. Such *procedures* and protocols shall, at a minimum, require that physical access by visitors to any *City information system*, including *network equipment*, be controlled in accordance with Sections 5.1.1 (b), (c) and (d) of this *policy*, and specifically, that all visitors be escorted by authorized *City employees* whenever they have such physical access.

#### **5.1.5 Exception Management**

This *policy* is not intended to preclude or interfere with the use of *City information processing facilities*, *information systems* and *information* to meet the legitimate business needs of the *user* or the *user's agency*. If an *agency* or *user* needs to have access to *information processing facilities*, *information systems*, or *information* in a manner prohibited by this *policy* or otherwise to act contrary to the *policy* in order to meet legitimate business needs and carry out the responsibilities of the *agency* and the *user*, the *agency* is responsible for obtaining *Information Security Group* approval for an appropriate exception to the *policy*.

### **6 ENFORCEMENT; DISCIPLINARY ACTION**

Each *City agency* head shall be responsible for enforcing compliance with this *policy* by *agency information users*.

*Information users* that violate this *policy* may be subject to disciplinary action, up to and including, termination of employment in accordance with the disciplinary *policies* of the *information user's agency* and, for *information users* represented by the Fraternal Order of Police, International Association of Firefighters, District Council 47 or District Council 33, the terms of the applicable collective bargaining agreement.

If a *City contractor* or *third party user* knowingly or negligently commits or permits a material violation of this *policy*, the City may terminate the contract in accordance with its terms, and/or terminate the *contractor's* or *third party user's* access to *City information systems* and *information*, in addition to any legal or remedial actions the City may take to enforce and protect its interests.

### **7 GETTING MORE INFORMATION**

Questions about this *policy* and other *information security* matters should be addressed to the *Information Security Group* (Email: [ISG@phila.gov](mailto:ISG@phila.gov) Phone: (215) 686-8180).

**Office of Supportive Housing**  
**Homeless Management Information System**  
**User Agreement**

This agreement between the City of Philadelphia (City) and the undersigned user of its Homeless Management Information System (HMIS) specifies policies, rights and responsibilities, and ethical guidelines with regard to the use of the HMIS.

I. Background

The City's Office of Supportive Housing (OSH) is the entity designated by the US Department of Housing and Urban Development (HUD) as the administrator of Philadelphia's Continuum of Care (CoC)-wide HMIS. Entities using this HMIS currently include OSH and the agencies and organizations within the CoC. In accordance with HUD directives, HMIS participation will continue to expand to include additional agencies and organizations within the Philadelphia CoC.

II. Training

Any individual who has not received OSH-approved training on how to properly use the system should not use the HMIS. All HMIS users will therefore be required to complete HMIS training prior to using the system. Any OSH user who feels he or she needs refresher training should contact their supervisor. Non-OSH employees should contact the HMIS Site Administrator from their organization.

III. User Identifications Codes and Passwords

Upon successful completion of training and signing of this HMIS User Agreement, and subject to approval by the City, each HMIS user will be provided with a unique personal User Identification Code (User ID) and initial password to access the HMIS.

While the User ID provided will not change, HUD standards require that the initial password only be valid for the user's first access to the HMIS. Upon access with the initial password, the user will see a screen that will prompt the user to change the initial password to a personal password created by the user.

- A. Only the user will know the personal password he or she creates. It is the user's responsibility to remember the password.
- B. The password may not be stored in a publicly accessible location and written information pertaining to the User ID, password, or how to access the HMIS may not be displayed in any publicly accessible location.
- C. The user is not permitted to divulge this password or to share this password with anyone.

IV. Security, Privacy, and Confidentiality of Client Data

The HMIS contains a range of Personal Protected Information (PPI) on clients and all such information must be treated carefully and professionally by all who access it. According to HUD, PPI is defined as "any information maintained by a Covered Homeless Organization about a living homeless client or homeless individual that: (1) Identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual." A Covered Homeless Organization (CHO) is defined as "any organization (including its employees, volunteers, affiliates, and associates) that records, uses or processes PPI on homeless clients for an HMIS." HMIS users are therefore subject to the following guidelines regarding the security, privacy, and confidentiality of client PPI.

- A. The only individuals who may view or receive data from the HMIS are authorized users of the HMIS, users of other City databases for which clients have granted explicit informed consent to share data, and the individual clients to whom the data pertains. The User ID and password assigned to each individual HMIS user is to be used only for his or her access to the HMIS. An HMIS user may not allow access to the HMIS with his or her User ID and password to any other individual, regardless of whether or not the individual is an authorized HMIS user or whether or not the individual has the same job role or the same level of access rights.
- B. Each HMIS user may only view, obtain, extract, or use the data from the HMIS that is necessary to perform his or her job. Each HMIS user may only operate the HMIS using the Job Roles assigned to him or her.
- C. Failure to properly log off the HMIS may result in a breach of system security and the privacy of client data. A computer that has the HMIS application open must therefore never be left unattended. Every computer that is used to access the HMIS must have a password-protected screen saver that automatically turns on when the computer is temporarily not in use. If an HMIS user will be away from the computer for an extended period of time, he or she is required to log off from the HMIS before leaving the work area in which the computer is located.
- D. The guidelines regarding the security of paper or other hard copy containing PPI that is either generated by or for the HMIS, including, but not limited to reports, data entry forms, and signed consent forms are:
  1. A CHO must supervise at all times any paper or other hard copy generated by or for the HMIS that contains PPI when the hard copy is in a public area.
  2. When CHO staff is not present, the information must be secured in areas that are not publicly accessible.
  3. Written information specifically pertaining to user access (e.g., User ID and password) must not be stored or displayed in any publicly accessible location.
- E. Information obtained by the HMIS user from the HMIS is to remain confidential even after the HMIS user's relationship with the City and/or the participating agency that employs him or her changes or concludes for any reason.

VI. Data Quality Control

- A. To the extent that clients and other agencies supplying information have provided accurate data, HMIS users are responsible for the accuracy of the data they enter into the HMIS.
- B. HMIS users are required to enter data into the HMIS in a timely manner and in accordance with OESS performance standards and with any existing applicable agreements between OESS and its provider agencies.

VII. Problems with the HMIS

An HMIS user employed by a provider agency encountering a problem using the HMIS should contact his or her supervisor(s) and the HMIS Site Administrator from their organization. If the HMIS Site Administrator is not able to answer the question or solve the problem, he or she will contact the OSH Information Technology Helpdesk at 215-686-7110 or HMIS@phila.gov. An OSH HMIS user encountering a problem using the HMIS should contact his or her supervisor(s) and the OSH Information Technology Helpdesk at 215-686-7110 or HMIS@phila.gov.

**I affirm that I have read this Homeless Management Information System (HMIS) User Agreement and received training on how to use the HMIS. I agree that I will use the HMIS only for its intended use and in accordance with the training and access rights I have received. If I believe a security breach has occurred, I will notify the OSH Information Technology Helpdesk at 215-686-7110 or HMIS@phila.gov or the HMIS Site Administrator of the provider agency that employs me. I understand and agree to comply with the terms of this agreement. My failure to uphold terms of this agreement may result in progressive disciplinary action, up to and including termination of my employment. There is no expiration date of this agreement.**