Philadelphia Continuum of Care
HMIS Security Plan

Purpose
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 Homeless Services (OHS) and details the baseline security requirements for all HMIS Participating Agencies.

Responsibilities of HMIS Lead Agency
As HUD mandates, the HMIS Lead Agency shall:

1. Establish a security plan;
2. Designate a security officer
   a. Criminal background check must be conducted on the designee and other users with administrative privileges;
3. Conduct workforce security screening;
4. Report security incidents;
5. Establish a disaster recovery plan;
6. Conduct an annual security review;

Responsibilities of Participating Agency or Look-Up Agency
Participating Agency or Look-Up Agency shall:

1. Designates a security officer
   a. Criminal background check must be conducted on the designee and other users with administrative privileges;
2. Conducts workforce security measures;
3. Ensure that each user completes security training at least annually;
4. Conducts an annual security review;

Designations
OHS has designated the Lead Helpdesk Technician position of the HMIS Unit as our HMIS Security Officer.

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.

User Authentication

Upon successful completion of training and subject to approval by OHS, 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 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 (A through Z and/or a through z).
   - The first character of the password must be a letter (A through Z or a through z).
   - The password must contain at least one number (0 through 9).
   - The password must contain at least one symbol or punctuation character (i.e. $, #).
   - The password may not contain your User ID.
   - The password may not contain the consecutive upper- or lower-case letters “HMIS” or “hmis.”

Providers are responsible for communicating all staff departures to the HMIS Helpdesk in a timely manner to ensure user profiles for departed staff are inactivated.

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.

Application Security

In addition to the HMIS application training, users will also be offered security-awareness training. User are also expected to undergo annual security awareness training. All computers connecting to HMIS must run a current version of anti-virus software. This is enforced for City of Philadelphia workers through an Active Directory network policy, and applies to devices directly attached to the City of Philadelphia's Wide Area Network. HMIS Participating Agencies must maintain anti-virus software on all PCs on their network. PCs that access the Internet must be configured to automatically download updated virus definitions. HMIS participating providers are responsible for assuring that devices used to access the Philadelphia Continuum of Care's HMIS are protected. Steps should also be taken to prevent the intrusion of “adware” and “spyware” programs.

The application is accessed by users via a secure HTTPS connection to the software web application server. The HTTPS protocol, which is designed to prevent eavesdropping and tampering, provides a secure communication channel to the application.
Physical Access to Systems with Access to 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.

Security Violations and Sanctions

Noncompliance with this policy by participating agency and/or its end user is unacceptable. Any Agency or end user found to be in violation of security protocols will be sanctioned accordingly. Sanction may include but are not limited to suspension of system privileges and revocation of system privileges. Violations of this policy may also be violations of applicable Federal, State, or Local laws leading to prosecution, both as an individual or as an organizational entity, and criminal and civil penalties.

Disaster Protection and Recovery

Backup procedures and off-site storage facilities – Incremental/differential database backups are performed every three (3) hours. Transaction logs are backed up every four (4) hours. A full database backup to the hosted offsite secure storage facility is performed nightly. All backups are encrypted with 256-bit Advanced Encryption Standard (AES).

Restoration and recovery procedures at the host level – In the event that the primary Eccovia Solutions, Inc. hosting facility experiences a catastrophic interruption in service, the service will fail over to the secondary hosting facility within a Recovery Time Objective (RTO) of four (4) hours or less. For all other interruptions in service affecting data integrity, the Recovery Point Objective (RPO) will be to the last backup, which is three (3) hours or less.

Issue Severity Levels

Issues will be categorized and handled according to an assigned Severity Level. The Issue Severity Level is assigned by Eccovia Solutions, Inc. based upon initial triage processes.
<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Description</th>
<th>Response Times</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1 - Critical (Security Related)</td>
<td>The issue relates to the security of private data or the perception that private data may be available to unauthorized users.</td>
<td>1 hour</td>
</tr>
<tr>
<td>Level 2 - Urgent (Data Integrity)</td>
<td>The issue relates to the integrity of data being saved or viewed. No reasonable workaround is available.</td>
<td>1 hour</td>
</tr>
<tr>
<td>Level 3 - High (Availability)</td>
<td>The issue related to the availability of the Application, including all issues related to latency.</td>
<td>1 hour</td>
</tr>
<tr>
<td>Level 4 - Medium (Warranty)</td>
<td>The issue relates to a bug impacting normal use of the Application as it was intended or configured to perform.</td>
<td>1 business day</td>
</tr>
<tr>
<td>Level 5 - Medium (Information Request)</td>
<td>Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; request for a System change.</td>
<td>2 business days</td>
</tr>
</tbody>
</table>

**Support Escalation Table**

- All Severity Level 1 and 2 issues should be escalated to the 3rd level of the Escalation Table at the time of issue submission.
- All Severity Level 3 issues should be escalated to the 1st level of the Escalation Table at the time of Issue submission.
- Any Incident handling that does not achieve its objective response time for its Severity Level or for which a resolution plan is viewed as unsatisfactory by either party should be escalated to the next level, and to each successive escalation level until satisfaction is achieved.

<table>
<thead>
<tr>
<th>Level</th>
<th>ClientTrack Resource</th>
<th>Licensee Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st Level</td>
<td>Support Manager</td>
<td>Project Manager</td>
</tr>
<tr>
<td>2nd Level</td>
<td>Director-level Contact</td>
<td>Director-level Contact</td>
</tr>
<tr>
<td>3rd Level</td>
<td>Corporate Officer Contact</td>
<td>Corporate Officer Contact</td>
</tr>
</tbody>
</table>

**Disposal**

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

**Encryption**

The application is accessed by users via a secure HTTPS connection to the software web application server. The HTTPS protocol, which is designed to prevent eavesdropping and tampering, provides a secure communication channel to the application.
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 or Look-Up 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. Hard copy records containing PPI must be disposed of through means such as cross cut shredding and pulverizing.

3. When HMIS Participating Agency or Look-Up Agency staff is not present, the information must be secured in areas that are not publicly accessible.

4. 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 CoC’s HMIS Lead.
Update Log

Created: January 30, 2014

Reviewed and Reapproved: March 18, 2015
August 29, 2016
September 11, 2017

Elizabeth G. Hersh
Director, City of Philadelphia Office of Homeless Services

John Ducoff
Co-Chairperson, Philadelphia Continuum of Care Board

Date 9/12/17

Date 9/11/2017

Attachments
  ⇒ Information Security Policy Access Control
  ⇒ Information Security Policy Physical and Environmental Security
  ⇒ HMIS Vendor: Comprehensive Data Security, Privacy, and Confidentiality Policy and Plan for HIPAA
  ⇒ HMIS Vendor: Hosting and Security

Revised: June 1, 2017

HMIS Security Plan
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 andAuthentication

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 Phone: (215) 686-8180).
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 Phone: (215) 686-8180).
Eccovia Solutions uses industry best practices for data access, hosting, and security and partners with companies who meet stringent standards for uptime, security, and performance. Our solutions are hosted with ViaWest, an IT solutions provider that has been in business for more than 16 years. ViaWest operates 29 data centers in seven states and Canada.

Our hosting facility, ViaWest’s Cornell data center, is a SSAE 16 Type II Certified facility. The network is fully redundant and the database environment is designed with Availability Groups to ensure customer access. The ClientTrack platform is hosted in the HIPAA Compliant Cloud, a private server cloud purpose-built for the heavily regulated healthcare sector. It provides an audit-ready Compliance-as-a-Service (CaaS) solution to meet the IT and compliance needs for organizations that work with electronic Protected Health Information (ePHI).

The independent auditor reports or certifications that ViaWest obtains include:
- SSAE 16/ISAE
- SysTrust
- Service Organization Controls 1, 2, 3
- IPAA and HITECH physical controls
- PCI DSS Compliance
- NIST 800-53
- ITAR
- U.S./EU Safe Harbor Privacy

The HIPAA Compliant Cloud is designated HIPAA Audit Ready which means that the network design, security protocols, and measures and architecture go through rigorous audits to ensure data protection and security. The HIPAA Compliant Cloud offers enhanced security measures including expanded data monitoring, intrusion detection, change management monitoring, and data encryption for data at rest and in transmission.

The HIPAA Compliant Cloud is referenced, assessed and audited to HIMSS-Good Informatics Practices (GIP) specifications and procedures that have been used within the healthcare industry for more than a decade.

ViaWest’s data center facilities are accessible 24 hours a day and are staffed by employees skilled and experienced in hosting operations, data center management and customer service. The data centers are equipped with the latest environmental and security equipment, including redundant heating, ventilation and air conditioning (HVAC) systems; dry pipe and multi-zone fire detection systems; uninterruptible power supply (UPS); and generator backups for all data center operations. ViaWest has also implemented physical security measures, such as badge card access, personal identification numbers (PINs) and biometric fingerprint scans, and video surveillance with 24-hour monitoring by the local Data Center Customer Support (DCCS) or remote ViaWest Technical Assistance Service (VTAC).

Each data center maintains redundant links to the internet and other ViaWest data centers. Devices are configured to be monitored in the monitoring tool and are not accessible for management access outside the ViaWest network. Additionally, the network design supports redundancy for critical network components, and 24x7x365 monitoring procedures are in place to monitor ViaWest and customer systems. Monitoring systems are redundant to provide failover capability, and current network diagrams are available for use by authorized users.
## TECHNICAL SPECS OF THE VIAXWEST CORNELL DATA CENTER

<table>
<thead>
<tr>
<th>SECURITY</th>
<th>24x7 access via dual factor authentication</th>
<th>Monitored security cameras and intercom system</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>COMPLIANCE</strong></td>
<td>ViaWest has a dual standard SSAE 16 and ISAE 3402 Service Organization Control (SOC) 1 Type II, SOC 2 Type II, and SOC 3 reports covering each of ViaWest's data centers to include Operations, physical and environmental security controls</td>
<td>ViaWest also has facility-specific PCI DSS and HIPAA Reports of Compliance for physical security, information security policies and managed firewall services</td>
<td></td>
</tr>
<tr>
<td><strong>FIRE DETECTION &amp; SUPRESSION</strong></td>
<td>Certified data center smoke detection system</td>
<td>Certified incipient smoke detection</td>
<td>Dual-interlock pre-action dry pipe sprinkler</td>
</tr>
<tr>
<td><strong>POWER</strong></td>
<td>A and B source power circuit delivery capabilities Dual redundant 6.5 Megawatt power utility deliveries with onsite substations</td>
<td>10.4 megawatt diesel power generation capacity Automatic power switching</td>
<td>15,000 kVA UPS system capacity Redundant battery strings with monitoring</td>
</tr>
<tr>
<td><strong>HVAC &amp; ENVIRONMENTAL DESIGN</strong></td>
<td>3,760 tons of redundant cooling capacity</td>
<td>Anti-static raised flooring with designed cable runs and cold air delivery</td>
<td>Hot aisle/cold aisle configuration</td>
</tr>
<tr>
<td><strong>NETWORK</strong></td>
<td>Multiple redundant fiber optic telecommunication networks delivered via Telcordia/Bellcore standards with diverse conduit and entrance facilities</td>
<td>Industry leading VMware Technology</td>
<td>Cisco powered architecture</td>
</tr>
<tr>
<td><strong>VIAXWEST'S TECHNICAL ASSISTANCE CENTER (V-TAC)</strong></td>
<td>Single Point of Contact for all technical support needs for all remote calls</td>
<td>Available 24x7x365 by experienced TAC support engineers</td>
<td></td>
</tr>
<tr>
<td><strong>LOCAL DATA CENTER SUPPORT TEAMS</strong></td>
<td>On location – staffed 24x7x365 with Data Center Technicians (first real responders &amp; remote)</td>
<td>All Physical entry, environmental, power &amp; networks monitored real-time</td>
<td></td>
</tr>
</tbody>
</table>

www.eccoviasolutions.com
© Eccovia Solutions 2016
Comprehensive Data Security, Privacy, and Confidentiality Policy and Plan for HIPAA
ON THE CLIENTTRACK PLATFORM
DATA SECURITY, PRIVACY AND CONFIDENTIALITY

Work performed, and data managed by Eccovia Solutions includes data which may be the property of our customers, may include personal information, and may be subject to regulation under one or more federal or state privacy laws.

Eccovia Solutions respects privacy rights; thus, Eccovia Solutions is committed to protecting the privacy and confidentiality of the data and information in our care through the use of effective administrative, technical and physical safeguards for the protection of information. Eccovia Solutions uses industry standard best efforts to comply with federal and state laws, regulations regarding privacy, and confidentiality and security of data.

In general, compliance with such regulations can be achieved by broadly applying the relevant privacy standards of the Health Insurance Portability and Accountability Act (HIPAA) to protecting the privacy and confidentiality of the data and information in our care.

HIPAA Compliance
Eccovia Solutions embraces the Health Insurance Portability and Accountability Act, which is more commonly known as HIPAA. ClientTrack™ solutions are HIPAA compliant provided they are utilized properly.

Health Insurance Portability and Accountability Act was enacted in 1996. The initial focus of this bill was to provide a solution to the problem that some 25 million Americans who, if they changed jobs, risked losing ongoing health insurance because of preexisting medical conditions. HIPAA also addressed the privacy and protection of personal health care information by creating regulations which require effective administrative, technical and physical safeguards for the protection of personal information.

POLICY AND PLAN OBJECTIVE

The purpose of this policy and plan is to ensure the security and confidentiality of protected information; protect against any anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

Policy Statement
Eccovia Solutions and its employees will use industry standard best efforts to comply with the Health Insurance Portability and Accountability Act of 1996 including the use and disclosure of Protected Health Information in compliance with the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule") (45 C.F.R. Parts 160 and 164) under HIPAA; and, will each use industry standard best efforts to comply federal and state laws and regulations regarding privacy, confidentiality and security of data.

Eccovia Solutions will provide yearly education to its employees on HIPAA and encourage its customers, employees, and vendors to be aware of HIPAA and how affects them and their performance of duties. HIPAA Policy & Plan
Policy Scope
In formulating and implementing this policy and plan, Eccovia Solutions intends that all data and information belonging to Eccovia Solutions which Eccovia Solutions reasonably believes is confidential, proprietary or otherwise should be properly protected as private information shall be covered by this policy plan.

All data pertaining to ClientTrack customers and their clients disclosed to Eccovia Solutions by their customers in connection with the performance of services on behalf of such customers shall be covered by this policy plan. That is, Eccovia Solutions will safeguard the confidentiality of customer data using the same standard of care that Eccovia Solution uses for its own confidential materials.

Sanctions for Non-Compliance
Noncompliance with this policy by Eccovia Solutions personnel or vendors is unacceptable and will be subject to disciplinary action up to and including termination of the employment or vendor relationship. Violations of this policy may also be violations of applicable federal or states laws leading to prosecution, both as an individual or as an organizational entity, and criminal and civil penalties.

POLICY AND PLAN IMPLEMENTATION

In formulating and implementing this plan, Eccovia Solutions will appoint a “Data Security Coordinator” who will be responsible for:

A. Initial implementation of this plan;
B. Training employees;
C. Regular testing of the Plan’s safeguards;
D. Evaluating the ability of each of Eccovia Solutions’ third party vendors to comply with this policy and plan; and taking the steps reasonably necessary to ensure that such third party vendors are applying such privacy and information protective security measures that are at least as stringent as those required under this policy
E. Reviewing the scope of the security measures in this plan at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing covered information. Such reviews will include best efforts to:
   - Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing covered information;
   - Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the covered information;
   - Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
   - Design and implement safeguards to minimize those risks, consistent with the requirements of HIPAA regulations regarding “Business Associates of Covered entities”
   - Regularly monitor the effectiveness of those safeguards:
F. Conducting an annual training session for all owners, managers, employees and relevant individuals, including temporary and contract employees who have access to information covered under this plan. All attendees at such training sessions are required to certify their attendance at the training, and their familiarity with Eccovia Solution’s procedures and requirements for ensuring the protection of covered information.

Data Security Coordinator
Eccovia Solutions designates Terry Johnson, Chief Financial Officer to implement, supervise and maintain this plan under the general supervision of Eccovia Solution’s President, and CEO.

GENERAL PROVISIONS

To mitigate risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing covered information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately.

Data Confidentiality
In general, all data will be considered and kept as confidential. Release of data by individuals is permitted when the disclosure is necessary to properly perform the duties of the individual’s roles and responsibilities, but only to the extent that any such disclosure is necessary and legal; required by law or court order; or otherwise with proper permission.

Minimum Necessary Rule
All access to covered information will be limited to only that amount reasonably necessary to accomplish the legitimate business purpose for which the data is being accessed, used or otherwise disclosed.

Individuals accessing covered information will only do so after receiving proper permission; consistent with their role, assignment, and responsibility; and to the extent required to perform the specific action, activity or purpose for which the specific data is to be accessed. Such actions, activities and purposes must be legal, proper, and necessary in the performance of the individual’s duties and assignments.

Reasonable Care
Individuals accessing or utilizing covered information will use reasonable care to ensure that the data remains confidential and is not damaged, lost, or stolen. This reasonable care will include such actions as:

- Paper or electronic records (including records stored on hard drives or other electronic media) containing covered information shall be disposed of only in a proper manner.

- Employees are prohibited from leaving their workstations “logged-in” or keeping open paper materials and files containing covered information on their desks when they are not at their desks.
• At the end of the work day, all files and other records containing covered information must be secured in a manner that is consistent with protecting the security of personal information.

• To the extent reasonably feasible, files containing covered information residing on removable media or laptops should be encrypted utilizing and acceptable encryption utility such as: AxCrypt File Encryption Software.

Notice and Training
A copy of the plan will be available to each employee, or other relevant individuals, who will, upon receipt of this plan, acknowledge in writing that he/she has received a copy of this plan.

Eccovia Solutions will provide yearly education on the HIPAA and this plan. The training materials from the last annual training will be maintained for “at will training”.

Annual Review
All security measures shall be reviewed at least annually, or whenever there is a material change in our business practices that may reasonably implicate the security or integrity of records containing personal information. The Data Security Coordinator shall be responsible for this review and will fully apprise management of the results of that review and any recommendations for improved security arising out of that review.

Incident Reporting and Response
Employees are encouraged to report any suspicious or unauthorized use of covered information.

Should a violation of this plan or other incident occur where an inappropriate release of covered information occurs or may have occurred, the incident will be immediately reported to the Data Security Coordinator, Eccovia Solution’s President, and CEO, and other appropriate Eccovia Solutions management, who will appropriately investigate, respond, and make such notifications as may be prudent or required by law. (Nothing in this section should be interpreted to relieve any Eccovia Solutions employee or other individual from any and all actions which may be reasonable and required to prevent, mitigate or otherwise prevent the inappropriate release of covered information).

As soon as is reasonably practical, the Data Security Coordinator will undertake an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in this plan or security practices are required to improve the security of covered information. The Data Security Coordinator will fully apprise management of the results of that review and any recommendations for improved security arising out of that review. Incidents will be escalated and reported using the standard Eccovia Solutions processes.

INTERNAL RISKS
For the purposes of this plan “internal Risks” will be defined as those risks which may be associated with administrative, technical and physical factors related to the day-to-day business operation of
ClientTrack as performed by Eccovia Solutions personnel and vendors on a ClientTrack, customer, or vendor site.

To mitigate internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing covered information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately.

**Internal Risk Mitigation**

Employees' user-ID(s) and passwords will be changed periodically and “strong” (8 – 12 characters long inclusive of one capitol letter, one lower case letter, one number, and one special character) passwords will be utilized. Employees will not transmit or share identification or password codes to persons other than authorized users, permit the identification or password codes to be cached in proxy servers and accessed by individuals who are not authorized users.

Access to covered information shall be restricted to active users and active user accounts only. Access to electronically stored files containing covered information will be electronically limited to those employees having a unique individual log-in ID; and re-log-in shall be required when a computer has been inactive for more than a few minutes.

Employees are responsible to make and maintain appropriate backup of important data files, appropriately use file encryption and other security measure to protect the security of important data files, ensure that passwords are maintained securely and that they maintain a secured list of de-encryption password/keys to ensure that they (and Eccovia Solutions management if required) can decrypt files that they have encrypted. This list will be secured and maintained by Eccovia Solutions Controller.

Employees are responsible to comply with this policy and with the Eccovia Solutions employee handbook, which includes the following “Computer User Code of Ethics for Eccovia Solutions” (provided here for convenience):

- **Users should maintain secure passwords for all accounts assigned to them.**
- **Users should take precautions against others obtaining unauthorized access to their computing resources. This obligation applies particularly to users who are responsible for confidential information.**
- **Users should not willingly divulge passwords and other access control information for their personal accounts to any other person.**
- **Users must not use or attempt to use computing facilities or accounts to which they have not been granted explicit access by an appropriate system administrator.**
- **Users must use only those computing facilities and accounts for which they have proper authorization, provided by the Chief Technology Officer.**
- **Users must use computing facilities and services only for the purposes for which they were authorized.**
- **Specifically, ClientTrack Computing Accounts, Resources, Assets are to be used only in the course of conducting ClientTrack business.**
- **All files, data, information generated belong to Eccovia Solutions.**
- Specifically, Eccovia Solutions computing accounts must not be:
  - Used for private consulting or for any form of direct personal financial gain. (except for appropriate contract and external accounts).
  - Sold to any other person.
  - Provided as free resources to other persons for unauthorized purposes.
  - Personal uses of e-mail and instant messaging or unauthorized browsing.
- Users must respect all copyrights and licenses associated with Eccovia Solution's computing facilities. Terms and conditions in software licenses can vary considerably. The onus is on users/owners to familiarize themselves with their responsibilities and limitations under each software license agreement.
- Users must not attempt to:
  - Access and use software belonging to or licensed to other users or to ClientTrack without proper authorization to do so.
- Move or copy programs, subroutines and any other forms of software from one computing system to another without proper authorization. This includes personal computer, microcomputer and personal workstation software.
  - Duplicate, distribute, sell or otherwise make available software when such activity is prohibited by the license agreement for that software.
  - Access data or information stored on personal or Eccovia Solutions-owned computers without the permission of the owner or custodian of that information.
- Users must not attempt to interfere with the normal operation of shared systems.
- Users must not attempt to encroach on others' use of computing facilities or to deprive others of resources.
- Users must not attempt to subvert the restrictions associated with their computing accounts.
- Users must not use computing facilities to send or receive obscene, vulgar, data, information, or harassing messages.
- Users must not attempt unauthorized access to computing installations outside of ClientTrack using Eccovia Solutions' computers or communications facilities. More generally, users must adhere to all conditions associated with agreements between Eccovia Solutions and external network providers.
- Although system administrators may attempt to provide and preserve security of files, account numbers, passwords and programs, it is possible that security can be breached through action or causes beyond reasonable control. Users are therefore urged to safeguard data and to take full advantage of file security mechanisms built into systems (for example by changing passwords as often as necessary). System administrators of shared facilities have a responsibility to inform users of their obligations in the use of these systems.
- All data, information from emails, instant messaging, communications, is available to the company for purposes of managing the security and code of ethics.
- Protect all data in accordance with this document.

Terminated employees must return all records containing personal information, in any form, that may at the time of such termination be in the former employee's possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)
A terminated employee's physical and electronic access to personal information must be immediately blocked. Such terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the firm's premises or information. Moreover, such terminated employee's remote electronic access to personal information must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated.

The Data Security Coordinator will ensure that Eccovia Solutions maintain a highly secured master list of all relevant lock combinations, passwords and keys. Security will be maintained by the Controller.

Visitors shall not be permitted to visit unescorted any area within our premises that contains covered information.

In furtherance of this policy and plan, each department manager may develop rules (bearing in mind the business needs of that department) that ensure that reasonable restrictions upon physical access to records containing covered information are in place, including a written procedure that sets forth the manner in which physical access to such records in that department is to be restricted; and each department must store such records and data in locked facilities, secure storage areas or locked containers. Employees are notified and warned that such rules will be enforced under the "Sanctions for Noncompliance" provision of this policy and plan.

EXTERNAL RISKS

For the purposes of this plan "External Risks" will be defined as those risks which may be associated with administrative, technical and physical factors related to the day-to-day unauthorized physical or electronic access to ClientTrack electronic or physical infrastructure. This section specifically excludes issues related specifically to the ClientTrack™ application suite and/or ClientTrack™ data centers. These risks are discussed elsewhere in this policy and plan.

To mitigate internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing covered information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately.

External Risk Mitigation

All Eccovia Solutions servers, workstations and internal networks devices will be protected behind reasonably up-to-date firewall and Internet VPN appliance(s).

All Eccovia Solutions servers, workstations (including laptops) will be maintained with reasonably up-to-date operating systems, operating system security patches, and security agent software which includes antiviral / malware protection.

To the extent reasonably feasible, all covered information and files transmitted across public networks should be encrypted with at least a 128-bit encryption algorithm.
ClientTrack systems administrators will use best efforts to monitor systems for unauthorized use of or access to covered information and will make use of secure user authentication protocols and password location and format that does not compromise the security of the data they protect. Default vendor-supplied default passwords will be changed to make use of strong passwords.

Eccovia Solutions’ physical facilities will be protected by appropriate entry locks and alarm systems. Employees are required to appropriately secure, lock and arm alarm systems for all work areas when not in use.

Any breach of security will be escalated and reported based on Eccovia Solutions standard processes.

**CLIENTTRACK™ DATA CENTERS**

Eccovia Solutions will locate all servers and associated Application Service Provider (ASP) infrastructure and ClientTrack™ Software as a Service (SaaS) in SAS-70 Type II data center environments.

Within this data center environment, servers and associated Application Service Provider (ASP) infrastructure will be deployed in a fault-tolerant manner designed to meet or exceed published ClientTrack™ SaaS service level agreement levels.

Eccovia Solutions will utilize industry standard SSL Certificates and 128-bit SSL encryption as implemented through the Microsoft .NET and SQL 2005/2008 standard encryption platform.

**CLIENTTRACK™ COMPLIANCE FEATURES**

ClientTrack™ utilizes industry standard SSL Certificates and 128-bit SSL encryption as implemented through the Microsoft .NET and SQL 2005/2008 standard encryption platform.

The ClientTrack™ Service Oriented Architecture (SOA) resides on a foundation consisting of the industry-leading Microsoft .NET framework and Microsoft SQL Server relational database system. ClientTrack™ adds a Data Access and Security Component layer through which all transactions and data passing in and out of the database must flow. This layer ensures that data is always contained within a comprehensive security and privacy protected environment. As data is accessed via ClientTrack™ the Data Access and Security Component, all security rules related to that data are enforced and the currently logged-in user's credentials are presented and revalidated by the Data Access and Security Component.

This security includes these key components:

- *Access to electronically stored information is limited to those employees having a unique individual log-in ID; and re-log-in shall be required when a computer has been inactive for more than a few minutes.*
• Required use of strong passwords and access to user identification after multiple unsuccessful attempts to gain access is blocked.
• Access to information is restricted to active users and active user accounts only.
• Active Accounts are automatically deactivated based upon a system defined (default of 90 days) inactivity period.
• Audit trail usage and transaction monitoring
• ClientTrack™ system defaults password expiration based on best practice

ClientTrack™ workgroups, workflows utilizing conditional logic and rules-based configurability provide for the ability to meet the “Minimum Necessary Rule” including role-based information access.

ClientTrack™ provides the ability to have a separate Designated Record Set for each covered entity and provides for the appropriate exchange of data between covered entities based upon electronic “Memorandum(s) of Understanding (MOUs), which provide procedural and rules based enforcement of data sharing / “do not share” activities.

ClientTrack™ whole database export and soft delete functionality provide capability for data integrity, business continuity, and records retention compliance.

The ClientTrack™ platform is architected to scale from deployment on a single server or seamlessly across multiple clustered database servers and large farms of web servers. This provides the ability to meet high availability and business continuity requirements.

REVIEW TABLE:

<table>
<thead>
<tr>
<th>Date</th>
<th>Reason</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/10/2010</td>
<td>Annual Review</td>
<td>//Dario Benavidez//</td>
</tr>
<tr>
<td>5/10/2011</td>
<td>Annual Review</td>
<td>//Dario Benavidez//</td>
</tr>
<tr>
<td>3/23/2012</td>
<td>Minor edits</td>
<td>//Dario Benavidez//</td>
</tr>
<tr>
<td>3/23/2013</td>
<td>Minor edits/ Annual Review</td>
<td>//Dario Benavidez//</td>
</tr>
<tr>
<td>3/2/2015</td>
<td>Annual Review</td>
<td>//Terry Johnson//</td>
</tr>
<tr>
<td>8/10/2016</td>
<td>Annual Review</td>
<td>//Mickey Wright//</td>
</tr>
</tbody>
</table>