7. Access Control

All City of Chicago (“City”) employees must be positively authenticated and authorized prior to gaining access to all computer assets. Access controls must be in place to ensure that information access is provided on a minimum necessary, as needed basis. Appropriate access controls must be implemented commensurate to the sensitivity and risks assumed by the storage of data.

This policy reviews the following policy areas:

7.1 Business Requirements for Access Control

7.1.1 Access Control Policy

7.2 User Responsibilities

7.2.1 Clear Desk and Clear Screen Policy

7.2.2 Unattended User Equipment

7.2.3 Password Use

7.3 User Identification

7.3.1 User Registration

7.3.2 User Identification

7.3.3 Default Accounts

7.3.4 Third Party Account

7.4 Authentication

7.4.1 Password Standards

7.4.2 Inactive Accounts

7.4.3 Session Restrictions

7.4.4 Secure Network Controls

7.4.5 Secure System Login

7.5 Authorization

7.5.1 Review of User Access Rights

7.5.2 Privileged Access

7.6 Remote Access

7.6.1 Mobile Computing and Remote Access

7.7 Revision History
7.1 Business Requirements for Access Control

Proper access controls must be placed around all City computer assets and limited to only those persons whose jobs require such access. Asset access must be properly documented and granted only when required. Access to data must be made through a formal request process.

7.1.1 Access Control Policy

Access to information to all City of Chicago system components must be documented and restricted.

a. Technical Operations and Enterprise Network Architecture is responsible for ensuring that physical and logical access controls are established.
   HIPAA: 164.308(a)(1), ISO: 11.1.1, PCI: 7.2.1, 12.5.4

b. Technical Operations and Enterprise Network Architecture is responsible for ensuring that access rights granted and revoked from systems are approved using an authorization form signed by Application Owners. Access rights granted to systems must be limited to the minimum access rights necessary for the user to fulfill their responsibilities as determined by their role. Technical Operations and Enterprise Network Architecture must document user access authorization and approval for requested privileges via a service ticket or an access request form (ARF), which must be retained in accordance with organization retention policies.
   HIPAA: 164.308(a)(4)(B), ISO: 11.1.1, PCI: 7.1, 7.1.3

c. Technical Operations and Enterprise Network Architecture must ensure that each user is authorized to use the system for which access is granted, and that user IDs & passwords must be implemented in accordance with the scope of the authorization.
   PCI: 8.5.1

d. For users with similar duties, groups or role-based access controls (RBAC) must be used to assign access to individual accounts based on job descriptions, duties or function
   HIPAA: 164.312(a)(1), ISO: 11.1.1, PCI: 7.1.2, 7.2.2

e. The Information Owner must work with Technical Operations and Enterprise Network Architecture to remove access to information as soon as that access is no longer needed. It is the responsibility of both the Information Owner and the employee’s Manager to see that access privileges are aligned with the needs of the business, assigned on a need-to-know basis, and the proper access lists of authorized users are communicated.
   HIPAA: 164.308(a)(3)(C), ISO: 11.2.2

f. Technical Operations and Enterprise Network Architecture must ensure that all access to confidential data is administered via an automated access control system.
   PCI: 7.1.4

g. Technical Operations and Enterprise Network Architecture must ensure that all access to computer systems is controlled by an authentication method involving a minimum of a username and password combination. The username and password combination must provide verification of the user’s identity. Based on risk, two-factor authentication should be implemented.
   HIPAA: 164.312(d), ISO: 11.2.3, PCI: 12.3.2, 8.1, 8.2

h. Technical Operations and Enterprise Network Architecture must ensure that an access control mechanism is established for system components with multiple users that restricts access based on a user’s need to know, and should be set by default to “deny all” unless specifically allowed.
   HIPAA: 164.312(a)(1), ISO: 11.1.1, PCI: 7.2.3
i. Technical Operations and Enterprise Network Architecture must ensure that there is a default “deny-all” setting on all technical platforms. Administration accounts or accounts that can override system or application controls must be based upon job function and necessity. These privileges must only be allocated on a need-to-have basis.
HIPAA: 164.308(a)(4)(C), ISO: 11.2.2, PCI: 7.1.1

j. Departments must use the access request process to immediately notify the Department of Innovation and Technology of a change in employment status (such as when a User takes a leave of absence, transfers departments, or is terminated). The account of a User on a leave of absence can be retained, suspended, or deleted at the discretion of the User’s department.
7.2 User Responsibilities

All City employees must maintain a clear working environment to avoid theft of information or information systems.

7.2.1 Clear Desk and Clear Screen Policy

Special controls for office equipment must be in place (e.g., password-protected screensavers, cable-locks on all portable desktop equipment).

a. Users must ensure that private hardcopy information is kept in a secure, locked location.
   ISO: 11.3.3
b. Users must ensure that all incoming and outgoing mail points, facsimile machines and photocopiers are protected against unauthorized use or interception.
   ISO: 11.3.3
c. Users must ensure that passwords are not written down or stored on information systems in an unprotected form.
   Users must not hard code any username/passwords in scripts or clear text files such as system shell scripts, batch jobs or word processing documents.
   HIPAA: 164.308(a)(5)(D), ISO: 11.2.3

7.2.2 Unattended User Equipment

Users must log off of information systems manually or automatically when no longer using the systems.

a. Users must log-off all information processing systems when they are finished using them. This includes:
   • Point of Sale Systems (via pin, token, card swipe, etc.)
   • Servers;
   • Corporate desktops, laptops; and
   • Networking devices.
   HIPAA:164.310(b), ISO:11.3.2
7.2.3 Password Use

a. All IDs and accounts which permit access to any computer resource (e.g. e-mail, server, network, etc.), must be password protected. All new accounts will be created with a temporary password. The temporary password must be changed upon first use.

b. Mobile devices must be password protected; this includes but is not limited to personal digital assistants (PDA), smart phones, laptops, desktops, tablets, handhelds (e.g. Blackberries, smartphones, etc.).

c. Passwords used on the City’s systems and on non-City systems that are authorized for use must have the following characteristics unless otherwise approved by the Department of Innovation and Technology:
   - Passwords must be a minimum of 8 characters in length;
   - Passwords must contain both alphabetic and numeric characters;
   - Passwords must not be the same as the username;
   - Passwords must not contain proper names or words taken from a dictionary;
   - Passwords must be changed at minimum every 90 days;
   - Passwords used for production systems must not be the same as those used for corresponding non-production system such as the password used during training
   - Passwords must be unique for each system, site and/or environment.

d. Passwords must not be disclosed to anyone.

e. Group passwords and/or shared passwords are explicitly prohibited.

f. All passwords are to be treated as Confidential information.
7.3 User Identification

All City system users, including third party users, must have a unique identification number and be registered on the systems they use to conduct business. Additionally, default accounts must be removed from systems to avoid potentially unwanted access.

7.3.1 User Registration

Users must follow registration procedures (e.g., obtain a user id, change the default password, etc.) prior to accessing a new system.

a. Technical Operations and Enterprise Network Architecture must ensure that user registration, modification, and de-registration procedures are implemented for user access rights on all information systems. These procedures must be documented and include:
   - Proper authorization from Information Owners to gain access to systems or information resources;
   - Sign-off and verification that access granted is the same as the access requested;
   - A process for verifying that the access granted to users is appropriate for the business purpose;
   - A reconciliation process for verifying which users are valid users;
   - A process for ensuring that redundant user IDs are identified and corrected;
   - A process for immediately removing system access following user role changes or users leaving the organization;
   - Maintaining a record of all persons provisioned for the service and a history of user registration activities based on organizational retention requirements.
   ISO: 11.2.1, PCI: 8.5.1

b. Technical Operations and Enterprise Network Architecture must ensure the initial passwords are unique. All initial passwords must meet City password composition standards. The user must be forced to change their password upon initial logon, and user credentials should never be provided via insecure communication methods (e.g. email, instant messaging, etc.)
   HIPAA: 164.308(a)(5)(D), ISO: 11.2.1, 11.2.3

c. When new voicemail accounts are created, initial passwords must contain a minimum of five (5) unique numbers.
   ISO: 11.2.1
7.3.2 User Identification

Users must provide unique user identification prior to gaining access to City of Chicago information assets.

a. Technical Operations and Enterprise Network Architecture must ensure that access to all "non-Public" classified data (see Data and Asset Classification Policy) be controlled by an approved authentication method (e.g. ID and Password).

b. Technical Operations and Enterprise Network Architecture must ensure that all City employees have their own unique username for access to City network and systems. Individual or group sharing of usernames and passwords is strictly prohibited.
   
   PCI: 8.1, 8.5.8

HIPAA: 164.312(a)(1)(i), ISO: 11.5.2

PCI: 8.5.6

HIPAA: 164.312(a)(1)(i), ISO: 11.2.3

e. Technical Operations and Enterprise Network Architecture must ensure that all users that have access to privileged accounts have their own personal accounts for normal business use. Normal user accounts must be used to access accounts that cannot be tracked, such as shared super user or privileged accounts. Shared super user or privileged accounts must never be logged into directly if their usage cannot be tracked.
   
   HIPAA: 164.312(a)(1)(i), ISO: 11.5.2

7.3.3 Default Accounts

Default, system, and non-user accounts must be safeguarded to prevent unauthorized access to City information assets.

a. Technical Operations and Enterprise Network Architecture must ensure the default vendor passwords are changed immediately following installation.
   
   HIPAA: 164.312(d) ISO: 11.2.3 PCI: 2.1.1

7.3.4 Third Party Account

Additional security measures must be implemented to monitor the use of contractor or vendor accounts and ensure the ongoing security of City information assets.

a. Technical Operations and Enterprise Network Architecture must ensure that any accounts used by contractors or vendors are only activated during the time period needed to complete the current maintenance task.
   
   PCI: 8.5.6
7.4 Authentication

Authentication to all City information systems must be governed by strong password composition guidelines in addition to strong session.

7.4.1 Password Standards

Password standards for construction and sharing must be properly documented and enforced.

a. Security awareness training must communicate password procedures and policies to all City of Chicago employees.
   PCI: 8.5.7

b. Technical Operations and Enterprise Network Architecture and Application Development must ensure that specific procedures are implemented to verify a user’s identity prior to conducting a password reset. Where a user requests a password reset by phone, email, web, or other non-face-to-face method, appropriate user verification practices will be employed before the password is reset.
   PCI: 8.5.2

c. Technical Operations and Enterprise Network Architecture must ensure that computers, databases, and applications that store user account and password information restrict access only to authorized operations personnel and that all password information is rendered unreadable during transmission and storage on all system components using strong cryptography based on approved standards.
   HIPAA: 164.308(a)(5)(D), ISO: 11.5.3, PCI: 8.4

d. Technical Operations and Enterprise Network Architecture is responsible for ensuring that any interactive password system used employs the following:
   - Requiring users to be uniquely identified by means of a user ID and password combination;
   - Allowing users to create and change their own passwords;
   - Requiring passwords to be confirmed by the user;
   - Requiring passwords to meet quality and complexity requirements;
   - Enforcing password changes at regular intervals;
   - Enforcing users to change initial passwords assigned to new accounts at first log-on;
   - Maintaining a history of previously used passwords for each individual and preventing their re-use;
   - Concealing passwords as they are entered into systems;
   - Storing passwords in separate locations from operational information and data; and
   - Storing and transmitting passwords in a secure fashion.
   - User names and passwords must be transmitted in separate channels.
   HIPAA: 164.308(a)(5)(D), ISO: 11.5.3

e. Technical Operations and Enterprise Network Architecture must ensure that users create passwords that are a minimum of eight (8) characters in length and also comprised of letters, numbers, and special characters to the extent possible.
   HIPAA: 164.308(a)(5)(D), ISO: 11.3.1, PCI: 8.5.10

f. Technical Operations and Enterprise Network Architecture must ensure that systems are configured to automatically lock out a username after a minimum of 6 invalid login attempts. Lockout duration must be set to a minimum of 30 minutes, or until an administrator manually unlocks the account.
   PCI: 8.5.13, 8.5.14
g. Technical Operations and Enterprise Network Architecture must ensure that information systems use password history techniques to maintain a password history of users. The history file must contain the last 4 passwords of users and store them in an encrypted form. Users must not be allowed to use a password contained within specific user's password history. 
HIPAA: 164.308(a)(5)(D), ISO: 11.2.3, PCI: 8.5.12

h. Users must be forced to change passwords at least every ninety (90) days. Technical Operations and Enterprise Network Architecture must enforce this through technical means by enabling password aging controls on systems. HIPAA: 164.308(a)(5)(D), ISO: 11.2.3, PCI: 8.5.9

7.4.2 Inactive Accounts

The City must implement specific procedures to ensure that inactive accounts are disabled or deleted in a timely manner. Accounts that meet the criteria noted below may be disabled or deleted without warning.

a. Technical Operations and Enterprise Network Architecture must ensure that user accounts that have not been accessed for 90 days are automatically disabled. 
HIPAA: 164.308(a)(8), ISO: 11.2.3, PCI: 8.5.5

b. Technical Operations and Enterprise Network Architecture must ensure that after 180 days of inactivity, accounts are deleted.

7.4.3 Session Restrictions

Computer sessions that are not being actively used will be automatically terminated or locked.

a. Technical Operations and Enterprise Network Architecture must ensure that systems terminate user sessions or require the user to reenter their password after 15 minutes of inactivity has been reached. 
HIPAA: 164.312(a)(1)(iii), ISO: 11.5.5, PCI: 12.3.8, 8.5.15

7.4.4 Secure Network Controls

Network access controls must be implemented to ensure only authorized devices are allowed to access the City’s network.

a. Non-City owned computer assets are not permitted to use or connect to the City’s private, enterprise network. Exceptions can only be granted by Technical Operations and Enterprise Network Architecture. Exceptions must be documented and renewed every six (6) months.

b. Technical Operations and Enterprise Network Architecture must implement network access control technologies within the PCI environment to limit access to the City of Chicago Network to only authorized systems. 
PCI: 9.1.2
7.4.5 Secure System Login

Controls must be in place to ensure the security of user credentials and the identity of the organization are safeguarded throughout the login process.

a. Prior to a successful login, Technical Operations and Enterprise Network Architecture must ensure that remote service banners (e.g. SSH, FTP, VPN) do not identify the City, any specific physical location or hostname. ISO: 11.5.1

b. Technical Operations and Enterprise Network Architecture must ensure the log-on banners for the City's information processing devices and systems inform the user that:
   - The system is to be used only by authorized users;
   - By continuing to use the system, the user represents that he or she is an authorized user; and
   - The use of this system constitutes consent to monitoring.
   ISO: 11.5.1

c. Technical Operations and Enterprise Network Architecture must ensure that systems do not provide users with any login information prior to successful login. The login process must not disclose which portion of login sequence (user ID or password) was incorrect.
   HIPAA: 164.308(a)(5)(D), ISO: 11.5.1

d. No network protocols or communication methods will be used that transmit passwords in clear text (e.g. FTP, telnet, rsh, rlogin, rexec, etc.).

e. Technical Operations and Enterprise Network Architecture must ensure that systems providing authentication services do not transmit passwords in clear text. Passwords must not be visibly displayed on the system when being entered into the system.
   HIPAA: 164.308(a)(5)(D), ISO: 11.5.1, PCI: 2.3
7.5 Authorization

All authorized users must be authenticated before granting access to any City system. Information systems must be reviewed regularly in order to ensure proper authorization for access.

7.5.1 Review of User Access Rights

Information Owners are responsible for reviewing system privileges on a periodic basis and must promptly revoke or amend privileges no longer required by users.

a. Technical Operations and Enterprise Network Architecture and Information Owners must ensure that privileges assigned to employees transferring or changing job responsibilities are reviewed and re-allocated as determined by their new role.
   HIPAA: 164.308(a)(3)(C), ISO: 11.2.4

b. Technical Operations and Enterprise Network Architecture and Information Owners must ensure that all special or privileged access to systems (such as administrative or supervisor accounts) are reviewed quarterly. Any changes made to privileged accounts must be logged and periodically reviewed.
   HIPAA: 164.308(a)(4)(C), ISO: 11.2.4

c. Information Owners are responsible for reviewing system privileges on a periodic basis and must promptly revoke or amend privileges no longer required by users. Reviews must be performed twice yearly. It is the responsibility of the Technical Operations and Enterprise Network Architecture to ensure that Information Owners are provided with the proper reports to review current user access.
   HIPAA: 164.308(a)(4)(C), ISO: 11.2.4

7.5.2 Privileged Access

Additional safeguards must be implemented to protect accounts of elevated or privileged access. All authorized access must be requested, approved and signed by the Information Owner. The documentation must be retained in compliance to retention standards.

a. Technical Operations and Enterprise Network Architecture is required to ensure the utilities capable of overriding system and application controls or used to perform low-level system maintenance must:
   - Be identified and have procedures in place for authorizing their use;
   - Make use of authentication processes before allowing user access;
   - Be segregated from application systems;
   - Be restricted to a very limited group of authorized users;
   - Have time restrictions and limitations attached to their use;
   - Have their authorization levels documented;
   - Be disabled or removed if they are deemed unnecessary;
   - Not be used by users who have segregation of duties responsibilities for the related systems or applications;
   - Be stored off-line if not required on a daily basis; and
   - Include logging facilities to record their use.
   HIPAA: 164.312(a)(1), ISO: 11.5.4

b. Prior to access being given, Information Security Office is responsible for ensuring that the authorization is obtained from Information Owners.
   HIPAA: 164.308(a)(4)(B), ISO: 11.2.2
7.6 Remote Access

Proper security controls must be placed around all devices providing remote access capabilities to adequately restrict access to City’s network and infrastructure.

7.6.1 Mobile Computing and Remote Access

a. All remote access into the PCI or HIPAA network zones must use two-factor authentication. HIPAA: 164.312(d), ISO: 11.5.2, PCI: 8.3

b. All mobile devices and removable media that contain confidential information must have full disk encryption enabled per the encryption standards laid out in the Information Exchange Management policy.

c. Personal media devices (for example, MP3 players such as iPods) must not be used as peripheral devices on City-issued workstations.

d. Remote access is provided by the City as an information conduit to assist in the accomplishment of municipal duties and goals. Any other use is strictly prohibited. Requests for remote access must have a valid business reason and be approved by Technical Operations and Enterprise Network Architecture and the Information Security Office.

e. All remote access connections must be through a secure, centrally administered point of entry approved by the City. Authorized remote access connections must be properly configured and secured according to City-approved standards including the City’s password policy. All remote desktop protocol implementations must be authorized by Technical Operations and Enterprise Network Architecture and the Information Security Office. Remote access through unapproved entry points or methods (e.g. pcAnywhere, LogMeIn, GoToMyPC, TeamViewer) is not permitted and will be terminated without notice when discovered.

f. Non-City owned computer equipment used for remote access must be approved and must also comply with the City’s standards. The City will not be responsible for maintenance, repair, upgrades or other support of non-City owned computer equipment used to access the City’s network and computer resources through remote access services.

g. Employees or contractors who utilize workstations that are shared with individuals who have not signed a Confidentiality Agreement with the City must ensure that the City’s data is removed or deleted after each use in accordance with the policies and standards for disposing confidential information from equipment.
## 7.7 Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Description</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/15/2013</td>
<td>0.5</td>
<td>Initial Draft</td>
<td>ISO</td>
</tr>
<tr>
<td>07/26/2013</td>
<td>1.0</td>
<td>Approved as Release Candidate v1</td>
<td>CISO</td>
</tr>
<tr>
<td>12/30/2013</td>
<td>2.0</td>
<td>Approved as Release Candidate v2</td>
<td>CISO</td>
</tr>
</tbody>
</table>