2. Physical and Environmental Security

Robust physical and environmental controls must exist to protect information assets and systems from unauthorized access and safeguard against environmental threats. Access to secured data areas and data system display mechanisms will be limited to individuals with an approved and demonstrated business need. Users are prohibited from using the City of Chicago’s (“City”) Data and Information facilities in any way that violates this policy, Federal, State, Municipal Law and Personnel Rules. A list of authorized personnel must be established and maintained regularly to reflect changes in personnel access privileges.

This policy reviews the following areas:

2.1 Equipment Security ........................................................................................................................................... 2
   2.1.1 Network Jacks and Cabling Security ........................................................................................................... 2
   2.1.2 Equipment Maintenance ............................................................................................................................... 2
   2.1.3 Data Center Environmentalism .................................................................................................................... 3
   2.1.4 Data Center Supporting Utilities .................................................................................................................. 3
   2.1.5 Removal of Property ..................................................................................................................................... 4
   2.1.6 Security of Off-Site Equipment .................................................................................................................... 4

2.2 Secure Areas .......................................................................................................................................................... 5
   2.2.1 Physical Security Perimeter ........................................................................................................................ 5
   2.2.2 Physical Entry Controls ............................................................................................................................... 5
   2.2.3 Securing Data Center Facilities .................................................................................................................... 6
   2.2.4 Working in Secure Areas ............................................................................................................................. 7
   2.2.5 Protecting Against External and Environmental Threats ........................................................................ 8

2.3 Auditing, Review, Certification and Termination of Access ................................................................................. 9
   2.3.1 Data Center Access Levels ........................................................................................................................ 9
   2.3.2 Audits, Certification and Termination of Access ......................................................................................... 9

2.4 Revision History .................................................................................................................................................... 10
2.1 Equipment Security

All City of Chicago ("City") information systems must be properly protected from potential physical and environmental threats to ensure the confidentiality, integrity, and availability of the data contained within.

2.1.1 Network Jacks and Cabling Security

Network jacks and cables must be properly secured from unauthorized physical access and environmental threats.

a. Technical Operations and Enterprise Architecture must restrict access to all publicly accessible network jacks or implement network access control to restrict access to network resources to unauthorized systems. HIPAA: 164.310(a)(1)(ii), ISO: 9.2.3, PCI: 9.1.2

b. Technical Operations and Enterprise Architecture must ensure additional cabling security for critical systems and may include one or more of the following:
   - Segregated, locked conduit rooms/boxes
   - Alternative routing or segmented cabling schemes
   HIPAA: 164.310(a)(1)(ii), ISO: 9.2.3

c. Technical Operations and Enterprise Architecture must ensure that all power and telecommunications equipment and cabling coming into information processing facilities from external sources are protected against deliberate or accidental interruption of service. This includes protecting control boxes, cables, wiring closets and other equipment from fire, vandalism, interception of communications or disruption of service.
   HIPAA: 164.310(a)(1)(ii), ISO: 9.2.3

d. Technical Operations and Enterprise Architecture must ensure that conduits for network cabling are protected against interference or interruption. This includes avoiding routes through public areas, segregation from power cabling to eliminate interference, and clearly identified labeling on equipment.
   HIPAA: 164.310(a)(1)(ii), ISO: 9.2.3

e. Technical Operations and Enterprise Architecture must ensure that all City network connections are removed and/or deactivated when a site is being vacated.
   HIPAA: 164.310(a)(1)(iv), ISO: 9.2.3

2.1.2 Equipment Maintenance

City of Chicago systems must be properly maintained by authorized individuals.

a. Technical Operations and Enterprise Architecture must ensure that all utilities (e.g. Uninterruptible Power Supply [UPS], generator) equipment is monitored in accordance with manufacturer specification and correctly maintained to ensure the availability, integrity and confidentiality of information contained within it.
   ISO: 9.2.4

b. Technical Operations and Enterprise Architecture must ensure that only authorized maintenance personnel are allowed to perform repairs and that all repairs or service work is documented.
   HIPAA: 164.310(d)(1)(iii), ISO: 9.2.4
2.1.3 Data Center Environmentalism

All new and remodeled computer or communications centers must be constructed so that they are protected against fire, water damage, vandalism, and other threats known or likely to occur at their respective locations.

a. Technical Operations and Enterprise Architecture must ensure that smoking, drinking and eating in computer processing rooms is strictly prohibited.  
   HIPAA: 164.310(b), ISO: 9.2.1  

b. Technical Operations and Enterprise Architecture must ensure that rooms adjacent to the data center do not pose a high risk to the data center itself.  
   HIPAA: 164.310(a)(1)(ii), ISO: 9.2.1

c. Technical Operations and Enterprise Architecture must ensure that walls surrounding computer facilities are non-combustible and resistant to fire for at least one hour. All openings to these walls (e.g., doors, ventilation ducts, etc.) must be self-closing and resistant to fire for at least one hour.  
   ISO: 9.2.1

d. Technical Operations and Enterprise Architecture must ensure that all computer equipment operates in a climate-controlled atmosphere at all times. Redundant ventilation must be provided in the event that air conditioning systems in data center facilities fail.  
   HIPAA: 164.308(a)(7), ISO: 9.2.1

e. Technical Operations and Enterprise Architecture must ensure that computer equipment is housed in an environment equipped with fire detection and suppression measures.  
   ISO: 9.2.1

f. Technical Operations and Enterprise Architecture must ensure that procedures exist for facilities management to test fire suppression system equipment at least once every 6 months. The test results must be documented.  
   HIPAA: 164.308(a)(7)(D), ISO: 9.2.1

g. Technical Operations and Enterprise Architecture must ensure that all computer room personnel are trained in the use of any automatic fire suppression systems, the use of portable fire extinguishers and in the proper response to smoke and fire alarms.  
   HIPAA: 164.308(a)(7), ISO: 9.2.1

2.1.4 Data Center Supporting Utilities

All utilities (e.g., water, electricity, etc.) must be adequate for the systems they are supporting. In addition, Disaster Recovery procedures must be properly documented.

a. Technical Operations and Enterprise Architecture must ensure that a suitable, redundant electrical power supply is in place to avoid power failures. Based on business criticality, the use of a back-up generator must be considered.  
   HIPAA: 164.308(a)(7)(B), ISO: 9.2.2

b. Technical Operations and Enterprise Architecture must ensure that UPSes are used for equipment supporting critical business operations to facilitate system availability or orderly system shutdown. UPS equipment must be checked on a regular basis to ensure it has adequate capacity and must be tested in accordance with the manufacturer's recommendations.  
   ISO: 9.2.2

c. Emergency power switches must be located in equipment rooms and other locations as necessary.  
   HIPAA: 164.308(a)(7)(C), ISO: 9.2.2
d. **Technical Operations and Enterprise Architecture** must ensure that a suitable, redundant telecommunications infrastructure is in place to avoid communication failures and single points of failure. Based on business criticality, the use of backup communications lines or providers must be considered.  
HIPAA: 164.308(a)(7)(B), ISO: 9.2.2

e. All utilities, (e.g., water, electricity, sewage and heating/ventilation) must be adequate for all systems they are supporting and must be inspected on a regular basis.  
HIPAA: 164.308(a)(7), ISO: 9.2.2

f. Disaster Recovery procedures must be documented to ensure proper fallback or fail-over processes for the following supporting utilities:

- Electrical power
- Communications
- HVAC

### 2.1.5 Removal of Property

Removal of City property from City premises must be authorized and logged.

a. Employees or contractors must not remove property from the City data center premises without prior authorization from **Technical Operations and Enterprise Architecture**. All individuals must be aware that spot checks may take place when leaving data center facilities.  
HIPAA: 164.310(d)(1), ISO: 9.2.7

b. **Technical Operations and Enterprise Architecture** must ensure that an inventory of all computing equipment (excluding employee laptops) removed from the City data center premises is logged out when removed and logged back in when returned.  
HIPAA: 164.310(d)(1)(iii), ISO: 9.2.7

### 2.1.6 Security of Off-Site Equipment

Authorized equipment and media taken outside City premises must be controlled, secured and protected.

a. Security standards documented within the security policy apply to all City technical equipment and information regardless of physical location.  
HIPAA: 164.310(b), ISO: 9.2.5

b. Employees that travel with a laptop or other equipment with sensitive information, including briefcases, personal digital assistants (PDAs) and portable hard drives, must be cautious and keep the items with them at all times. These items should not be included with checked luggage.  
HIPAA: 164.310(b), ISO: 9.2.5
2.2 Secure Areas

All City facilities must have controls in place to protect the assets contained within from physical and environmental threats. Access to facilities must be controlled at defined access points.

2.2.1 Physical Security Perimeter

A security perimeter must be established for all non-public City facilities. All visitors to non-public City facilities must be logged and escorted as required.

a. Facility Management personnel must ensure that a security perimeter is established for non-public City facilities. The strength of the security perimeter will be determined by an assessment of the risks and threats to the physical environment. Technical Operations and Enterprise Architecture is responsible for coordinating additional security perimeter controls around data center facilities.

HIPAA: 164.310(a)(1)(ii), ISO: 9.1.1

b. The security perimeter for all of City's sensitive facilities should have a staffed reception area to control access to the main entry of the facility and appropriate controls to secondary entrances. For facilities without a staffed reception area, the perimeter must be controlled via access controls on doors and windows, and doors and windows must be locked at all times. Facility Management personnel must ensure that access is properly maintained.

HIPAA: 164.310(a)(1)(ii), ISO: 9.1.1

c. Technical Operations and Enterprise Architecture must ensure that all City buildings are separated into secure areas based on sensitivity. Based on the sensitivity of the secure area, additional physical security measures must be implemented to provide adequate protection.

HIPAA: 164.310(a)(1), ISO: 9.1.1

d. For all City facilities, Facility Management personnel must ensure that the security perimeter has alarmed fire control doors in accordance with local and organizational safety requirements.

ISO: 9.1.1

2.2.2 Physical Entry Controls

A process for restricting and monitoring physical access to City facilities must be implemented.

a. The Information Security Office must ensure that access rights to all data center facilities are reviewed, quarterly, and approved by an appropriate party. Those identified as having separated from the City or no longer have a business need to access the facility must be terminated.

HIPAA: 164.308(a)(4)(C), ISO: 9.1.2

b. Technical Operations and Enterprise Architecture must ensure that physical access to all non-public areas is tightly controlled. Doors must be secured at all times and only authorized personnel may have access.

HIPAA: 164.310(a)(1), ISO: 9.1.2

c. Badges must be worn by all employees, contractors, third party users and visitors and must clearly distinguish between visitors and employees. Temporary badges must expire after a set period of time. Badges must be visible at all times while in City non-public facilities.

ISO: 9.1.2, PCI: 9.3

d. All employees, contractors, vendors and visitors must report any lost identification badges immediately.

ISO: 9.1.2
e. All employees, contractors, vendors, and visitors must be authorized by an authorized member of the Technical Operations and Enterprise Architecture, Information Security Office, Human Resources or an appropriate approving party for physical entry into non-public City facilities. 
   HIPAA: 164.310(a)(1)(iii), ISO: 9.1.2

f. Authorized employees must not allow unknown or unauthorized individuals into restricted areas without an escort. Employees must notify Human Resources, Building Security and/or the Information Security Office of any unrecognized and unescorted personnel within a non-public area. Human Resources is responsible for escalating the situation as appropriate and notifying the appropriate parties, including the Information Security Office.
   HIPAA: 164.310(a)(1)(iii), ISO: 9.1.2

g. Visitor log information must be retained for a minimum of 90 days, and reviewed by the Information Security Office.
   HIPAA: 164.310(a)(1)(iii), ISO: 9.1.1, PCI: 9.4

h. Employees hosting visitors must ensure that their visitors are escorted when on a premises containing secure facilities.
   HIPAA: 164.310(a)(1)(iii), ISO: 9.1.1

2.2.3 Securing Data Center Facilities

Access to all City data center facilities must be monitored, authorized, and periodically reviewed to avoid unauthorized access.

a. Technical Operations and Enterprise Architecture must ensure that Data Center access is limited to only those people with a valid business reason for access. Access must be reviewed quarterly and revoked immediately once it is no longer needed.
   HIPAA: 164.310(a)(1)(iii), ISO: 9.1.3

b. Information Owners must ensure that directories and internal documents identifying locations of City’s information processing facilities or any other sensitive or secure area are not accessible by the public.
   ISO: 9.1.3

c. Technical Operations and Enterprise Architecture must ensure that all critical computer rooms and data centers, including those operated by third parties, are monitored 24 hours per day. This monitoring must include video surveillance and secured and alarmed doors. All data collected through this monitoring, including video surveillance, must be maintained for a rolling 90 day period.
   ISO: 9.1.3, PCI: 9.1.1

d. Technical Operations and Enterprise Architecture must ensure that unauthorized users are not permitted unsupervised access to the data center.
   HIPAA: 164.310(a)(1), ISO: 9.1.3

e. Technical Operations and Enterprise Architecture must ensure that data centers are not used for printing, faxing, storage of computers, or any other purpose other than to support City computer hardware and information assets.
   ISO: 9.1.3

f. Technical Operations and Enterprise Architecture must ensure that computer facility rooms are equipped with doors that automatically close immediately after they have been opened, and that set off an audible alarm when they have been kept open beyond a pre-determined period of time.
   ISO: 9.1.3
g. **Facility Management** personnel must ensure that rooms containing network, wiring or communications equipment (e.g., wiring closets, etc.) are locked at all times with access restricted to authorized personnel only. Signs are not to be posted on wiring closets, telephone rooms, data center facilities or other equipment components that would attract the attention of unauthorized individuals.

HIPAA: 164.310(a)(1), ISO: 9.1.3, PCI: 12.3.6

### 2.2.4 Working in Secure Areas

All work areas and the City material contained within must be secured to protect from physical threats.

a. **Technical Operations and Enterprise Architecture** with responsibility for a secure area are responsible for any person working in or having access to the secure area. The managers of secure areas must inform personnel that they are working in a secure area and advise them of any additional security requirements they must follow. The manager is also responsible for implementing any additional physical or procedural security requirements needed to protect information stored in the secure area.

HIPAA: 164.310(a)(1), ISO: 9.1.5

b. **Facility Management** personnel must ensure that any third party granted access to a secure area, including support services such as cleaning and waste removal, is strictly controlled and monitored. All parties with access to the area must be authorized and logged.

HIPAA: 164.310(a)(1)(iii), ISO: 9.1.5

c. Recording equipment such as photo, video and audio is not permitted within a secure area unless specifically authorized by **Information Security Office**.

HIPAA: 164.310(b), ISO: 9.1.5

d. During any relocation of an employee’s workspace, the relocating employee must ensure that all information assets are protected during the moving process. This includes, but is not limited to, computer and hard copy files.

HIPAA: 164.310(d)(1)(iv), ISO: 9.1.5

e. Employees must collect all printed documents (e.g., printouts, faxes, and photocopies) in a timely manner. Printers, faxes and photocopiers in secure work areas must be checked regularly (at least every day after business hours) for prints which are not collected. **Uncollected items must be destroyed or secured until the proper owners of the documents are available.**

HIPAA: 164.310(b), ISO: 9.1.5, PCI: 9.6

f. Employees must ensure that all information on whiteboards or work boards is wiped after use.

ISO: 9.1.5
2.2.5 Protecting Against External and Environmental Threats

All City facilities must be properly protected and/or separated from potential external and environmental threats.

a. Facility Management personnel must ensure that any hazardous or combustible materials are stored at a safe distance from any secure area in accordance with local safety regulations and manufacturer specifications. ISO: 9.1.4

b. Facility Management personnel must ensure that appropriate firefighting equipment is available at all sites. Equipment must be checked periodically. All firefighting equipment location and maintenance must be in compliance with local fire regulations. HIPAA: 164.308(a)(7)(C), ISO: 9.1.4

c. Technical Operations and Enterprise Architecture must ensure that backup and recovery media and facilities are located at a safe distance from main facilities. The backup facilities must be at a distance that would protect them from damage from any incident at the main site(s). HIPAA: 164.308(a)(7)(A), ISO: 9.1.4
2.3 Auditing, Review, Certification and Termination of Access

The Information Security Office will review swipe card usage for the Data Center monthly. Any questionable access will be investigated and the necessary staff will be contacted to appropriately resolve an incident.

2.3.1 Data Center Access Levels

Access to the Data Center, by way of a HID swipe card, assigned to authorized individuals. A swipe card assigned to an individual cannot be loaned to another individual.

a. Escorted Access
   Escorted Access is granted to individuals that have an infrequent need for Data Center access. Individuals with Escorted Access be accompanied by a person with Authorized Access, and must sign in and out, in the Data Center access log and specify the reason for entry. They are required to provide identification on demand and leave the facility when requested to do so.

b. Authorized Access
   Employees that work inside the Data Center and other individuals that have been granted the access based a demonstrated business need have 24/7 access to the Data Center. Persons requesting Authorized Access must complete a Data Center Authorized Access Application.

c. Vendor Access
   Approved vendors with HID Cards may be granted unescorted access to the Data Center to perform scheduled maintenance or repair work. Vendors not approved for Authorized access may be granted escorted access.

d. Data Center Tours
   Tours must be pre-approved by Technical Operations and Enterprise Architecture, or the Information Security Office. All visitors must sign in and out and must be escorted while touring the Data Centers.

e. Maintenance and Custodial Access
   Custodial staff access is limited to the times they are assigned to work in the Data Center. All Custodial Staff must sign the access log upon entering and leaving the Data Center. Maintenance staff must inform the Information Security Office of any maintenance work, and enter the maintenance work in the operations log.

2.3.2 Audits, Certification and Termination of Access

a. Data Center reports that provide information on individual access to the data center will be provided to the appropriate staff, managers and data center vendors, for verification and review.

b. The Information Security Office will review, quarterly, the access list for recertification. Those identified as having separated from the City or no longer have a business need to access the Data Center will be terminated.

c. The Information Security Office will request immediate termination of access rights of employees or vendors leaving the department. Human Resources Department or Approved vendors will notify the Information Security Office as part of an employee separation procedure.

d. Managers and Vendors will receive a report with the names of their staff that have access to the data Center. They should indicate which members have separated and/or no longer need access to the Data Center.
2.4 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>