Information Security and Technology Policy	Number 1.0		Policy Owner
	Policy Responsibility & Oversight		Department of Innovation and Technology
	Effective	**07/26/2013**	
	Last Revised	**07/26/2013**	

1. Policy Responsibilities & Oversight

The purpose of this Information Security Policy is to formalize the Security and Internal Control standards that the City of Chicago has adopted to mitigate security risks to employee and constituent data as well as to comply with applicable regulations including the Health Information Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Payment Card Industry's Data Security Standards (PCI-DSS).

In addition, this policy specifically defines how computing and communication assets, systems and resources should be accessed, configured, used and protected and the types of monitoring activities City personnel should execute to maintain the security of the City operating environment.

This document is published under the authority of the City's Chief Information Officer and provides a framework for safeguarding data and information including personally identifiable information (PII), protected health information (PHI) and payment cardholder data (cardholder data), including the creation, processing, management, transmission, storage, and disposal of information within the scope the City of Chicago.

This policy reviews the following areas:

1.1 Roles and Responsibilities

All employees, contractors and agents must support the information security program detailed herein.

1.1.1 Management Commitment to Information Security & Sponsorship

Management must approve and be committed to all Information Security initiatives set forth in this Information Security Policy. As such, management must identify a sponsor to drive assessment, compliance, and enforcement activities.

a. Ultimately, the Chief Information Officer will be responsible for compliance and enforcement activities associated with this Information Technology and Security Policy. The Information Security Office will be responsible for driving day to day activities and enforcement.
HIPAA: 164.308(a)(2).

b. The Information Security Office is the internal group responsible for managing and directing a city-wide information protection program. Specific responsibilities include:

- developing or coordinating the development of security policy, standards, guidelines and procedures;
- managing a data, application and platform classification program which includes the identification of information and application owners;
- ensuring the coordination of all corporate security-related functions (e.g., physical security, personnel security, the security of information stored in non-electronic form and incident response activities);
- identifying information protection goals and objectives within the scope of a strategic plan;
- identifying key information security program elements;
- identifying key corporate information security initiatives and standards;
- developing information security guidelines for personnel;
- developing and managing an information security program budget;
- ensuring the timely publication of approved information security related policies and procedures;
- coordinating information security awareness activities across the City of Chicago;
- taking appropriate action on security violations;
- coordinating information security for future initiatives related to privacy and security of data or other areas as deemed appropriate by the City Compliance Office; and
- Reporting on a regular basis to the City Compliance Office.

HIPAA: 164.308(a)(2), ISO: 6.1.1

1.1.2 Allocation of Information Security Responsibilities

Roles and responsibilities for ensuring support of the Information Security Policy must be assigned.

a. The City's Chief Information Officer is responsible for overall security of information assets and technology at the City. The CIO may delegate specific responsibilities related to information security to others within the City based on their job function. Specific responsibilities are assigned as follows:

- The responsibility to establish, document, and distribute security policies and standards is assigned to the Chief Information Security Officer. Should the Chief Information Security Officer position become vacant, this responsibility will be assigned to a security-knowledgeable member of management by the Chief Information Officer.

  PCI DSS 12.5.1

- The responsibility to establish, document, and distribute procedures and guidelines that are aligned to pertinent policies and standards is assigned to each support organization that is responsible for the delivery of the product or service.

  PCI DSS 12.5.1

- The responsibility to monitor and analyze security alerts and information, and distribute to appropriate personnel is assigned to the Chief Information Security Officer. Should the Chief Information Security Officer position become vacant, this responsibility will be assigned to a security-knowledgeable member of management by the Chief Information Officer.

  PCI DSS 12.5.2

- The responsibility to establish, document, and distribute information security incident response and escalation procedures to ensure timely and effective handling of all situations is assigned to the Chief Information Security Officer. Should the Chief Information Security Officer position become vacant, this responsibility will be assigned to a security-knowledgeable member of management by the Chief Information Officer.

  PCI DSS 12.5.3

- Overall responsibility for administering user accounts, including additions, deletions, and modifications, is assigned to the Head of Technical Operations and Enterprise Network Architecture. Should that position become vacant, this responsibility will be assigned to a security-knowledgeable member of management by the Chief Information Officer. Wherever additional user accounts may be required for a specific software application or Program, the responsibility for administering user accounts, including additions, deletions, and modifications, is assigned to the Program Manager responsible for that Program.

  PCI DSS 12.5.4

- The responsibility to monitor and control all access to data is assigned to the Head of Technical Operations and Enterprise Network Architecture for file, print, email and network access. Should the IT Director's position become vacant, this responsibility will be assigned to a security-knowledgeable member of management by the Chief Information Officer. For data that is created, maintained and/or managed in conjunction with a specific software application or Program, the responsibility to monitor and control all access to data is assigned to the Program Manager responsible for that Program.

  PCI DSS 12.5.5

b. The Information Security Office is responsible for coordinating the review of risks and security implications associated with the use of all technologies within the City's operating environment.
PCI: 12.3.1

c. An Information User is any City employee, vendor, contractor, or other authorized person who uses City information in the course of their daily work. Information User responsibilities include:

- maintaining the confidentiality of their user credentials;
- reporting suspected security violations to the Information Security Office;
- adhering to corporate information security policies, standards and technical controls; and;
- using City information resources responsibly and for authorized purposes only.

ISO:6.1.3, PCI:12.4

d. An Information Owner is a manager responsible for the City information assets. Individual business units or departments, not the Department of Innovation and Technology, own information. Information Owner responsibilities include:

- assigning initial information classification levels;
- periodic reviews to ensure current information classification meets the current business need and level of perceived risk;
- verifying that employee and third party access rights are current;
- determining security access criteria; and
- determining availability and backup requirements for the information they own.

ISO: 6.1.3

e. An Information Custodian is any the City employee, vendor, contractor, or other authorized person who has the responsibility for maintaining and/or supporting information. Information Owners have the right to delegate data maintenance and ownership responsibilities to Information Custodians. The Information Owner may designate one or more Information Custodians based on the level of delegated responsibilities. The Information Custodian must provide the following:

- assistance to the Information Owners in determining appropriate levels of data classification (see Information Classification (6.2)); and
- operationally provide assurance for the confidentiality, integrity and availability of information.

ISO: 6.1.3

f. System Administrators are required to maintain, operate and implement technology solutions for the City in accordance with the security policy. Access to servers is restricted to authorized System Administrators who are responsible for deploying, implementing and monitoring security controls on an operational basis. Guidance for the specific controls must be provided by Information Security Office. Responsibilities include:

- system security patch applications;
- system documentation;
- system performance;
- security monitoring;
- application of necessary technical security controls; and
- communication to Information Security Office on security related incidents and issues.

ISO: 6.1.3

g. The Information Security Office or a designated Internal Audit group is responsible for monitoring compliance with the standards and guidelines outlined by the security policy. If an Internal Audit group is designated, frequent communication between the Information Security Office and Internal Audit is critical to the protection of the City's information assets. The Information Security Office must aid Internal Audit by assisting in the identification of security threats and vulnerabilities throughout the City environment. These risks must be communicated appropriately so suitable mitigating controls can be put in place.
HIPAA:164.308(a)(8), ISO: 6.1.3

h. Technical Operations and Enterprise Network Architecture is responsible for the day-to-day data center operations. This includes the management of the Uninterruptible Power Supply (UPS) and all other environmental controls, in addition to racking new devices, pulling cabling, and operating network jacks. This team is also responsible for understanding, maintaining and operating the data center fire suppression systems.

i. Technical Operations and Enterprise Network Architecture is responsible for configuring and maintaining the City network. This includes implementing specific logical controls for segmenting the network and providing network access control.

1.1.3 Independent Review of Information Security

A review of the City environment must be conducted by either the Information Security Office or a designated internal audit team or an independent third party to identify any new threats and to ensure proper security controls are in place throughout the organization.

a. The City's security policy, standards and security environment must be reviewed annually. Any recommendations from this review must be resolved and considered for incorporation into the security policy and implemented as applicable. Determining the level of assurance is the responsibility of the Information Security Office and/or Internal Audit.
HIPAA: 164.308(a)(8), ISO: 6.1.8, PCI: 12.1.2

1.2 Information Technology and Security Policy Maintenance

The City of Chicago Information Security Policy must be approved, maintained, and annually reviewed in order to ensure its effectiveness.

1.2.1 Security Policy Approval

The Information Security Policy must be approved by management. Based on the review being conducted, all approvals must follow the pre-defined, documented information security policy approval process.

a. The Information Security Office is responsible for creating, reviewing and coordinating the approval and implementation of any security practices, policies, and standards.
HIPAA: 164.308(a)(2), ISO: 5.1, PCI: 12.5.1

b. The Information Security Office is responsible for ensuring that all security practices and standards are reviewed and approved on an annual basis.
ISO: 5.1

1.2.2 Additions & Changes to Policy

Any additions or changes to the Information Security Policy must be managed and approved. All additions to the information security policy must follow the pre-defined, documented information security policy change process.

a. Any business unit, group or department may initiate practice or standards development with the Information Security Office. The Information Security Office will analyze requests and address each at their discretion based upon this analysis.
ISO: 5.1

b. The Information Security Office is responsible for ensuring that all new information security policies and standards follow the existing practice structure and format of the information security policy or as deemed appropriate by the Chief Information Officer. At a minimum, the following tasks must be conducted for all new or changed information security policies:

   - A communication plan must be developed, at a minimum including notification of new practices, integration into security awareness materials, and special training for technical users/personnel (if deemed necessary);
   - An impact analysis must be conducted or coordinated by the Information Security Office prior to all information security policy changes to measure the risk and security implications driving the requested change and potential implementation requirements for full implementation of the changed policy;

   HIPAA: 164.316(b)(1)(ii), ISO: 5.1

1.2.3 Review of the Information Security Policy

An annual review of the Information Security Policy must be conducted to ensure relevance and identify any gaps in the policy.

a. The Information Security Office is responsible for initiating an annual review of the information security policy.
HIPAA: 164.308(a)(8), ISO: 5.2, PCI: 12.1.3

b. The Information Security Office must perform a technical review to ensure standards remain in sync with business requirements, vendor- and industry-recommended practices and current technology and regulatory requirements.
HIPAA: 164.308(a)(8), ISO: 5.2

c. The annual review must include a review of any impacting legal changes to ensure practice compliance with all applicable municipal, state and federal laws.
HIPAA: 164.308(a)(8), ISO: 5.2

d. The annual review results must be presented to the City's Chief Information Officer. All comments and requests made must be addressed and any modifications must be made via the Information Security Policy Change Procedures processes outlined by the Information Security Office.
ISO: 5.2

1.3 Revision History

Date	Version	Description	Author
01/15/2013	0.5	Initial Draft	ISO
07/26/2013	1.0	Approved & Released	CISO

Information Security and Technology Policy	Number 2.0		Policy Owner
	Physical and Environmental Security		Department of Innovation and Technology
	Effective	**07/26/2013**	
	Last Revision	**07/26/2013**	

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 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

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 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 City facilities. All visitors to City facilities must be logged and escorted as required.

a. Facility Management personnel must ensure that a security perimeter is established for City facilities. The strength of the security perimeter will be determined by an assessment of the risks and threats to the physical environment. The Technical Operations and Enterprise Architecture Management 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. 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 secure 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 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 secured 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 secure 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

Date	Version	Description	Author
01/15/2013	0.5	Initial Draft	ISO
07/26/2013	1.0	Approved & Released	CISO

Information Security and Technology Policy	Number 3.0		Policy Owner
	Personnel Security		Department of Innovation and Technology
	Effective	**07/26/2013**	
	Last Revised	**07/26/2013**	

3. Personnel Security

All employees are responsible for ensuring the security of City of Chicago (City) information Technology resources and data. Information security expectations must be clearly defined and communicated to all staff through targeted communications, training, and awareness programs. Appropriate disciplinary actions, in accordance with City of Chicago Personnel Handbook must be in place to address instances of non-compliance.

This policy reviews the following areas:

3.1 Acceptable Use

Information security, confidentiality, and copyright protection are matters of concern for employees of the City of Chicago ("City") and for all other persons who have access to City computer files and information assets, whether they are employees, vendors, consultants, or others. The City maintains information in the form of computerized files for City departments, boards, and agencies as well as other entities. The City utilizes computer software and methodologies created internally and by third parties who are protected by intellectual property, patent, copyright and trade secret laws. As such, the City is contractually obligated to prevent any and all unauthorized disclosure or use of these information assets.

3.1.1 Obligations

A position of trust has been conferred upon every authorized person who, as part of their job function, comes in contact with confidential information to keep this information secure and private. Both City employees and contractors are obligated to recognize and adhere to these responsibilities while on or off the job. Therefore, an employee of the City or a person authorized to access City data files and information is required:

a. To follow the City's privacy and security policies, standards and guidelines
b. Not to expose customers' or employees' confidential information (such as social security number, driver's license number, and credit card data or account information);
c. To maintain credit card data confidential and in full compliance of the current Payment Card Industry (PCI) Data Security Standards;
d. Not to expose health information (such as an individual's diagnosis or treatment) as protected by HIPAA privacy and security rules;
e. Not to engage in or permit unauthorized use of any information in files or programs maintained by the City;
f. Not to seek to benefit personally or permit others to benefit personally through the release of confidential information which has come to him/her by virtue of their job function or assignment;
g. Not to copy, alter, modify, disassemble, reverse engineer or decompile any intellectual property. Intellectual property that is created for the City by its employees, vendors, consultants and others is property of the City unless otherwise agreed upon by means of third party agreements or contracts;
h. Not to exhibit or divulge the contents of any City record to any person except in the conduct of his/her work assignment or in accordance with the policies of the City;
i. Not to disclose the specifics of non-public City related business to unauthorized personnel;
j. Not to remove or cause to be removed copies of any official record or report from any file from the office where it is kept except in the performance of his/her duties;
k. Not to use or request others to use the City's information technology for personal reasons beyond limited personal use as described in the Information Security Policy;
l. Not to conduct City business on devices that allow P2P communication (such as music file sharing) without explicit approval from the Department of Innovation and Technology;
m. To password protect mobile devices issued by the City or those authorized to connect to the City's information technology resources. Examples include but are not limited to: personal digital assistants (PDA), smart phones, laptops, handhelds (e.g. Blackberries) and off-site desktops;
n. To treat all passwords as Confidential information;
o. Not to aid, abet, or act in conspiracy with another to violate any part of this Confidentiality and Acceptable Use Policy;
p. To report any violation of this code by anyone to his/her supervisor immediately

3.2 Current Employees and Contractors

The Department of Innovation and Technology should define all IT related positions such that there is a clear separation of duties enforceable by the Access Controls defined in the Access Control Policy

All City employees and contractors must understand their specific responsibilities related to information security, as set forth in this Information Security and Technology Policy (I, as well as the consequences of not abiding by the IS Policy.

3.2.1 Employee and Contractor Responsibilities

All City employees and contractors are responsible for adhering to the IS Policy while in and outside of City facilities. For broader employee responsibilities, please see the City Employee Code of Conduct and the City Personnel Handbook.

a. All employees, contractors, vendors, and persons with access to City facilities and information must abide by the standards as documented in the security policy and include security as one of their core job responsibilities.
HIPAA: 164.308(a)(1)(C), ISO: 8.1.3

b. All employees, contractors, vendors, and persons with access to City of Chicago facilities are required to protect City of Chicago assets, both physical and logical, from any compromise of confidentiality, integrity or availability.
ISO: 8.1.1

c. Employees must maintain confidentiality of information outside of work and in remote access situations.
HIPAA: 164.310(b), ISO: 8.1.3

d. Employees must report any security incidents, potential security risks or vulnerabilities to the Information Security Office.
HIPAA: 164.308(a)(5)(C), ISO: 8.1.1

e. User information stored on or passed through City computer communications hardware is not considered private. Users of this equipment must not have expectations of privacy of any data or information, including electronic mail and voice mail.
ISO: 8.1.1

f. Human Resources must provide a copy of the information security policies and/or security awareness materials to new employees appropriate for their position and role within City of Chicago. New employees must acknowledge in writing that they understand their responsibilities as stated in the policies.
HIPAA: 164.308(a)(5), ISO: 8.1.1, PCI: 12.6.2

g. Employees and contractors are responsible for all actions taken by them or through their assigned access accounts.
HIPAA: 164.312(a)(1)(i), ISO: 8.1.1

3.2.2 Disciplinary Process

Violations of the Information Security and Technology Policy will result in disciplinary actions, coordinated through Human Resources as defined by the employee personnel Handbook. Any violation of this Policy, or any Part or provision hereof, may result in disciplinary action, including termination and/or civil action and/or criminal prosecution.

a. For City employees or contractors, disciplinary action as a result of the Information Security and Technology Policy violations must be consistent with the severity of the incident, as determined by an investigation. Disciplinary actions may include, but are not limited to, loss of access privileges to data processing resources, dismissal of consultants, cancellation of contracts, termination of employment, or other actions as deemed appropriate. Disciplinary actions are to be coordinated through Human Resources as defined by the employee personnel Handbook.
HIPAA: 164.308(a)(1)(C), ISO: 8.2.3

3.3 Prospective Employees

Prospective City employees must be adequately screened and understand the terms and conditions of employment prior to being hired.

3.3.1 Screening

A pre-employment screening, to include a criminal background check, process must be undertaken prior to offering employment to a new employee. Any information collected on the potential employee must be properly secured.

a. Human Resources must perform a pre-employment screening for all potential employees, including a background check to determine or validate a potential employee's qualification, past performance and appropriateness for a particular position.. If the employee is being hired via a third party or staffing agency, proper screening checks must be verified by that agency.
   HIPAA: 164.308(a)(3)(B), ISO: 8.1.2, PCI: 12.7

b. Information gathered on potential employees or contractors must be secured in accordance with all laws and regulations and be limited to a 'need to know' basis.
   ISO: 8.1.2

3.3.2 Terms and Conditions of Employment

All new employees are responsible for reviewing and understanding the Information Security and Technology Policy and procedures. Employees must agree in writing to accept and abide by the standards set forth in the IS Policy and may be required to sign a Non-Disclosure Agreement where applicable.

a. Contract staff, contractors, vendors or other third parties must be covered under a non-disclosure agreement under the third party contract. If persons under a third party's responsibility are to access confidential information, an individual confidentiality agreement must be signed by that individual
   HIPAA 164.308(a)(1)(C), ISO 8.1.3

b. Human Resources must ensure that all employees and relevant non-employees meet Information Security and Technology Policy requirements prior to accessing any City facilities that house confidential information.
   ISO: 8.1.3

c. Before gaining access to City information systems, all employees must:

   - Review of the IS Policy, or a synopsis thereof, and acknowledge their understanding and agreement to accept and abide by the standards as set forth in the IS Policy;
   - Acknowledge their understanding of City network monitoring, and sign appropriate confidentiality and non-disclosure agreements as required by the Employee Handbook.

     HIPAA: 164.308(a)(1)(C), ISO: 8.1.3

3.4 Termination or Change of Employment

Upon termination of employment with the City, the employee's access rights must be removed from all systems and all City assets must be returned by the employee. It is the responsibility of the employee's immediate supervisor or manager to initiate the required actions or process, based on the circumstances, to terminate access.

3.4.1 Removal of Access Rights

Access to all City information systems and information, physical locations, and other assets must be removed immediately for any terminated employee.

a. Employee Managers must immediately notify Human Resources upon the resignation or termination of any employee.
   HIPAA: 164.308(a)(3)(C), ISO: 8.3.1

b. Upon notification of termination, user provisioning processes must ensure that the terminated employee's user ID access is revoked or modified and any employee access badges are collected. Any access to confidential data must be removed immediately upon termination. Information Security Office is responsible for performing periodic audits ensuring this process is adequately functioning.
   HIPAA: 164.308(a)(3)(C), ISO: 8.3.3, PCI: 8.5.4

c. Upon termination of an employee or contractor, the person who requested access to technology resources must request the termination of that access using the City's access request procedure. In the event that the requestor is not available, the responsibility is placed upon the manager of the employee or contractor. The City may automatically disable or delete accounts where termination is suspected even if formal notification was by-passed.

3.4.2 Return of Assets

All information assets are the property of the City. All City assets must be returned by the employee immediately upon termination.

a. Any items issued to an employee or contractor such as laptop computers, keys, ID cards, software, data, documentation, manuals, etc. must be returned to their manager or Human Resources as appropriate, immediately upon termination.
   HIPAA: 164.308(a)(3)(C), ISO: 8.3.1

b. When an employee or contractor leaves the City, all Information Assets remain the property of the City. The employee or contractor must not take away such information or take away a copy of such information when he or she leaves the City without the prior express written permission of the City.

3.5 User Training

All City employees must be made aware of information security threats through a variety of physical, electronic, and verbal information security training and awareness programs. The City's Intranet site contains the City's Information Security Policies as well as educational materials, such as the "Security First" presentation. Employees should read the Security Reminders that are distributed periodically. System users must also respond to any Information Security Notice that is displayed while logging on to City systems.

3.5.1 Information Security Awareness, Education, and Training

Responsibility for training City employees on an annual basis must be assigned to ensure all employees are properly educated on security awareness. Security Awareness begins during the hiring process and it is the responsibility of the employee to remain aware of current security policies

a. The Information Security Office must create a security awareness, education, and training program to promote constant security awareness to all employees. The security awareness program must consist of training and continuous awareness briefings.
   HIPAA: 164.308(a)(5), ISO: 8.2.2, PCI: 12.6

b. Upon permanent or contract employment at City, all new employees must be briefed on the Information Security Policy and related procedures. A written summary of the basic information security measures must be provided to new employees and contractors and a signed copy must be kept on file in the employee folder maintained by Human Resources. Also, contractors must receive a copy of the non-disclosure agreement signed between the City and the contractor's employer.
   HIPAA: 164.308(a)(5), ISO: 8.2.2, PCI: 12.6.1

c. The Information Security Office is responsible for the development of security materials. These materials must define security requirements and expectations, legal responsibilities, and provide training in the proper use of City resources.
   HIPAA: 164.308(a)(5), ISO:8.2.2

d. The Information Security Office is responsible for posting security advisories for all system users who may be affected by security issues. Security advisories should include warnings about viruses, social engineering, new technical vulnerabilities and other specifics security risks to City as well as their associated counter measures.
   HIPAA: 164.308(a)(5)(A), ISO: 8.2.2

e. All employees and contractors must be briefed on information security awareness annually.
   HIPAA: 164.308(a)(5)(A), ISO: 8.2.2, PCI: 12.6.1, 12.6.2

3.6 Revision History

Date	Version	Description	Author
01/15/2013	0.5	Initial Draft	ISO
07/26/2013	1.0	Approved & Released	CISO

Information Security and Technology Policy	Number 4.0		Policy Owner
	Device Build and Configuration Management		Department of Innovation and Technology
	Effective	**07/26/2013**	
	Last Revised	**07/26/2013**	

4. Device Build and Configuration Management

A set of well-defined, enterprise device build and configuration management controls must be implemented across all City of Chicago (City) IT Infrastructure. The City must conduct an appropriate analysis of each platform's information security requirements and appropriate controls must be implemented to mitigate identified risks. An asset inventory of configured devised must be and updated to reflect the current infrastructure.

This policy reviews the following areas:

4.1 Security Requirements of Systems

An analysis must be performed on all critical information systems to determine appropriate security controls. Controls identified through this analysis must be dictated through City device build and configuration management standards.

4.1.1 Security Requirements Analysis and Specification

All platforms and enterprise applications being used within the City must undergo a security analysis to determine the controls needed to meet information security policy requirements. All software products must be formally tested for security functionality, including new software developed internally and software purchased from external parties.

a. Software Development must ensure that security requirements are determined prior to the application development phase for all systems. Application Development Management must ensure that these requirements are implemented during testing. System requirements must include specifications for:

   - Access control
   - Authorization
   - System criticality
   - Information classification
   - System availability
   - Information confidentiality and integrity

   ISO: 12.1.1

b. Software Development must ensure that a security assessment is conducted and control requirements are documented.

   ISO: 12.1.1

c. The Information Security Office must ensure that security requirements are defined and documented for all external software products purchased by the City. The Application Owner must ensure these guidelines are considered during product evaluation.

   ISO: 12.1.1

4.1.2 Platform/Device Build Standards

Platform and device build standards must exist to ensure proper security controls are placed around the information contained or transmitted by all devices in the City's environment.

a. IT Operations must ensure that technical build standards exist for all critical platforms and contain clearly defined, required security parameters. Such build standards must ensure that the platform requirements set forth in this information security policy are implemented and include the following:

   - each server in the cardholder data environment is allocated only one primary function;
   - unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers are removed from systems prior to use, and;
   - all unnecessary and insecure services and are disabled.

   PCI: 2.2.1, 2.2.2, 2.2.3, 2.2.4

   - Technical Operations and Enterprise Network Architecture Management, and Software Development must ensure that a common configuration management standard, which complies with the requirements set forth in this information security policy, is enforced across all devices and includes but is not limited to, Network Devices, City PCs, and Point of Sale Systems.

4.2 Revision History

Date	Version	Description	Author
01/15/2013	0.5	Initial Draft	ISO
07/26/2013	1.0	Approved & Released	CISO

Information Security and Technology Policy	Number 5.0		Policy Owner
	Application Development		Department of Innovation and Technology
	Effective	**07/26/2013**	
	Last Revised	**07/26/2013**	

5. Application Development

City of Chicago (City) staff and contract application developers must use a standardized development framework which requires specific information security steps, to ensure the protection of sensitive information, application availability, and data integrity.

This policy reviews the following areas:

5.1 Security in Development and Support Processes

A system development lifecycle methodology, in accordance with current industry best practices and standards for secure application development, must be followed. Clear segregation of duties must be established between release managers, testers, and developers in order to effectively manage viewing, changing, and migration of source code. Additionally, a technical review must be performed after each software change to ensure security standards are met.

5.1.1 Separation of Development and Production Environments

Appropriate requirements and controls must be in place requiring the physical separation of development, test and production environments.

a. Technical Operations and Enterprise Network Architecture must ensure that the production, test, and development environments are physically separated.

   ISO: 10.1.4, PCI: 6.3.2

b. Technical Operations and Enterprise Network Architecture must ensure that test environments emulate the production environment as closely as possible, including the use of a common operating system, database, web application server, and similar hardware to the degree possible.

   ISO: 10.1.4

c. Technical Operations and Enterprise Network Architecture must ensure that only authorized release managers and system administrators have access to the production environment where the production executable code for an application resides. Application developers may have read-only access to production log and configuration files as deemed necessary.

   HIPAA: 164.310(a)(1)(iii), ISO: 10.1.4

5.1.2 Segregation of Duties

Segregation of duties controls must be in place to manage the ability to view, change, and migrate source code. Developers, release managers, and testers must specifically be controlled in the actions they can take in the development, test, and production environments.

a. Application Development Management must ensure that specific segregation of duties controls are in place and that distinct, separate roles exist for developers, release managers, and testers.

   PCI: 6.3.2

b. Application Development Management must ensure that developers, release managers, and testers are restricted in the activities they can perform, as defined in the table below.

   PCI: 6.3.2

c. Separation of duties must exist between personnel assigned to the development/test environments and those assigned to the production environment.

PCI: 6.3.3

	Environment		
Role	Development	Test	Production
Developer	V, C	V	V
Release Manager	M	M	M
Tester		V	V

(V)iew: This action allows for the viewing of source code within the environment

(C)hange: This action allows for the changing of source code within the environment

(M)igrate: This action allows for the migration of code between environments

d. Application Development Management and Information Security Office must ensure that directories or repositories containing application source code are secured from unauthorized access.

HIPAA: 164.310(a)(1)(iii), ISO: 12.4.3

e. Application Development Management must ensure that access controls are developed to prevent unauthorized parties from gaining access to source code in an uncontrolled manner. This includes restricted access for developers to production systems and monitoring of access by developers to production systems during maintenance or support activities.

HIPAA: 164.310(a)(1)(iii), ISO: 12.4.3

f. Source code must not be stored on production systems when possible.

ISO: 12.4.3

g. Application Development Management must ensure that access levels restrict developers from making changes to the code maintained in the test environment during acceptance testing. When appropriate, a change control software tool must be utilized to ensure that programmers are adequately restricted from accessing production environments and testing environments.

HIPAA: 164.310(a)(1)(iii), ISO: 12.4.3

h. Application Development Management must ensure that all changes to code are logged in a central version control solution. To the extent possible, this solution should also log all access to source code files.

ISO: 12.4.3

i. Application Development Management must ensure that access and modification access is properly assigned. During acceptance and system testing, logical access restrictions must ensure that developers have no update access and that the code being tested cannot be modified without the consent of the user. The developer must make appropriate modifications in the development environment and submit it to the release engineer for retesting.

HIPAA: 164.310(a)(1)(iii), ISO: 12.5.1

5.1.3 Information Leakage

Controls must be implemented to prevent information leakage at system runtime.

a. Application Development Management must ensure that system information provided through error messages does not provide any information about an application's architecture or the City network.

   HIPAA: 164.310(a)(1)(iii), ISO: 12.5.4, PCI: 6.5.6

5.1.4 Outsourced Software Development

All outsourced development must be reviewed and approved by appropriate City personnel. In addition, all contracts for outsourced development must include the necessary provisions to ensure secure coding.

a. All contracts for outsourced development must be reviewed by the Department of Law and Application Development Management.

   ISO: 12.5.5

b. All code, software, or infrastructure provided by an outsourced development contractor must be reviewed and accepted in writing by the Application Development Management in conjunction with Information Security Office.

   ISO: 12.5.5

c. The Department of Law must ensure that all outsourced software development contracts provide protections for the City including the following:

   - Licensing arrangements, code ownership, and intellectual property rights
   - Service level agreements, including quality assurance and control of delivered software
   - "Right to audit" contractor's processes, infrastructure, development methodologies, security or any other control area deemed necessary by Internal Audit
   - Acceptance requirements

   ISO: 12.5.5

d. Application Development Management is responsible for monitoring all activity performed by software development firms engaged by the City.

   ISO: 12.5.5

e. Application Development Management or any business unit seeking to contract for outsourced software development must notify the Information Security Office prior to the release of any requests for proposal or information.

   ISO: 12.5.5

5.1.5 Technical Review of Applications after Changes

All software releases and updates/patches to production systems must to be tested for functionality and security.

a. After changes (e.g., patches, upgrades, or new versions), Application Development Management must ensure that applications and support processes are reviewed and tested as deemed necessary. These processes include but are not limited to the following

   - Application control and integrity procedures
   - Support and development plans for operating system changes
   - Proper notification of changes to user community
   - Updates to any applicable business continuity plans and/or recovery processes

   HIPAA: 164.312(c)(1), ISO:12.5.2

b. Application Development Management must ensure that all new or modified software, including the application of patches, is adequately tested, approved, and consistent with change and management standards before being deployed to the City's production environment. Such testing must include validation of input into the application, proper error handling, proper use of Role Based Access Controls (RBAC), secure cryptographic storage, and secure cryptographic communications as required for specific data and within the cardholder environment.

   ISO: 12.5.1, PCI: 6.3.1

c. Code changes must be reviewed by individuals (other than the originating code author) educated in the execution of code review techniques and secure coding practices, or by an automated code review tool approved by Application Development Management. Based on the code review results, appropriate corrections must be made, and the code review results must be reviewed and approved by management prior to release into production.

   PCI: 6.5, 6.3.7

d. Application Development Management must ensure that all significant modifications, major enhancements, and new systems undergo system testing prior to installation of the software in production. System stress testing, volume testing, and parallel testing should be performed as appropriate. System testing must be conducted in a separate, independently-controlled environment.

   ISO: 12.5.1

e. Application Development Management must ensure that all significant modifications, major enhancements, and new systems undergo acceptance testing by the appropriate Application Owners prior to installation of the software in production. The user acceptance plan must include tests of all major functions, processes, and interfacing systems, as deemed necessary.

   ISO: 12.5.1

5.2 Secure Coding Standards

Developers must be trained in secure coding techniques such as input validation and restricted error reporting.

5.2.1 Secure Coding Requirements

A secure coding standard must be utilized as part of the software development methodology.

a. All web-based applications must be developed based on a current version of the OWASP secure code guidelines, and must account for the following:

- Cross-site scripting (XSS) (validate all parameters before inclusion)
- Injection flaws, particularly SQL injection (validate input to verify user data, cannot modify meaning of commands and queries)
- Malicious file execution (validate input to verify application does not accept filenames or files from users)
- Insecure direct object references (do not expose internal object references to users)
- Cross-site request forgery (CSRF)
- Information leakage and improper error handling (do not leak information via error messages or other means)
- Broken authentication and session management (properly authenticate users and protect account credentials and session tokens)
- Insecure cryptographic storage (prevent cryptographic flaws)
- Insecure communications (properly encrypt all authenticated and sensitive communications)
- Failure to restrict URL access (consistency enforced access control in the presentation layer and business logic for all URLs)

PCI: 6.5.1, 6.5.2, 6.5.3, 6.5.4, 6.5.5, 6.5.6, 6.5.7, 6.5.8, 6.5.9, 6.5.10

5.2.2 Input Data Validation

Data entered into City application systems must be validated where possible to ensure information quality and mitigate the impacts of web-based attacks.

a. Application Development Management must implement data checks within information systems and applications to validate business transactions, standing/master data or parameter tables. Dual input checks, such as boundary checking or limiting fields to specific ranges of input data, must be used on critical inputs for systems when applicable. Checks may include:

- Out-of-range validation checks
- Invalid characters in fields
- Mandatory field definition
  HIPAA: 164.312(c)(2), ISO: 12.2.1, PCI: 6.5

b. Application development Management must ensure that all data input fields properly validate the input in order to minimize the threat of cross site scripting and SQL injection.

HIPAA: 164.312(c)(1), ISO: 12.2.1, PCI: 6.3.1.1

c. Application Development Management must ensure that data being entered into City application systems is validated where possible to increase information quality.

HIPAA: 164.312(c)(2), ISO: 12.2.1

d. An application firewall must be configured and placed in front of all externally facing web applications containing private data to detect and prevent external web-based attacks. Application Development Management must be involved in the configuration of the web application firewalls in order to ensure that application-specific requirements are properly accounted for.

PCI: 6.6

5.2.3 Developer Training

All City staff and contractor application developers must be properly trained in secure coding standards.

a. The City must ensure its developers are adequately trained in secure coding techniques, based on best practice guidance.

PCI: 6.5

5.3 Security of System Files

Operational systems must be configured according to the standards set forth in this policy prior to going into a production environment to ensure the security of the files contained within.

5.3.1 Control of Operational Software

All operational software must be an authorized version supported by the vendor, where applicable, and configured securely.

a. Application Development Management must ensure that operational systems only hold/store approved code. Development code or compilers must not be stored on production systems.

   HIPAA: 164.310(a)(1)(iii), ISO: 10.1.4, 12.4.1

b. Application Development Management must ensure that vendor-supplied software is maintained at a version supported by the vendor.

   ISO: 12.4.1

c. An audit log of all program updates must be maintained and a library of previous source code versions must be retained.

   HIPAA: 164.310(a)(1)(iii), ISO: 12.4.1

d. Application Development Management is responsible for archiving old versions of software along with configurations, parameters, procedures and other supporting documentation, as deemed appropriate.

   ISO: 12.4.1

e. Application Development Management must ensure that updates to operational software, applications and program libraries are performed by designated, trained personnel.

   HIPAA: 164.308(a)(1), ISO: 12.4.1

f. Application Development Management must ensure that all vendor-supplied default passwords are changed prior to the system being placed in a production environment.

   HIPAA: 164.308(a)(5)(D), ISO: 12.4.1, PCI: 2.1

g. Application Development Management must ensure that system default settings are reviewed prior to installation to determine potential security holes. Settings that could potentially compromise security must be changed prior to the system being placed into a production environment.

   HIPAA: 164.308(a)(1), ISO: 12.4.1, PCI: 2.1

5.3.2 Protection of Live Data in Test Environments

All data classified as private or higher used in any non-production environment must be altered or obfuscated.

a. Any unaltered production data used for test purposes in nonproduction environments must be approved by Information Owners and the Information Security Office. In the case where production data contains private data elements, the Department of Law must also provide written approval to use or copy production data for test purposes.

   HIPAA: 164.310(a)(1)(iii), ISO: 12.4.2

b. Production data consisting of payment card data must not be used for testing or development.

   PCI: 6.3.4

c. Application developers must ensure that test data, test accounts, custom application accounts, user IDs and/or passwords are removed before a system is implemented into production.

   PCI: 6.3.5, 6.3.6

d. Where production data is copied to a test system, Application Development Management must ensure that the data is subject to a similar level of control as the production version including all legal, regulatory, or security requirements. The controls must include:

   - Similar authorization methods and procedures for access to the data or test systems
   - Defined plan for deletion of data after testing has been completed
   - Audit log of activity and personnel accessing system and data
   - Similar access controls to production to ensure confidentiality of data is maintained

   HIPAA: 164.308(a)(4)(B), ISO: 12.4.2

5.4 Revision History

Date	Version	Description	Author
01/15/2013	0.5	Initial Draft	ISO
07/26/2013	1.0	Approved & Released	CISO

Information Security and Technology Policy	Number 6.0		Policy Owner
	Data and Asset Management		Department of Innovation and Technology
	Effective	**07/26/2013**	
	Last Revision	**07/26/2013**	

6. Data and Asset Management

A risk-based information data and asset classification scheme must be established in order to ensure that data is handled and managed appropriately. Data and computer assets must be classified in a manner that indicates the need, priorities, and expected degree of protection appropriate to the nature of the data and the potential impact of misuse.

This policy reviews the following areas:

6.1 Responsibility for Assets

All computer and information assets must be accounted for and have an assigned owner. Acceptable use of City assets must be understood by all employees and contingent staff.

6.1.1 Acceptable Use of Assets

The acceptable use of resources, information and assets must be documented and understood by all staff. Use of these resources is intended for business purposes in accordance with individual job function and responsibilities. Personal use which is limited and in accordance with the City's Ethics Ordinance, Personnel Rules and other Applicable Use policies is permitted. The limited personal use of information technology resources is not permissible if it creates a non-negligible expense to the City, consumes excessive time, or violates departmental policy. The privilege of limited personal use may be revoked or limited at any time by the City or department officials.

a. The Information Security Office is responsible for defining acceptable use of resources, information and assets including appropriate labeling and handling procedures. In the absence of specific guidance, Information Owners and Department Management are primarily responsible to develop recommendations and minimum standards.
HIPAA: 164.310(d)(1)(iii), ISO: 7.1.3, PCI: 12.3, 12.3.5

b. An up-to-date list of all technologies as approved/coordinated by Technical Operations and Enterprise Network Architecture must be maintained and readily available.
PCI: 12.3.7

6.1.2 Inventory of Assets

An inventory of all information assets, including systems, software, and service providers, must be kept current at all times.

a. Technical Operations and Enterprise Network Architecture must compile and maintain a data repository catalog on all third party software-related assets (e.g., application software, development tools and all third party purchased software). This catalog must be reviewed and updated annually. The catalog should contain descriptive asset information (e.g., vendor, logical locations/associated applications or systems, physical location (if applicable), owner/responsible party, information custodial responsibilities, information classification and criticality level). Business leaders are required to assist in maintaining this catalog and should communicate any changes or additions.
HIPAA: 164.310(d)(1)(iii) ISO: 7.1.1

b. Technical Operations and Enterprise Network Architecture must compile and maintain a data repository catalog of all physical assets owned by the City. This catalog must be reviewed and updated annually. The catalog must contain descriptive asset information. Business unit managers are required to assist Technical Operations and Enterprise Network Architecture in maintaining this catalog and should communicate any changes or additions in a timely manner.
HIPAA: 164.310(d)(1)(iii), ISO: 7.1.1, PCI 12.3.3

6.1.3 Ownership of Assets

Unless specifically identified and approved by the Legal Department, all information possessed or used by a particular department and all information stored and processed over the City's technology and information systems are the property of the City and must have a designated Information Owner. Users of the system have no expectation of privacy associated with the information they store in or send through these systems, within the limits of the federal, state and local laws of the United States and, where applicable, foreign laws.

a. All physical computing assets must have an assigned Asset Owner.

b. All production information possessed or used by a particular organization or business unit within the organization must have a designated Information Owner. Ownership and custodianship of assets must be documented. HIPAA: 164.310(d)(1)(iii), ISO: 7.1.2

6.2 Information Classification

Information classification is based on the level of sensitivity of the data and the potential impact of inappropriate handling should the confidentiality, integrity or availability of the information or data compromised. A classification scheme, which establishes the baseline security controls for safeguarding information, must be used to ensure appropriate security protections are placed around information during handling.

6.2.1 Information Classification Guidelines

An information classification scheme must be used throughout the organization to protect City of Chicago's assets.

a. The Information Security Office is responsible for defining the Information Data Classification scheme.

b. Information Technology Operations and Enterprise Network Architecture is responsible for management oversight of all IT assets and must define procedures for proper data identification and handling.
HIPAA: 164.308(a)(7)(E), ISO: 7.2.1, PCI: 9.7.1

c. Information Owners or an assigned Information Custodian is responsible for defining the classification of an information asset.
ISO: 7.2.1

d. It is the Information Owner or delegated Information Custodian's responsibility to monitor information assets and continuously review the information's classification. The Information Owner or delegated Information Custodian must sponsor a formal declassification effort before information can be downgraded to a lower classification, based upon the definitions of the classification.
ISO: 7.2.1

e. Employees, contractors, and vendors must protect all of the City's information in any format (e.g., hard copy, disk, tape, flash drive) at the level commensurate with its value as determined by its information classification. These standards mitigate the risk that information of different classification levels be inadvertently combined and released. Correctly classified information with proper controls can be instituted to manage the dissemination of information throughout the City’s environment.
HIPAA: 164.310(d)(1), ISO: 7.2.1

6.2.2 Information Classification Scheme

The City has a four-tier classification system consisting of “Public,” “Internal”, “Sensitive” and “Confidential” levels of classification. The Public, Confidential, and Internal classifications are driven by regulatory and business considerations.

a. **Public** Information is defined as information that is intended for unrestricted public disclosure and is not exempt from disclosure under the Illinois Freedom of Information Act (FOIA).

   Examples include open datasets, announcements, press releases and marketing materials, and employment advertisements.

b. **Internal** Information is defined as information that is related to the day to day operations of City departments and services. All internal data is subject to the Illinois Freedom of Information Act (FOIA) and if disclosed would have minimal to no impact on confidentiality, integrity, availability.

   Examples include most business documents, minutes of meetings, emails and data related to how City services are developed and delivered.

c. **Sensitive** information is defined as information that in isolation may not present any specific risk to the confidentiality, integrity or availability of City operations, resources or constituents but if combined with other data could represent inappropriate risk. Sensitive information can be exempt from the Illinois Freedom of Information Act (FOIA). FOIA exempt information must be approved the Legal Department.

   Examples include network diagrams, internet protocol (IP) addresses of computer assets, design documents, user manuals, procedure documents,

d. **Confidential** information is defined as information that if lost, disclosed, or inappropriately modified could cause significant impact to the confidentiality, integrity, availability of City operations, resources or constituents. Prior to designation, the “Confidential” classification must be approved by the Legal Department or Information Security Office. Confidential information is exempt from disclosure under the Freedom of Information Act (FOIA).

   Examples include information related to the City’s Information Security controls, means and methods all passwords and data defined as Card Holder Data (CHD-PCIDSS), Personal Health Information (PHI-HIPAA/) and Personally Identifiable Information (PII).

6.2.3 Information Labeling and Handling

All media must be labeled with its information classification to ensure the proper security controls are placed around the media while handling.

a. Information Owners are responsible for ensuring that all removable media containing non-public data is labeled with its information classification, owner, contact information and purpose.
HIPAA: 164.310(d)(1), ISO: 7.2.2, PCI: 12.3.4

b. Information Technology Operations and Enterprise Network Architecture Management is responsible for ensuring that efforts are made to separate confidential information from other information with specific security or control requirements.
ISO: 7.2.2

c. All employees are responsible for ensuring that any electronic information deleted from computer systems and discarded hard copy documents are destroyed in a manner to protect disclosure of the information to external parties commensurate with the information's business value or confidentiality.
HIPAA: 164.310(d)(1)(i), ISO: 7.2.2

d. Information Owners or designated Information Custodians are responsible for ensuring that all information with high criticality, business value, confidentiality, integrity or availability control requirements is secured in one of the following ways:
ISO: 7.2.2

- hard copy information must be kept in an access-controlled room which is secured when unoccupied or within locked file cabinets with limited access if a secured room is not available; and
- Private and Secret electronic information must be encrypted using an Information Security Office-approved method when stored on any media (e.g., hard drive, tape, compact disc, flash drive).

HIPAA: 164.310(a)(1), ISO: 7.2.2

e. Technical Operations and Enterprise Network Architecture Management or Information Custodians are responsible for ensuring that removable media containing Confidential and Sensitive data are stored in a locked container or room designated for the storage of such information (e.g., computer hard drives). As an alternative to physically securing the media, this information may be protected by approved encryption.
HIPAA: 164.310(a)(1), ISO:7.2.2

6.3 Revision History

Date	Version	Description	Author
01/15/2013	0.5	Initial Draft	ISO
07/26/2013	1.0	Approved & Released	CISO

Information Security and Technology Policy	Number 7.0		Policy Owner
	Access Control		Department of Innovation & Technology
	Effective	**07/26/2013**	
	Last Revision	**07/26/2013**	

7. Access Control

All City of Chicago (City employees must be positively authenticated and authorized prior to gaining access to 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

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 Confidential and Internal 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, and that access controls are driven by the business and the Information Security Office.
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. IT Operations 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 within 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. User accounts that have not been used for 90 days may be disabled without warning. After 180 days of inactivity, these accounts may be deleted without warning.

k. 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 laptops; and
   - networking devices.

   HIPAA:164.310(b), ISO:11.3.2

7.2.3 Password Use

a. All e-mail, network, domain accounts 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, tablets, handhelds (e.g. Blackberries, smartphones, etc.) and off-site desktops.

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:
   i. Passwords must be a minimum of 8 characters in length;
   ii. Passwords must contain both alphabetic and numeric characters;
   iii. Passwords must not be the same as the username;
   iv. Passwords must not contain proper names or words taken from a dictionary;

v. Passwords must be changed at minimum every 90 days;

vi. 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

vii. 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 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

b. Technical Operations and Enterprise Network Architecture must ensure that legacy group user IDs may only be used if there is a clear business case and are approved by both the Information Owners and the Information Security Office. The Information Owners must be aware of all the risks associated with using group IDs such as the loss of individual accountability.
   HIPAA: 164.312(a)(1)(i), ISO: 11.5.2

c. Technical Operations and Enterprise Network Architecture must ensure the users are limited to only one user account for each individual information system for non-administrative purposes. Any deviations from this, including application or special use accounts, must be approved by the Information Security Office.
HIPAA: 164.312(d), ISO: 11.2.3

d. 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;
- forcing 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 6 invalid login attempts. Lockout duration must be set to 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 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 deleted or removed 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 Network Access Control

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

a. Technical Operations and Enterprise Network Architecture must implement network access control technologies to limit access to the City of Chicago Network to only authorized, City-owned 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, VNP) 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. 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 Information Security Office 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.

Technical Operations and Enterprise Network Architecture must additionally ensure that all remote access into the City network use two-factor authentication.

HIPAA: 164.312(d), ISO: 11.5.2, PCI: 8.3

7.6.1 Mobile Computing and Remote Access

a. All mobile devices and removable media that contain sensitive or confidential information must have full disk encryption enabled per the encryption standards laid out in the Communications policy.

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

c. 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 DoIT.

d. 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 DoIT. Remote access through unapproved entry points will be terminated when discovered.

e. 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.

f. 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

Date	Version	Description	Author
01/15/2013	0.5	Initial Draft	ISO
07/26/2013	1.0	Approved & Released	CISO

Information Security and Technology Policy	Number 8.0		Policy Owner
	Network Security		Department of Innovation and Technology
	Effective	**07/26/2013**	
	Last Revised	**07/26/2013**	

8. Network Security

Network infrastructure must be configured securely in order to protect City of Chicago (City) information assets and maintain network integrity and availability. All employees and contractors must ensure that specific processes are followed to ensure that internal networks are not accessible to unauthorized external parties.

This policy reviews the following areas:

8.1 Network Administration/Security Management

Standards for properly securing network devices must be documented; and, all network devices within the City environment must be secured in accordance with these standards.

8.1.1 Device Configuration

Firewall and router configuration standards must be in place to ensure consistency in configuration and ensure security of the City network.

a. Technical Operations and Enterprise Network Architecture management must implement IP masquerading by using Network Address Translation (NAT) technologies such as Port Address Translation (PAT) to prevent internal network addresses from being translated and revealed on the Internet.

   PCI: 1.3.8

b. Technical Operations and Enterprise Network Architecture must ensure that external firewalls employ stateful inspection or dynamic packet filtering to allow only established connections into the City network.

   PCI: 1.3.6

c. Technical Operations and Enterprise Network Architecture management must ensure that routers are governed by a router technical configuration standard, and that security hardening of the routers is a component of the standard.

   PCI: 1.2.2

d. Technical Operations and Enterprise Network Architecture management must ensure that a common router configuration file is synchronized across all routers and that routers are not managed in a one-off fashion.

   PCI: 1.2.2

8.1.2 Network Documentation

Network configuration and topology must be adequately documented.

a. Technical Operations and Enterprise Network Architecture management must maintain appropriate network documentation, including a high-level network diagram specifically noting inbound and outbound network connections into areas containing private data, including wireless network components.

   PCI: 1.1.2

b. Application Owners are responsible for maintaining network documentation specific to the confidential and sensitive data environment, including transaction level detail highlighting the points at which confidential and sensitive data is transferred throughout the City of Chicago network and to external organizations. This documentation must be kept current to reflect any changes to network infrastructure or business processes associated with the confidential and sensitive data environment.

   PCI: 1.1.2

8.2 Networks

All internal networks and connections into and out of the internal network, including the DMZ, must be documented and managed.

8.2.1 Connection Approval

All devices connected to and any connections, inbound or outbound, must be properly documented by Technical Operations and Enterprise Network Architecture management and approved by the Information Security Office.

a. Technical Operations and Enterprise Network Architecture management must manage and implement a formal process for approving new external connections, inbound or outbound, to the City internal network, specifically requiring approval from the Information Security Office.

b. Technical Operations and Enterprise Network Architecture management must manage and implement a formal process for testing and approving all changes to external firewalls and routers. This process must clearly define the steps and requirements for adequate testing of the change and set forth a structure of approvals required to implement various changes.

   PCI: 1.1.1

a. Only City managed and approved computer assets may be connected to the City network. Exceptions may only be granted by Technical Operations and Enterprise Network Architecture or Information Security Office management. Unapproved devices can be disconnected and confiscated without notification.

8.2.2 Demilitarized Zone

Demilitarized Zones (DMZ) and network segmentation must be used between networks and other untrusted networks.

a. Technical Operations and Enterprise Network Architecture management must ensure that a DMZ has been implemented in order to limit traffic into the City network to only necessary protocols.

   PCI: 1.3.1

b. Technical Operations and Enterprise Network Architecture management must ensure that the DMZ is configured such that inbound Internet traffic is only allowed into the DMZ, and that no direct inbound or outbound traffic is allowed between the Internet and the confidential and sensitive data network.

   PCI: 1.3.2, 1.3.3, 1.3.5

c. Technical Operations and Enterprise Network Architecture must ensure that internal addresses cannot pass through the Internet into the DMZ.

   PCI: 1.3.4

d. Technical Operations and Enterprise Network Architecture management must ensure that any database containing cardholder data is placed securely on the internal network, properly segmented from the DMZ.

   PCI: 1.3.7

8.3 Firewalls

All firewalls and their associated rules within the City of Chicago network must be documented, approved, and managed. Firewalls must be installed and firewall configurations must be documented, approved, and maintained to protect confidential and sensitive data.

8.3.1 Use of Firewalls

Firewalls must be deployed to restrict inbound and outbound connections to the City of Chicago corporate network. Firewall configuration requirements must be in place that restrict connections between networks that are not managed by DoIT and any system components in the confidential and sensitive data environment

a. Technical Operations and Enterprise Network Architecture must ensure that firewalls are placed at each Internet connection and between any DMZ and the internal network.

   PCI: 1.1.3

b. Technical Operations and Enterprise Network Architecture management must ensure that personal firewalls are implemented on all laptop or employee-owned computers with direct access to the Internet and the City network.

   PCI: 1.4

c. Technical Operations and Enterprise Network Architecture management must ensure that firewalls are installed and configured to deny or control all traffic between any wireless networks and systems that store confidential and sensitive data.

   PCI: 1.2.3

8.3.2 Rule Management

Firewall rules must be implemented to prevent unauthorized access to the City of Chicago corporate network and must be reviewed regularly for adequacy. Requirements must be in place to prohibit direct public access between the Internet and any system component in the confidential and sensitive data environment

a. Technical Operations and Enterprise Network Architecture management must ensure that all traffic inbound and outbound to the confidential and sensitive data environment is restricted to those connections required by the confidential and sensitive environment. All other traffic must be specifically denied. Enterprise Network and Architecture management must ensure that all restrictions are appropriately documented.

   PCI: 1.2.1

b. Technical Operations and Enterprise Network Architecture management must ensure that the use of all services, protocols, and allowed ports are documented with a specific business justification.

   PCI: 1.1.5

c. The Information Security Office must ensure that a review of all firewalls and routers restricting access to the confidential and sensitive data environment are reviewed every six months. This activity must include a review of the specific ports/services/protocols allowed into the environment and proper documentation of the review.

   PCI: 1.1.6

8.4 Wireless Security

Proper security controls, such as authentication, logging, and encrypted transmission must be used for all wireless devices. Additionally, processes must be in place to detect rogue access points, manage users, and monitor access point usage.

8.4.1 Approval & Rogue Access Point Detection

A periodic process must be in place to identify and remove rogue access points connected to the City of Chicago corporate network.

a. The Information Security Office must approve the implementation of all wireless networks. Ad hoc wireless networks are not permitted.

b. The Information Security Office must ensure that rogue access points are not deployed anywhere throughout the City of Chicago network. As such, the Information Security Office must perform quarterly wireless scanning or deploy appropriate tools to identify rogue wireless access points. All identified rogue access points must be investigated and disabled.

   PCI: 11.1

8.4.2 System Configuration

All new wireless access points must be configured securely and approved by management to avoid unwanted access to the City of Chicago corporate network.

a. Technical Operations and Enterprise Network Architecture management must ensure that all wireless networks with access to the City of Chicago internal network implement WPA2 to adequately authenticate wireless systems/users and provide secure transmission of data.

   PCI: 4.1.1, 4.2

b. Technical Operations and Enterprise Network Architecture management must ensure that system default settings are reviewed with the Information Security Office before installation to identify potential security holes. Settings that could potentially comprise security must be changed before the wireless network is placed in a production environment. Specifically, Enterprise Network and Architecture management must ensure that default SSID's are not used and public SNMP community strings are changed.

   PCI: 2.1.1

c. Technical Operations and Enterprise Network Architecture management must ensure that all-vendor supplied default accounts (i.e., administrative and user) are changed prior to the system being placed in a production environment.

   PCI: 2.1.1

d. Technical Operations and Enterprise Network Architecture management must ensure that proper procedures are followed to ensure that wireless access point firmware is kept up-to-date. Updates to firmware must be performed by Enterprise Network and Architecture management.

8.4.3 Physically Securing Access Points

All wireless access points must be set up in a secure, unobtrusive location to avoid tampering.

a. Wireless access points should be positioned away from windows to minimize coverage outside of office premises and prevent ready access to the physical device (i.e., ceiling-mounted access points).

   PCI: 9.1.3

8.5 Revision History

Date	Version	Description	Author
01/15/2013	0.5	Initial Draft	ISO
07/26/2013	1.0	Approved & Released	CISO

Information Security and Technology Policy	Number 9.0		Policy Owner
	Communications Management		Department of Innovation and Technology
	Effective	**07/26/2013**	
	Last Revised	**07/26/2013**	

9. Communications Management

The way that City of Chicago (City) information is communicated must be clearly defined and managed. Employees and contractors are responsible for safeguarding their communications, no matter the form, to adequately protect the assets of City.

This policy reviews the following areas:

9.1 Exchange of Information

Employees and contractors exchanging business information, regardless of the medium (e.g., paper, electronic, verbal, etc.), must follow proper security procedures.

9.1.1 Information Exchange Policies and Procedures

Procedures must be developed that address the risks involved when exchanging information.

a. The Information Security Office must ensure that policies and procedures outlining the acceptable use of electronic communication facilities are established that:

- protect the exchange of information from interception, copying, modification, and destruction
- protect sensitive information included as attachments through the use of cryptography
- retain and dispose of business information in accordance with legislation and regulations
- remind employees, contractors and business partners of their responsibility to use City systems responsibly

HIPAA: 164.308(b)(4), ISO: 10.8.1

b. All employees, contractors, and other business partners must ensure that any data or media waiting to be distributed or produced is secured to a level consistent with its sensitivity. This includes:

- Printer spools on systems
- Printed materials awaiting distribution
- Printed materials awaiting pickup for external delivery services
- Media, such as backup tapes, awaiting pickup for off-site storage

9.1.2 Exchange Agreements

Business Associate agreements or Memoranda of Understanding must be formalized between the City and external parties prior to sharing data and establishing network connections to external systems.

a. The Information Security Office must be consulted to make specific considerations prior to interconnecting business information systems. Specific considerations must be based on the classification of data being shared, however, may include the following:

- Identify risks, threats, vulnerabilities, impacts and associated compensating controls and safeguards
- Determine which sensitive information is to be excluded from the system if an appropriate level of protection cannot be provided
- Determine restriction requirements for individuals working on sensitive projects
- Identify which users are employees, contractors and business partners
- Determine the backup and retention requirements of the system

ISO: 10.8.5

b. The Information Security Office, Department of Law, and the contracting business party must ensure that agreements that include an exchange of private City information must include:

- Management responsibilities and procedures for handling transmission, dispatch and receipt
- Procedures to ensure traceability and non-repudiation
- Packaging and transmission technical standards

- Responsibilities and liabilities of the contracting party in the event of information security incidents
- Ownership definition ad responsibilities for protecting data, copyrights and licensing
- Special controls for protecting private information.

HIPAA: 164.308(b)(1), ISO: 10.8.2, PCI: 12.8.2

9.1.3 Paper-based Information Transfer

Paper-based transfer of information must be used on an as-needed basis only and must follow proper handling procedures.

a. Any transfer of paper-based credit card holder data (CHD) or any other City sensitive or confidential data must be logged as part of a management-approved business process

   PCI: 9.7.2

b. Sensitive or confidential data must be sent to third parties approved by the respective Data Owners by way of commercial courier, shipping service, or other delivery method that can provide delivery confirmation.

   PCI: 9.7.2

c. Employees must ensure that any media sent via interoffice mail, courier, or other means are clearly labeled with the appropriate recipient information.

   HIPAA: 164.310(d)(1), ISO: 10.7.3

d. City information must only be generated in hard copy to the extent necessary to complete normal business operations. Copies of information must be kept to a minimum to better facilitate control and distribution. Sensitive and confidential information must be stored in locked drawers, cabinets, or rooms specifically designated for that purpose and accessible only by authorized individuals.

   HIPAA: 164.310(b), ISO: 10.7.3

e. All hard copy information must be disposed of properly by either shredding the information or leaving the information in secured, designated shredder bins.

9.1.4 Verbal Information Transfer

Employees must take caution when exchanging information verbally to avoid unnecessary transfers.

a. Discussions of or including sensitive or confidential information must not take place in public areas. These areas include but are not limited to elevators, hallways, public transportation, airplanes, etc.

b. Employees, contractors, and business partners must not leave messages containing sensitive or confidential information on any type of telephone voice message or answering machine or forward voice messages to an external destination.

   ISO: 10.8.1

9.1.5 Electronic Information Transfer

The electronic transfer of information must follow information classification guidelines to ensure the confidentiality and integrity of the information is maintained.

a. Copying, moving, and storing of sensitive or confidential data unto local hard drives or removable electronic media is prohibited without express permission from the Data Owner and Information Security Office.

   PCI: 12.3.10

b. IT Operations Management must ensure that payment card account numbers are masked when displayed on screens (the first six and last four digits are the maximum number of digits that may be displayed).

   PCI: 3.3

c. Employees may not forward email received at or sent from their City mailboxes to personal email accounts, nor may they use external mail aggregation services to manage their City email.

9.1.6 Removable Media Information Transfer

Transfer of information via removable media must be used on an as-needed basis only and must follow proper handling procedures.

a. Any transfer of removable media containing cardholder data or any other City sensitive or confidential data must be logged and authorized by the Information Owner, be sent in tamper resistant packaging and via a secured courier or other delivery method that can be tracked.

HIPAA: 164.310(d)(1), ISO: 10.8.3, PCI: 9.8

9.2 Encryption

A key-based encryption solution must be used by the City to protect sensitive and confidential data from unauthorized access while stored and in transit. Technical Operations and Enterprise Network Architecture must ensure that cryptographic key management processes and procedures are fully documented and including the following:

a. Cryptographic keys must be strong keys.

b. Cryptographic keys must be stored securely.

c. Cryptographic keys must be changed no less than annually.

d. Cryptographic keys must be retired securely and Cryptographic keys must be replaced if there is a known or suspected compromise. When a key is no longer needed, the original key and all of its copies must be destroyed in a manner such that it cannot be recovered.

9.2.2 Usage of Encryption

Encryption technologies must be approved and used where applicable.

a. The Information Security Office is responsible for validating all encryption software/algorithms used by the City, and maintaining/distributing an updated list of such technologies.

   HIPAA: 164.308(a)(2), ISO: 12.3.1

b. The Information Security Office must perform an annual review of the approved encryption algorithms and protocols.

   HIPAA: 164.308(a)(8), ISO: 12.3.1

c. Employees and contractors must not install any encryption software that has not been validated and approved by the Information Security Office.

   ISO: 12.3.1

d. Application Development Management and Technical Operations and Enterprise Network Architecture Management must ensure that only encryption software, algorithms and protocols approved by the Information Security Office are used to encrypt data in enterprise systems.

   ISO: 12.3.1

e. DoIT Senior Management reserves the right to request any key or password for encrypted files stored on City hardware. This includes passwords for files stored on local or network hard drives and portable media.

   ISO: 12.3.1

9.2.3 Key Management

Cryptographic keys used for encryption of sensitive or confidential data, including cardholder data, must be monitored and protected against both disclosure and misuse.

a. Employees and Contractors must treat keys (passwords or private keys) for encrypted data with the same level of confidentiality as passwords for systems or applications.

   HIPAA: 164.308(a)(5)(D), ISO: 12.3.1

b. Technical Operations and Enterprise Network Architecture must ensure that all hardware (either housing key management applications or used for generation of encryption keys) is protected at the highest level of security controls.

   ISO: 12.3.2

c. Any contractual or third party agreements involving encryption or key management must be approved by the Information Security Office and the Department of Law.

   ISO: 12.3.2

d. Technical Operations and Enterprise Network Architecture and the Information Security Office are responsible for jointly developing key management procedures as necessary for the organization. Procedures must be developed for the following:

   - Generation of keys
   - Management of public key certificates
   - Distribution of keys
   - Storage of keys
   - Revocation of keys
   - Rotation of keys (at least annually)
   - Key recovery
   - Archiving keys
   - Destroying keys
   - Key escrow

   ISO: 12.3.2, PCI: 3.6

e. Technical Operations and Enterprise Network Architecture is responsible for implementing monitoring and logging processes for all key management activities.

   ISO: 12.3.2

f. Technical Operations and Enterprise Network Architecture must ensure that access to cryptographic keys must be restricted to the fewest number of custodians necessary; and, cryptographic keys should be stored securely in the fewest possible locations and forms.

   PCI: 3.5, 3.5.1, 3.5.2

g. Technical Operations and Enterprise Network Architecture must ensure that dual control of cryptographic keys is in place and that all key management staff sign a form stating they understand and accept their key management responsibilities.

   PCI: 3.6.6, 3.6.8

h. The keys must be stored in an encrypted format and the key encrypting keys must be stored separately from the data encrypting keys

9.2.4 Data in Transit

All sensitive or confidential data in transit must be encrypted.

a. All employees and staff must ensure that data classified as sensitive or confidential is encrypted whenever sent over any network.

   HIPAA: 164.312(e)(1)(ii), ISO: 12.3.1, PCI: 4.1

b. All non-console administrative access must use appropriate encryption techniques/protocols (e.g. SSH, VPN, or SSL/TLS) to protect the confidentiality of City data.

   PCI: 2.3

c. Technical Operations and Enterprise Network Architecture must ensure that strong cryptography and security protocols such as SSL/TLS or IPSEC are used to safeguard sensitive cardholder data during transmission over open, public networks.

   PCI: 4.1

9.2.5 Data at Rest

Encryption must be used for sensitive and confidential data at rest throughout the City operating environment.

a. Technical Operations and Enterprise Network Architecture must ensure that payment card account numbers are rendered, at minimum, unreadable anywhere they are stored (including on portable digital media, backup media, in logs) by using any of the following approaches;

   - One-way hashes based on strong cryptography
   - Truncation
   - Index tokens and securely stored pads
   - Strong cryptography with associated key management processes and procedures
   - Disk encryption (Where disk encryption is used, logical access to encrypted file systems should be implemented via a mechanism that is separate from the native operating systems mechanism (e.g., not using local user account databases)).

   PCI: 3.4

9.2.6 Symmetric Key Encryption

Keys used for symmetric key encryption, also called secret key encryption, must be protected as they are distributed to all parties that will use them.

a. During distribution, the symmetric encryption keys must be encrypted using a stronger algorithm with a key of the longest authorized key length.
b. If the keys are for the strongest algorithm, then the key must be split, each portion of the key encrypted with a different key that is the longest key length authorized and the each encrypted portion is transmitted using different transmission mechanisms. The goal is to provide more stringent protection to the key than the data that is encrypted with that encryption key.
c. Symmetric encryption keys, when at rest, must be protected with security measures at least as stringent as the measures used for distribution of that key.
d. Symmetric cryptosystem key lengths must be at least 256 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength.
e. Key length requirements shall be reviewed annually as part of the yearly security review and upgraded as technology allows.
f. AES 256 is the City of Chicago's recommended encryption algorithm.

   PCI: 3.4

9.2.7 Asymmetric Key Encryption

Asymmetric cryptography, also called public key cryptography, uses public-private key pairs. The public key is passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it issued. The private key should only be available to the end user to whom the corresponding

a. All certificates used for SSL/TLS and for code signing must have a minimum key length of 2048 bits. All certificates must be owned and managed by DoIT.

   PCI: 3.4

9.2.8 Proprietary Encryption Algorithms

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the Information Security Office.

9.3 Revision History

Date	Version	Description	Author
01/15/2013	0.5	Initial Draft	ISO
07/26/2013	1.0	Approved & Released	CISO

Information Security and Technology Policy	Number 10.0		Policy Owner
	Operations		Department of Innovation and Technology
	Effective	**07/26/2013**	
	Last Revision	**07/26/2013**	

10. Operations

Information systems must be adequately configured, operated, and maintained in order to ensure their confidentiality, integrity, and availability. Risk assessments assessing the risks associated with confidentiality, integrity, and availability must be conducted on a regular basis to ensure that appropriate mitigating controls are in place to adequately protect the City of Chicago information systems and assets. In addition, monitoring capabilities and technical vulnerability analysis processes must be deployed and managed providing the capability of proactively detecting information risks or incidents related to the confidentiality, integrity, or availability of the City of Chicago information systems and assets.

This policy reviews the following areas:

10.1 Operational Procedures and Responsibilities

The development, testing and updating of software must be properly managed to ensure availability, confidentiality and integrity computer systems.

10.1.1 Documented Operating Procedures

All operating procedures must be documented for system and processes in the technical environment.

a. Documented operating procedures must be established and available to employees who require access for the following processes:

- Change, Patch, Incident and Problem Management
- User administration
- Backup
- Equipment maintenance
- Data Center Operations

HIPAA: 164.316(b)(1)(i), ISO: 10.1.1, PCI: 12.2

b. All System Owners must ensure that all system scheduling jobs and dependencies are documented. This documentation must include job start times, latest job completion times, delay procedures and handling procedures in case of failure or error.

HIPAA: 164.316(b)(1)(i), ISO: 10.1.1

c. Technical Operations and Enterprise Network Architecture must ensure that all system restart and shutdown procedures are documented. In case of system failures, restart and shutdown procedures, system validation or verification procedures and emergency contact information must be available for operations personnel.

HIPAA: 164.316(b)(1)(i), ISO: 10.1.1

d. All System Owners must maintain contact information for relevant external parties responsible for information systems.

HIPAA: 164.308(b)(4), ISO: 10.1.1

e. Changes to the formal operating procedures of the technical infrastructure must be approved by appropriate City of Chicago technical management.

HIPAA: 164.316(b)(1)(iii), ISO: 10.1.1

10.1.2 Change

All changes to computer assets must follow appropriate and approved change procedures. Change Control procedures are designed to reduce the risk of changes in an IT environment by requiring proper documentation of the change, sign-offs, testing and back out plans.

a. All System Owners must confirm that change controls around information processing systems, software and procedures ensure that:

- Significant changes and impact are identified and documented
- Change plans are established and tested
- Potential impacts of changes are identified and assessed
- Formal approval for changes is obtained (management sign-off by appropriate parties)
- Change details are communicated to all relevant individuals
- Fallback procedures are established with specific instructions for aborting and recovering from unsuccessful changes
- Documented back out procedures

ISO: 10.1.2

b. All System Owners must ensure that change requests are documented via an approved change request method. The change request form must contain the following information:

- Minimum requirements
- The person making the change
- Impact to the customer
- Time and date of change
- Priority
- The commands executed (if applicable)
- Business justification for the change
- Nature of defect (if applicable)

c. Additionally, the following must be determined and documented by appropriate technical personnel

- Estimated resource requirements necessary to complete the change
- Testing required
- Back-out procedures
- Systems impacted
- User contact information

HIPAA: 164.312(c)(1), ISO: 10.1.2, PCI: 6.4.1, 6.4.3, 6.4.4

d. All System Owners must ensure that the roles and responsibilities for individuals and involved in the change process are clearly defined. When defining various roles, properly segregate incompatible responsibilities.

   ISO: 10.1.2

e. All changes must be approved by appropriate City of Chicago or the system owner. The requester's manager must approve the business justification of the request, while the technical area manager must determine if the request is technically feasible. Information Owners must approve the request if it involves incorporating data from a different application or has potential impact to any environment containing private data.

   ISO: 10.1.2, PCI: 6.4.2

f. All System Owners must ensure that an audit trail of all changes is maintained via an approved change method.

   HIPAA: 164.308(a)(1), ISO: 10.1.2

g. Technical Operations and Enterprise Network Architecture must ensure that system and application software is backed-up before system upgrades or maintenance.

   ISO: 10.1.2

h. Security-related changes (e.g., file permissions, identification and authentication, audit and discretionary access control) impacting environments containing private data must be approved by Information Security Office. Permanent fixes must be subjected to the normal change standards.

   ISO: 10.1.2

i. Only those persons authorized by Information Owners or System Owners are allowed to make emergency changes to City of Chicago networks. These changes must be clearly and completely documented and approved within 24 hours of resolution of the problem at which time a permanent course of action must be determined.

   HIPAA: 164.312(a)(1)(ii), ISO: 10.1.2

j. All System Owners must ensure that all emergency requests are documented using the standard change request forms. An automated audit trail of the emergency activity must also be generated which logs all activity performed on the system including the user making the change, time and date, the commands executed, the program and data files affected, etc. The person making the emergency change must also provide a written description of the operations performed during the emergency to their manager for approval.

   HIPAA: 164.312(c)(1), ISO: 10.1.2

k. Applications Development must ensure that production source code is not changed in response to an emergency change. A controlled temporary version or a patch must be created and executed until the production source can be changed following the change standards and the executable updated.

   ISO: 10.1.2

10.1.3 Patch

Appropriate patch procedures must be in place for all computer assets.

a. All computer assets will have all Operating System (OS) and relevant Application security patches applied within the required timeframes as defined per the Patch Deployment Matrix below.

PCI: 6.1

b. Assets containing PCI, PII or ePHI data will have an Asset Criticality rating of High and all other assets shall be rated no lower than the highest rated data that either passes through or is contained within the asset as per the Asset policy.

PCI: 6.1

c. When available, the Common Vulnerability Scoring System (CVSS) will be used to determine patch ratings. Patches without a CVSS score will be aligned to the Patch Deployment Matrix by the Patch Team and approved by the Information Security Office.

PCI: 6.2

		ASSET CRITICALITY RATING		
		HIGH	MODERATE	LOW
CVSS & Microsoft Scores	8.0-10.0 ("Critical")	< 14 d	< 21 d	< 21 d
	5.0-7.9 ("Important")	< 21 d	< 28 d	< 28 d
	2.0-4.9 ("Moderate")	< 28 d	< 35 d	< 45 d
	0.0-1.9 ("Informative")	not required	not required	not required

Patch Deployment Matrix

d. Deployment of all patches must follow established Change processes and be tested before deployment. This includes but is not limited to the following tests when applicable;

- That functionality has not been impacted in an unacceptable manner
- That security issues are not introduced as part of the implementation
- Input validation & proper error handling
- Secure cryptographic storage
- Secure communications and proper roll based access controls (RBAC)

PCI: 6.4

e. All computer assets will be monitored for patch compliance. Assets rated "High" will be evaluated at least monthly for patch compliance. Violations of compliance will be reported to the Information Security Office, Technical Operations and Enterprise Network Architecture and System Owner.

PCI: 6.6

10.1.4 Security of System Documentation

Controls must be in place to protect system documentation from unauthorized access.

a. Non-Public system documentation must be controlled and protected against unauthorized access. Access to the documentation must be kept to a minimum and only granted to individuals that require access to perform their job functions. System documentation stored on or accessed using public networks must be appropriately protected. The following types of system documentation must be stored securely:

   - Data structures
   - Authorization processes
   - System and application documentation
   - Operations and production logs

   HIPAA: 164.316(b)(1)(ii), ISO:10.7.4

10.1.5 Management of Removable Computer Media

All removable media containing private data must be stored securely and documented appropriately during transit.

a. Technical Operations and Enterprise Network Architecture must ensure that an authorization list for physical access to magnetic tape, disk and documentation libraries is maintained. Only employees requiring access to perform their job functions may be granted physical access to the media. The authorization list must be reviewed periodically for appropriateness.

   HIPAA: 164.310(a)(1)(iii), ISO: 10.7.3

b. Information Owners must ensure that all media containing confidential data including paper and digital media are stored in a physically secured and environmentally controlled area. Any computer media leaving City of Chicago facilities must be authorized by the Information Owner. Media containing confidential data should be accounted for with an audit log. Media content that is no longer required must be erased prior to removal from the site.

   HIPAA: 164.310(d)(1)(iii), ISO: 10.7.1, PCI: 9.6

c. Technical Operations and Enterprise Network Architecture must ensure strict control over media containing confidential data. Specifically, media inventory logs of all confidential data must be maintained and an inventory should be taken on a yearly basis.

   PCI: 9.9.1

d. Removable media containing City of Chicago information (e.g., CD's, USB sticks, floppy disk, tapes, removable hard drives, DVD's and printed media) must be registered with and approved by the Information Owner.

   HIPAA: 164.310(d)(1)(iii), ISO: 10.7.1

10.2 Risk Assessment & Risk Acceptance

Risk assessments must be performed periodically across all City of Chicago information systems environment to determine, address, and mitigate security threats.

Risk Assessment must be performed upon initial acquisition on an information system in the event that the system is owned/operated by the City, or prior to initial establishment of service agreements if the information system is owned by a third party on behalf of the City.

10.2.1 Assessing Security Risks

Management must employ risk assessment and analysis techniques to ensure adequate controls are in place for all areas of responsibility.

a. Risk assessments, under the direction or coordination of Internal Audit or Information Security Office, must be performed annually.

   HIPAA: 164.308(a)(8), ISO: 4.1, PCI: 12.1.2, 11.3

b. Internal Audit or Information Security Office is responsible for defining the risk assessment process. The risk assessment process must allow for the systematic identification, prioritization and of information security risks.

   HIPAA: 164.308(a)(1)(B), ISO: 4.1

10.3 System Planning and Acceptance

All information systems must be monitored to identify areas where additional capacity is necessary to continue to support the business. Any additional systems necessary must follow an approved change process prior to deployment.

10.3.1 System Acceptance

Technical Operations and Enterprise Network Architecture is responsible to ensure that acceptance criteria for new systems, upgraded systems and new versions are clearly defined, agreed upon, documented and tested.

a. Acceptance criteria for new systems, upgraded systems and new versions must be clearly defined, agreed upon, documented and tested. The following must be included in the acceptance criteria:

- Security controls agreed upon
- Determination of impact to the overall security and technical architecture
- Computer performance and capacity requirements
- Business continuity
- Testing of operating procedures
- Training requirements for operational and user support

ISO: 10.3.2

10.4 Electronic Commerce Services

All electronic commerce (e-commerce) initiatives must be approved to ensure that customer information collected is properly secured and done so in a "least information necessary" manner.

10.4.1 Collection of Information and Privacy

City of Chicago must protect customer information and privacy by using appropriate levels of security for the type of information collected and maintained.

a. All System Owners must ensure that the City of Chicago adopts information practices that treat customers' personal information with care. All City of Chicago e-commerce sites must post and adhere to a privacy policy based on fair information principles, adopt appropriate measures to provide adequate security, and respect customers' preferences regarding unsolicited e-mail.

   ISO: 10.9.1

b. All System Owners must ensure that the e-commerce privacy policy is easy to find and understand. It must be open, transparent, and meet generally accepted fair information principles. The privacy policy must include details about the following:

   - What personal information is collected, used and disclosed to other parties
   - The choices the customer has with regard to the collection, use and disclosure of that information
   - The access the customer has to that information
   - The security measures taken to protect the information
   - Enforcement mechanisms that are in place to remedy any violations of the policy

   ISO: 10.9.1

c. All System Owners must ensure that the City of Chicago accurately describes proper business practices with regard to the use of unsolicited e-mail to customers. The City of Chicago must post and adhere to a "Do Not Email" policy. This policy must allow customers who do not wish to be contacted online to opt out of future communications from the City of Chicago.

   ISO: 10.9.1

10.4.2 Security of Transactions

All online transactions must meet certain requirements in addition to local laws and regulations.

a. Information Security Office must ensure that the level of protection associated with online transactions corresponds to the risk associated with the transaction and comply with all applicable laws and regulations. The following requirements must be met for all online transactions:

   - Controls are established to ensure the confidentiality and privacy of the transaction and parties involved
   - Communication paths are encrypted for all parties involved whenever private information is transferred over open, public networks
   - Transaction information is stored outside publicly accessible environments

   ISO: 10.9.2, PCI: 4.1

10.5 Media Disposal

Except as otherwise provided by law or court order, electronic information maintained in a department's office will be destroyed when the retention period expires, in compliance with the City's implementation of the State of Illinois Local Records Act. Procedures for handling and disposing of media in any form (including paper, removable media, and system hardware) must be properly documented and followed by all employees.

10.5.1 Disposal of Hardware and Removable Media

All hardware and removable media containing City of Chicago member information must be disposed of securely.

a. Technical Operations and Enterprise Network Architecture must ensure that electronic information storage devices (e.g., hard drives, tapes, USB sticks, removable hard disks, floppy disks, CD's and DVD's) are disposed of in a manner commensurate with its information classification. All electronic storage devices must be electronically wiped by a process such that data on the storage device cannot be recovered by individuals and/or technology.

   HIPAA: 164.310(d)(1)(i), ISO: 10.7.2, PCI: 9.10.2

b. Technical Operations and Enterprise Network Architecture must ensure external firms responsible for disposing of any type of City of Chicago information are held to the standards of the third party contracts. This includes confidentiality agreements and adequate security controls.

   HIPAA: 164.310(d)(1)(i), ISO: 10.7.2

c. Information Owners must ensure that media containing sensitive or confidential data is destroyed when it is no longer needed for business or legal reasons.

   PCI: 9.10

d. Computer storage devices, including hardware and removable devices must be turned over to Technical Operations and Enterprise Network Architecture for disposal. All electronic storage devices must be electronically wiped or destroyed by a process such that the data on the storage device cannot be retrieved.

   PCI: 9.10

e. All Information Owners must ensure that a log of all sensitive or confidential items disposed must be kept and maintained.

   ISO: 10.7.2, PCI: 9.10.2

10.5.2 Disposal of Paper

All paper containing City of Chicago sensitive or confidential information must be shredded and disposed of securely.

a. All employees must use proper destruction methods when disposing of information. Paper copies of sensitive or confidential information must be shredded or incinerated. Users of the information are responsible for disposing of it in secure disposal containers or using another proper destruction method.

   ISO: 10.7.2, PCI: 9.10.1

10.6 Monitoring

Logging must be enabled for all information systems. The logs must be time-synchronized and monitor system use for all accounts including users, applications, administrators, root, etc.

Users should have no expectation of privacy in their use of Internet services provided by the City. The City reserves the right to monitor for unauthorized activity the information sent, received, processed or stored on City-provided network and computer resources, without the consent of the creator(s) or recipient(s). This includes use of the Internet as well as the City's e-mail and instant messaging systems.

10.6.1 Monitoring System Use

All City of Chicago systems must follow monitoring and logging requirements based on the risk associated with the system.

a. Technical Operations and Enterprise Network Architecture must ensure that monitoring for unauthorized system access capture the following details:

- Failed or rejected actions performed by users
- Failed or rejected attempts to access data or resources
- Anti-malware software alerts
- File integrity monitoring system alerts
- Intrusion detection and prevention system alerts

HIPAA: 164.312(b), ISO: 10.10.2, PCI: 12.9.5

b. Technical Operations and Enterprise Network Architecture must ensure that monitoring for system alerts and failures capture the following details:

- Alerts or messages from consoles
- Exceptions in system logs
- Alarms generated by network devices or access control systems
- Accessing of audit log information

HIPAA: 164.312(b), ISO: 10.10.2, PCI: 10.2.3

c. Technical Operations and Enterprise Network Architecture must use automated logging tools to monitor events, specifically:

- All individual accesses to confidential data
- All actions taken by any individual with root or administrative privileges
- Access to all audit trails
- Invalid logical access attempts
- Use of identification and authentication mechanisms
- Initialization of the audit logs
- Creation and deletion of system-level objects

PCI: 10.2

d. Information Security Office must ensure that intrusion detection systems and/or intrusion prevention systems be used to monitor all traffic in the confidential data environment and to alert security personnel to suspected compromises. These systems must be subject to the patch and update policies.

PCI: 11.4

10.6.2 Audit Logging

All audit logs must be maintained as determined by business requirements.

a. Technical Operations and Enterprise Network Architecture must ensure that procedures for managing audit-trail and system log information are established.

   HIPAA: 164.312(b), ISO: 10.1.1, PCI 12.5.5

b. Technical Operations and Enterprise Network Architecture must ensure that operations logs are reviewed daily either through manual means or a log parsing tool for consistency and proper documentation. These reviews must include systems performing security-related functions, including intrusion detection/prevention systems and identity systems. All identified exceptions identified must be immediately raised to Information Security Office. Operations logs must be archived and available for independent verification.

   HIPAA: 164.308(a)(1)(D), ISO: 10.10.4, PCI: 10.2.2, 10.6

c. Technical Operations and Enterprise Network Architecture must ensure that intrusion detection systems or intrusion prevention systems are deployed to monitor all traffic within the confidential data environment. Such systems must be regularly updated.

   PCI: 11.4

d. Technical Operations and Enterprise Network Architecture must ensure that all audit trail log files for systems within the confidential data environment are stored for a minimum of 1 year, and that 3 months of data is readily available.

   ISO: 10.10.1, PCI: 10.7

e. Technical Operations and Enterprise Network Architecture must ensure that where audit trail events are recorded, system entries include the following information:

   - User identification
   - Type of event
   - Date and time
   - Success or failure indication
   - Origin of event
   - Identity or name of affected data, system component, or resource

   PCI: 10.3

f. All System Owners must ensure that open errors or issues remain open until they are satisfactorily resolved. Resolved events and errors must be reviewed to determine if they have been properly authorized and to determine if security controls have been compromised.

   HIPAA: 164.308(a)(1)(B), ISO: 10.10.5

g. All System Owners should log all reports of errors or problems with information processing or communication systems. The log must include the following information, at a minimum:

   - Name of person reporting event
   - Date/time of event
   - Description of error/problem
   - Name of party responsible for problem resolution

- Description of initial operations response
- Name of operations person entering event report
- Description of problem resolution
- Date/time of resolution

HIPAA: 164.308(a)(1)(D), ISO: 10.10.5

10.6.3 Protection of Log Information

All log files must be protected by security controls to prevent unauthorized manipulation.

a. Technical Operations and Enterprise Network Architecture must ensure that security controls are implemented to protect against unauthorized log alteration or deletion.

HIPAA: 164.312(a)(1), ISO: 10.10.3, PCI: 10.5.2

b. Technical Operations and Enterprise Network Architecture must ensure that the viewing of audit trails is limited to those with a specific job-related need to view those files.

HIPAA: 164.312(a)(1), ISO: 10.10.3, PCI: 10.5.1

c. Technical Operations and Enterprise Network Architecture must ensure that all audit trail log files, including those from externally facing systems hosted in the DMZ are promptly backed up to a centralized log server located within the internal City of Chicago network to prevent manipulation.

HIPAA: 164.312(a)(1), ISO: 10.10.3, PCI: 10.5.3, 10.5.4

d. Technical Operations and Enterprise Network Architecture must employ capabilities to detect unauthorized access or changes to log data to ensure that data cannot be changed without generating alerts. Monitoring must take place on servers that perform security functions like intrusion detection system and authentication, authorization, and accounting protocol servers.

HIPAA: 164.312(a)(1), ISO: 10.10.3, PCI: 10.5.5

10.6.4 Clock Synchronization

All information processing devices must synchronize their time with an agreed time source. All server clocks must be synchronized in a manner approved by the Department of Innovation and Technology in order to provide for timely administration and accurate auditing of systems

a. Technical Operations and Enterprise Network Architecture must ensure that information processing devices be set to an agreed standard and synchronized with an agreed, accurate time source. A procedure must be established that verifies the accuracy of the system time and provide corrections as needed.

HIPAA: 164.312(c)(1), ISO: 10.10.6, PCI: 10.4

10.7 Malicious Program Detection

Malicious program detection software must be installed and properly configured and updated on information systems deemed to be of greater risk for viruses.

10.7.1 Detection Software and Product Configuration

All information systems within the technical environment must utilize anti-malware solution.

a. Technical Operations and Enterprise Network Architecture must ensure that all systems utilize approved anti-malware software.

   PCI: 5.1

b. Technical Operations and Enterprise Network Architecture must define and implement an anti-malware product configuration capable of detecting and removing known malicious software.

   PCI: 5.1.1

c. Technical Operations and Enterprise Network Architecture must ensure that all anti-malware mechanisms are current, actively running, and capable of generating audit logs.

   PCI: 5.2

d. Technical Operations and Enterprise Network Architecture must ensure that anti-malware software programs are configured in a central location and deployed to end user computers from that location.

e. Information Security Office must ensure that users do not have access to modify the anti-malware product configuration

10.7.2 Product and Definition Updates

All anti-malware software updates must be implemented within appropriate timeframes. It is the City's policy to conduct virus scanning of its technology resources to protect them from the threat of malicious code. The City will intercept and/or quarantine any networking and computer resource that poses a virus threat to its information assets.

a. Information Security Office must ensure that anti-malware products are updated in a timely manner after the vendor has released a new definition file.

   PCI: 5.2

10.8 Technical Vulnerability

Roles and responsibilities for managing and addressing technical vulnerabilities must be assigned throughout the organization.

10.8.1 Roles and Responsibilities

Management must ensure proper documentation, testing and deployment of patch and vulnerability information.

a. Information Security Office must establish processes to identify, evaluate, prioritize and resolve security vulnerabilities.

   PCI: 6.2

b. Information Security Office is responsible for identifying and distributing information on incidents, threats, and vulnerabilities to internal parties related to software. It is the responsibility of Information Security Office to maintain distribution lists of contacts for each technical platform to facilitate resolution of identified issues. All operational groups should participate in maintenance of these distribution lists.

   HIPAA: 164.308(a)(5)(A), ISO: 12.6.1

c. Information Security Office is responsible for maintaining the documentation of the analysis produced by the technical vulnerability processes. Information Security Office is also responsible for escalating or de-escalating vulnerability classifications and communicating changes, as appropriate.

   ISO: 12.6.1

d. Technical Operations and Enterprise Network Architecture must ensure that the technical vulnerability process is reviewed on an annual basis.

   HIPAA: 164.308(a)(8), ISO: 12.6.1

e. Information Security Office and Technical Operations and Enterprise Network Architecture are responsible for developing processes for asset, classification, and prioritization of systems in support of the technical vulnerability processes. This includes a detailed asset inventory with appropriate documentation to facilitate prioritization and implementation of vulnerability remediation activities.

   HIPAA: 164.308(a)(7)(E), ISO: 12.6.1

f. Information Security Office must establish processes to identify, evaluate, prioritize and resolve security vulnerabilities.

   ISO: 6.2

g. Information Security Office is responsible for identifying and distributing information on incidents, threats, and vulnerabilities to internal parties related to software. It is the responsibility of Information Security Office to maintain distribution lists of contacts for each technical platform to facilitate resolution of identified issues. All operational groups should participate in maintenance of these distribution lists.

   HIPAA: 164.308(a)(5)(A), ISO: 12.6.1

h. Information Security Office is responsible for maintaining the documentation of the analysis produced by the technical vulnerability processes. Information Security Office is also responsible for escalating or de-escalating vulnerability classifications and communicating changes, as appropriate.

   ISO: 12.6.1

i. Information Systems must ensure that the technical vulnerability process is reviewed on an annual basis.

   HIPAA: 164.308(a)(8), ISO: 12.6.1

j. Information Security Office and Information Systems are responsible for developing processes for asset management, classification, and prioritization of systems in support of the technical vulnerability processes. This includes a detailed asset inventory with appropriate documentation to facilitate prioritization and implementation of vulnerability remediation activities.

10.8.2 Addressing Technical Vulnerabilities

All vulnerabilities must be properly classified and remediated according to the City of Chicago change process.

a. Information Security Office must ensure that publicly accessible systems are tested for vulnerabilities prior to being made available.

   HIPAA: 164.308(a)(1)(B), ISO: 10.9.3

b. Technical Operations and Enterprise Network Architecture must ensure that technical vulnerabilities, including vendor supplied patches, are classified. The CVSS system is to be used to classify technical vulnerabilities and their associated patches.

   HIPAA: 164.308(a)(1)(B), ISO:12.6.1, PCI 6.1

c. Technical Operations and Enterprise Network Architecture must ensure that vulnerability remediation efforts, including patch implementations, are coordinated and processed according to the change standards. This includes meeting all testing and documentation requirements.

   HIPAA: 164.308(a)(1)(B), ISO: 12.6.1

d. Information Security Office must perform internal and external network vulnerability scans on a quarterly basis and after any significant change in the network.

   PCI: 11.2

e. Information Security Office must perform internal and external penetration testing on an annual basis and after any significant infrastructure or application upgrade or modification. These penetration tests must include network-layer penetration analysis, and application-layer penetration analysis (including associated databases).

   PCI: 11.3

f. Information Security Office must ensure that file integrity monitoring is employed within the confidential data environment to alert personnel to unauthorized modification of critical system files, configuration files or content files. Software solutions selected shall be configured to execute critical file comparisons at least weekly.

   PCI: 11.5

10.9 Backup

Information backup processes must be documented and implemented.

10.9.1 Information Backup

Information backup schedules and procedures must be employed based on information criticality classification.

a. If backups are performed at the server or host level, the backup schedule of the most critical application on the server must determine the backup frequency of the server.

   HIPAA: 164.308(a)(7)(A), ISO: 10.5.1

b. Information Owners or an assigned delegated Information Custodian must develop off-site backup rotation and retention schedules in conjunction with the Legal Department for each application that they support. This schedule must reflect the criticality of the information being backed up.

   HIPAA: 164.308(a)(7)(A), ISO: 10.5.1

c. Technical Operations and Enterprise Network Architecture must perform an annual review of the off-site tape backup location to verify that the backup media is stored securely.

   PCI: 9.5

d. Each System Owner must have documented backup and recovery procedures.

   HIPAA: 164.308(a)(7)(A), ISO: 10.5.1

e. Users must backup critical files by transferring or duplicating files onto the local area network, which is backed up on a scheduled basis. This includes all user data created on City of Chicago PC's (e.g., files created in Microsoft Office).

   HIPAA: 164.308(a)(7)(A), ISO: 10.5.1

f. Technical Operations and Enterprise Network Architecture must ensure that backups of all critical applications are sent off-site to a remote location on a schedule designed to meet the specific application recoverability requirements. The remote location must have appropriate security controls in place, including physical and environmental protection.

   HIPAA: 164.308(a)(7)(A), ISO: 10.5.1, PCI: 9.5

g. Information stored on backups classified as Private or higher must be encrypted as defined in 9.2, Encryption.

   HIPAA: 164.308(a)(7)(C), ISO: 10.5.1

h. The City will perform regular backups of User files stored on the City's file servers and storage media that are centrally managed by the Department of Innovation and Technology. This process will be coordinated in conjunction with the City's User departments based on their individual business needs.

i. The City will not back up multimedia files in formats including, but not limited to, .mp3, m4a, m4p .avi and .mov

10.10 Revision History

Date	Version	Description	Author
01/15/2013	0.5	Initial Draft	ISO
07/26/2013	1.0	Approved & Released	CISO

	Number 11.0		Policy Owner
Information Security and Technology Policy	**Information Security and Technology Incident Management**		Department of Innovation and Technology
	Effective	**07/26/2013**	
	Last Revision	**07/26/2013**	

11. Information Security Incident Management

In the event of a specific incident affecting information systems, the City of Chicago (City) must have pre-planned methods for responding to various threats, including incidents related to data confidentiality, integrity, and application availability. In addition, reporting mechanisms must be in place to ensure that proper City personnel are informed of all incidents.

Responsibility for incident handling operations must be assigned to an Incident Management Team, whose trained members will execute the incident response plan.

This policy reviews the following areas:

11.1 Management of Information Security Incidents

An incident management process must be properly documented and include team responsibilities and data collection procedures.

11.1.1 Incident Definition

Incidents must be classified based on the risk posed to the City.

a. **Priority 1 (P1):** An event that is or could become a serious and immediate threat to the confidentiality, integrity or availability of at least one critical computer assets or data or more than 10 non-critical computer assets. Threatened devices may include routers, networks, servers, firewalls, network management hosts, attached LANs, or user hosts.

   ISO: 13.2.1

b. **Priority 2 (P2)**: An event that is, or could become, a future threat to the confidentiality, integrity or availability of a single, non-critical computer asset or data.

   ISO: 13.2.1

c. **Priority 3 (P3)**: An event that is, or could become, a minor threat, or which has been determined to be a non-threat resulting from either authorized or unauthorized network activity.

   ISO: 13.2.1

d. **Informational**: Violations of City of Chicago Security Policy that do not involve an active risk to company resources or systems.

   ISO: 13.2.1

11.1.2 Incident Management Team, Roles & Responsibilities

The incident management team must be composed of members responsible for each activity associated with incident management.

a. An Incident Response Team Leader will be identified for every Incident Response Team. The Leader will be responsible for:

   - Coordinating incident response efforts
   - Acting as a point of contact for team
   - Acting as liaison between incident response team and management, legal and law enforcement
   - Delegating and organizing efforts

   ISO: 13.2.1

b. The Management Representative on the Incident Response Team is responsible for the following:

   - Providing management support and guidance in response efforts
   - Directing or authorizing funding for incident response and recovery efforts
   - Determining appropriate time to contact law enforcement or continue the investigation
   - Communicating incident information to other management

   ISO: 13.2.1

c. An Incident Librarian must be a member of any Incident Response Team. The librarian is responsible for recording, documenting and organizing information from the incident including all intrusion and response activity. The librarian is also responsible for:

- Communicating documentation methods to all system administrators for consistency
- Documenting time spent on intrusion along with any monetary losses (e.g., loss due to man-hours)
- Coordinating collection of system logs, records, etc. with person responsible for securing evidence
- Maintaining summary reports of all incidents for historical documentation

ISO: 13.2.1

d. Technical Incident Response Team Members are responsible for performing technical analysis, support, and other technical tasks related to security incidents. This may include, but is not limited to, the following:

- Log analysis
- Collection of technical information
- Technical incident interpretation
- Gathering technical evidence
- Coordinating technical efforts with system administrators
- Coordinating recovery efforts

ISO: 13.2.1

e. A representative from the Legal Department must be identified to assist in computer related incidents. This legal analyst must be familiar with local, state and federal computer crime statutes, electronic evidence standards, investigative procedures and civil and criminal litigation processes.

ISO: 13.2.1

f. Key business unit leaders or analysts must be identified to assist with Red level (i.e., emergency) situations. If a threat, or potential threat, has been identified to specific systems, data or processes, a business analyst must be consulted to assist in quantifying the risk in business terms.

ISO: 13.2.1

g. Specific personnel must be designated to be available on a 24/7 basis to respond to alerts.

PCI: 12.9.3

h. All personnel with responsibilities related to incident management and breach response must undergo training on a yearly basis specific to responding to potential information security incidents.

PCI: 12.9.4

11.1.3 Incident Management Procedures

Incident management processes and procedures including escalation, evidence collection, storage of data, and incident closure must be adequately documented and defined.

a. Information Security Office is responsible for establishing, documenting, maintaining, and distributing security incident response and escalation procedures to ensure timely and effective resolution of all perceived or real threats that could impact City of Chicago operations.

   PCI: 12.5.3

b. The City of Chicago incident response procedures must, at a minimum, include the following:

   - Roles, responsibilities, and communication and contact strategies in the event of a compromise, including notification of the payment brands
   - Specific incident response procedures
   - Business recovery and continuity procedures
   - Data back-up processes
   - Analysis of legal requirements for reporting compromises
   - Coverage and responses of all critical system components
   - Reference or inclusion of incident response procedures from the payment brands

   PCI: 12.9, 12.9.1

c. The incident response plan must be tested at least annually.

   PCI: 12.9.2

d. Once incidents have been reported to the appropriate parties, the incident must be escalated for investigation. Security incidents will be investigated by Information Security Office to determine the severity of the incident. Investigative methods and procedures will be used based upon the alert level. Management must take appropriate corrective actions to follow up on security violations.

   HIPAA: 164.308(a)(6), ISO: 13.2.1

e. Information Security Office is responsible for following up on the reported issues in a swift and confidential manner. Incident handling procedures must be established to handle different types of security incidents including

   - System failures or loss of service
   - Malicious code and viruses
   - Denial of service
   - Breach of data confidentiality
   - Integrity rules and misuse of corporate information systems resources

f. Information Systems Department personnel (e.g., system administrators, database administrators, network administrators, and/or end-users) that are included in the investigation of an incident for any reason must follow the procedures as directed by Information Security Office. These individuals must not divulge any information regarding the incident to anyone outside the immediate investigation team, including internal employees and anyone external to City of Chicago.

   HIPAA: 164.308(a)(6), ISO: 13.2.1

11.1.4 Collection of Evidence

Paper and electronic documents being used as evidence must be secured and evidential procedures must be followed while collecting the evidence.

a. Information Security Office and the Legal Department are responsible for ensuring that all paper documents collected as evidence in the investigation of a security incident are secured, and the process of collecting the evidence is documented with a chain of custody.

   HIPAA: 164.308(a)(6), ISO: 13.2.3

b. For external incidents or threats, action must be taken to ensure evidential integrity is maintained and the appropriate legal action can be taken. Designated management personnel, appointed by the Legal Department are the only representatives of City of Chicago that will complete criminal referral procedures to law enforcement or regulatory authorities.

   HIPAA: 164.308(a)(6), ISO: 13.2.3

11.1.5 Learning from Information Security Incidents

Security policy violations and security incidents must be documented and reviewed.

a. Information Security Office must document all reports of security incidents. Information Security Office must also include a process to review all incidents, document "lessons learned", and coordinate training and learning sessions for applicable areas within City of Chicago.

   HIPAA: 164.308(a)(6), ISO: 13.2.2, PCI: 12.9.6

b. Information Security Office must maintain a database or records containing information about violations of the Information Security and Technology Policy and will report on these violations. All records of policy violations must be accessible to only authorized individuals.

   HIPAA: 164.316(b)(1), ISO: 13.2.2

11.2 Incident Reporting

All information technology and security incidents, including suspicious events, shall be reported immediately. A documented process for reporting and learning from security incidents must be in place.

Reporting Information Security Events and Weaknesses

a. Violations of the City's Information Technology and Security Policy or any or all parts or provisions of this Policy must be reported to Department Management or to the City's Information Security Office.

b. Users must ensure that a Service Desk or an Information Security Office representative is notified immediately whenever a security incident occurs. Examples of security incidents include a virus outbreak, defacement of a website, interception of email, blocking of firewall ports, and theft of physical files or documents.

c. All reports of alleged violations of this Policy, or any part or provision hereof, will be investigated by the appropriate authority. During the course of an investigation, access privileges may be suspended.

11.2.2 Reporting Information Security Events

Incident reporting and escalation processes must be employed to ensure security events are properly documented.

a. Information Security Office is responsible for defining an incident reporting and escalation processes within City of Chicago and establishing points of contact for security incident reporting. Reporting procedures must include proper documentation of resolution of security incidents.

   HIPAA: 164.308(a)(6), ISO: 13.1.1

b. Information Security Office is responsible for communicating all incident reporting and escalation processes to employees, contractors and third party users.

   HIPAA: 164.308(a)(6), ISO: 13.1.1

c. Disciplinary action resulting from a violation of the Information Security Policy must be consistent with the severity of the incident, as determined by an investigation. For further information, see the City of Chicago Employee Handbook and Code of Conduct. Disciplinary actions may include, but are not limited to:

   - Loss of access privilege to data processing resources
   - Dismissal of consultants
   - Cancellation of contracts
   - Termination of employment

d. Disciplinary actions must be coordinated through the Human Resources Department.

   HIPAA: 164.308(a)(1)(C), ISO: 13.1.1

e. To report a software malfunction or error, users must contact the Support Desk. The user should note any symptoms, error messages or failures. The Help Desk must notify Information Security Office if the software malfunction is in any way suspect or indicative of a security vulnerability.

   HIPAA: 164.308(a)(5)(C), ISO: 13.1.1

f. The Legal Department must be contacted in the event of an information security event to determine whether or not legal requirements dictate the necessity of reporting the security incident publicly or to an external party.

   HIPAA: 164.308(a)(5)(C), ISO: 13.1.1, PCI: 12.9.1

11.3 Revision History

Date	Version	Description	Author
01/15/2013	0.5	Initial Draft	ISO
07/26/2013	1.0	Approved & Released	CISO

Information Security and Technology Policy	Number 12.0		Policy Owner
	Business Continuity Management		Department of Innovation and Technology
	Effective	**07/26/2013**	
	Last Revision	**07/26/2013**	

12. Business Continuity Management

Business Continuity Management programs and processes must be in place to ensure the mitigation of unacceptable business losses in the event of a crisis. Such processes must include the identification of critical business processes and determination of business process priority, as well as set forth requirements for development of business continuity plans, adequate recovery strategies, potential work-around procedures, and disaster recovery plans. The business continuity and disaster recovery plans must include processes and controls to protect the business, the life and safety of the workforce and customers and to protect the image, reputation, assets, and resources of the organization.

This policy reviews the following policy areas:

12.1 Information Security Aspects of Business Continuity Management

City of Chicago must ensure that a robust business continuity management program is in place that performs regular prioritization of business processes and information systems to determine the implications of a lack of system confidentiality, integrity, or availability. Risk-reducing controls and application redundancy must be implemented for those systems resulting in unacceptable business losses in the event of downtime.

12.1.1 Business Continuity Business Impact Analysis

Management must execute a business impact analysis regularly on an appropriate rolling schedule to drive the determination of business requirements for recoverability.

a. A business continuity plan must be executed on a rolling cycle to identify critical business functions, set forth requirements for recovery, and determine overall function priority. Information Security Office must assist the business units and IT Senior Management to identify critical business functions and subsequently identify key systems supporting those critical functions. The analysis should include identification of threats such as:

   - Natural disasters
   - Fire
   - Loss of critical infrastructure services such as power, communications or water
   - Deliberate or accidental damage to equipment or data
   - System failures
   - Security breaches
   - Deliberate or accidental disclosure of confidential or proprietary information

   And consider potential impacts of system/process outage, including:

   - Customer/Member Impacts
   - Financial Implications
   - Legal & Regulatory Implications
   - Broader Reputational Impacts

   The plan should clearly indicate each critical function's recovery requirements. The plan must clearly define recovery time objectives and minimum acceptable recovery resources for each required supporting system.

   HIPAA: 164.308(a)(7)(E), ISO: 14.1.2

b. The business impact analysis must prioritize business functions based on the business impacts associated with the disruption of the process. Processes must be prioritized into criticality tiers. Tier-1 processes being those that have the least tolerance for outage and highest impact to the organization in the event of incident. Tier-2 processes being potential dependencies of tier-1 processes, and other important (but not critical) processes of the business. Tier 3 and Tier 4 processes represent those processes that may have high business importance, however, may not be required for operations or have a high tolerance for outage.

12.1.2 Business Continuity Planning Framework

Without a properly documented and tested plan, City of Chicago will be unable to ensure that all business units can re-establish normal and complete business operations in a timely manner. As such, management must ensure that each business unit develops a business continuity plan consistent with corporate guidelines and allows for the recovery of business functions before unacceptable losses are incurred (as defined by the Business Impact Analysis).

a. IT Senior Management must partner with business leaders to create a standard framework for all business continuity plans. A consistent format must be published and communicated to plan owners.

   HIPAA: 164.308(a)(7), ISO: 14.1.4

b. IT Senior Management must ensure that each business unit develops a business continuity plan consistent with corporate guidelines.

   HIPAA: 164.308(a)(7)(D), ISO: 14.1.4

c. IT Senior Management must ensure that all business continuity plans have a designated owner. The plan owner is responsible for the maintenance and testing of the plan, developing execution criteria and requirements, and determining activation status.

   HIPAA: 164.308(a)(7)(D), ISO: 14.1.4

d. An appropriate business leader must approve all business continuity plans prior to implementation and rollout. The plan must contain all necessary documentation, have approval by all affected business units, and meet all necessary requirements as determined by management.

   HIPAA: 164.308(a)(7), ISO: 14.1.4

e. IT Senior Management must ensure that all business continuity and incident response plans have a training and education schedule and that requirements are set for all affected personnel.

   HIPAA: 164.308(a)(7), ISO: 14.1.4, PCI: 12.9.4

f. All business continuity and incident response plans have a maintenance schedule. Each plan must be reviewed annually, at a minimum.

   HIPAA: 164.308(a)(7)(D), ISO: 14.1.4, PCI: 12.9.6

12.1.3 Developing and Implementing Continuity Plans

All business continuity plans must employ appropriate recovery strategies to restore or maintain business operations in the required time following any interruption of service or disaster through an appropriate combination of business-process workaround procedures, technical redundancy, and disaster recovery planning. Management must ensure that all business continuity plans are updated and distributed appropriately.

a. IT Senior Management must ensure that all business continuity plans restore or maintain business operations in the required time (as defined by the Business Impact Analysis) following any interruption of service or disaster. Therefore, the following elements must be included in the plan:

   - Failover conditions or requirements necessary to invoke the plan
   - Emergency and operational procedures for all essential business processes
   - Documentation of all personnel, systems, resources or assets necessary for recovery
   - Documentation of all roles, responsibilities, and agreements regarding actions during execution of the plan including internal personnel or any external party agreements
   - Documentation of explicit procedures for restoration of resources (e.g., all major services and systems, manual backup process documentation, logistics and action plans)
   - Documentation of any manual workarounds the business will invoke

- Training and education schedule for all affected or involved personnel
- Testing and updated schedule for the plan
- Recovery and reporting processes

HIPAA: 164.308(a)(7), ISO: 14.1.4

b. IT Senior Management must ensure that all business continuity plans are protected and are considered confidential information. Plans must be stored securely and backups must be stored at off-site locations.

HIPAA: 164.308(a)(7)(C), ISO: 14.1.3

c. IT Senior Management must ensure all copies of the business continuity plans are distributed appropriately when plans are updated.

HIPAA: 164.308(a)(7)(D), ISO: 14.1.1

d. If alternate temporary locations are used for business continuity planning purposes, security controls must be consistent with the primary site and approved by Information Security Office.

HIPAA: 164.310(a)(1)(i), ISO: 14.1.3

12.1.4 Testing, Maintaining and Re-Assessing Business Continuity Plans

All business continuity plans must have a documented testing schedule.

a. IT Senior Management must ensure that all continuity plans have a testing schedule. Business continuity plans considered critical by management will be tested on an annual basis. The process of testing will be determined by management, Internal Audit, and the business function owner. This test may include a full execution of the plan including swap-over of production operations or simulations of the plan to include contingencies and variations.

HIPAA: 164.308(a)(7)(D), ISO: 14.1.5

b. IT Senior Management must ensure that continuity plans for systems supporting tier-1 and tier-2 processes are tested on an annual basis at a minimum. Significant changes to the business should alter the continuity plan and be reviewed and tested. Tests must be documented and the results reported to the information owners and any other committee designated by City of Chicago management.

HIPAA: 164.308(a)(7)(D), ISO: 14.1.5

c. IT Senior Management and/or the owner of the business continuity plan is responsible for coordinating all updates to the plan including documentation and procedural updates. This includes:

- Current location/contact information for all parties relevant to the plan
- All procedures or processes necessary for execution of the plan
- All third party agreements, as applicable
- All asset inventories or requirements for the plan
- All training, awareness and education materials for participants
- Documentation on security and controls requirements

HIPAA: 164.308(a)(7)(D), ISO: 14.1.5

12.2 Revision History

Date	Version	Description	Author
01/15/2013	0.5	Initial Draft	ISO
07/26/2013	1.0	Approved & Released	CISO

Information Security and Technology Policy	Number 13.0		Policy Owner
	Compliance		Department of Innovation and Technology
	Effective	**07/26/2013**	
	Last Revision	**07/26/2013**	

13. Compliance

City of Chicago employees, contractors and associated business processes must fully comply with the Information Security Policy in addition to any other legal or industry-specific regulatory requirements applicable to City of Chicago.

This policy reviews the following policy areas:

13.1 Compliance with Security Policies, Standards and Technical Compliance

Employees and contractors of City of Chicago must ensure compliance with this information security policy and subsequent technical standards.

13.1.1 Compliance with Security Policy

Management must verify their security responsibilities are being executed. All escalation processes must be followed when exceptions to the Information Security Policy are noted.

a. All incidents of non-compliance or exceptions to the Information Security Policy must be reported to the Information Security Office.

   HIPAA: 164.308(a)(6), ISO: 15.2.1

b. All technical areas must regularly review processes and procedures within their area of responsibility to ensure security responsibilities and duties are carried out appropriately. Results of this review and corrective actions must be documented.

   HIPAA: 164.308(a)(8), ISO: 15.2.1

13.1.2 Technical Compliance Verification

Responsibilities to perform audits, attestations, assessments and/or reviews must be assigned to parties to maintain compliance with security practices.

a. Information Security Office and Internal Audit must assign review activities to parties to maintain compliance with City of Chicago security practices. Situations resulting in non-compliance to the practices must be reported to the appropriate function. Review activities should include operational compliance monitoring, individual system assessments, third party testing, internal compliance testing, and procedural reviews.

   HIPAA: 164.308(a)(8), ISO: 15.2.2

b. Information Security Office must ensure that operational systems are checked at regular intervals for their technical compliance. This includes checking compliance of all technologies, both hardware and software, to security implementation standards as detailed in the Information Security and Technology Policies.

   HIPAA: 164.308(a)(8), ISO: 15.2.2

13.1.3 Exception

All exceptions to the Information Security and Technology Policy must be appropriately documented and approved per the Information Security Office Exception Policy.

a. Operational and procedural exceptions to the requirements outlined in this Information Security and Technology Policy may only be granted by City of Chicago Information Security Office. All exception requests must be formally documented and submitted for review by Information Security Officer for review. Documented requests for policy exceptions must include:

   - Reference to the policy objective or requirement for which the exception is sought
   - Explanation of the reason why the policy objective or requirement cannot be achieved with the existing processes or technology solutions
   - The anticipated duration of the exception
   - Details of compensating controls in place or those to be implemented to mitigate and minimize the risk to the organization

   PCI: 12.5

b. Internal Audit should consider the impact of approved exceptions in its annual risk assessment to ensure potential threats and vulnerabilities continue to be identified and remediated to ensure confidential information environment and related business activities are not adversely impacted.

   PCI: 12.1.2, 12.1.3 HIPAA 164.312(c)2

c. Approval for the requested exception(s) shall be issued in writing and be indexed specifically to the process or technology in question for the duration of the exception. It is the responsibility of the Information Security Office to maintain approval records for approved exceptions.

   PCI: 12.5

13.2 Compliance with Legal Requirements

Obligations must be clearly understood relative to each geography and jurisdiction in which City of Chicago does business and appropriate sanctions applied against workforce members who fail to comply with the security policies and procedures in accordance with City Personnel Rules.

13.2.1 Intellectual Property Rights

Intellectual Property that is created for the City by its employees is property of the City unless otherwise agreed upon by means of third party agreements or contracts.

a. No User may transmit to, or disseminate from, the Internet any material that is protected by copyright, patent, trademark, service mark, or trade secret, unless such disclosure is properly authorized and bears the appropriate notations.

13.2.2 Prevention of Misuse of Information Processing Facilities

Users are prohibited from using the City's processing facilities—including data centers, network cabinets or closets, and other facilities housing the City's technology equipment--in any way that violates this Policy, and federal, state, or municipal law, including, but not limited to, the City's Municipal Code and Personnel Rules.

13.2.3 Compliance with Security Policies and Standards

All Users must read and sign the City's Compliance and Acceptable Use Agreement prior to being authorized to access the City's information technology and information assets.

13.2.4 Identification of Applicable Legislation

All applicable material legal regulations must be documented and defined by the City of Chicago Legal Department.

a. All applicable material legal, statutory, contractual, or regulatory requirements must be documented and defined by the City of Chicago Legal Department. The appropriate business unit is responsible for defining and implementing appropriate security controls based on the regulation. It is that business unit's responsibility to ensure compliance to the identified regulations.

   HIPAA: 164.308(a)(2), ISO: 15.1.1

13.2.5 Data Protection and Privacy of Personal Information

A Privacy or Data Protection Officer must be designated by Chief Information Officer or the Legal Department to ensure compliance to all legal regulations regarding personal information.

HIPAA: 164.308(a)(2), ISO: 15.1. 4

a. Information Security Office and the Legal Department are responsible for defining compliance requirements for data protection, privacy, and information security. This includes the gathering, securing and dissemination of personal information via any media, including information processing systems and physical and verbal communications.

   ISO: 15.1.4

13.2.6 Licensing of Software

All software used must be appropriately licensed and in compliance with software copyright agreements.

13.2.7 Record Retention

All documentation must be retained per all legal and regulatory requirements.

a. The Legal Department must ensure that standards for record retention, storage, handling and disposal are developed for any information covered under legal or regulatory statutes. The retention schedule for this type of information must be defined and disseminated. The retention schedule should contain, but is not limited to:
   - Type of information
   - Inventory of sources of this type of information
   - Record retention time periods
   - Any special requirements

b. It is the responsibility of Information Owners to work with the Legal Department to determine proper record retention schedules and procedures and work with Information Security Office to meet any security-related regulatory requirements.

   HIPAA: 164.316(b)(1)(I), ISO: 15.1.3, PCI: 3.1

c. Information Owners must ensure that application and business processes do not retain sensitive cardholder data elements after payment authorization has been completed. This includes full contents of any track from the magnetic stripe of a member's credit card, the card verification/security code (i.e., CVV2) or encrypted pin block.

   PCI: 3.2.1, 3.2.2, 3.2.3

13.3 System Audit Considerations

System audits must be executed by qualified staff and take place based on perceived regulatory and business risk.

13.3.1 System Audit Controls

Information Security Office must ensure that all system audit activities are properly planned, documented, logged, and monitored for quality by designated individuals.

a. All audit activities must be performed by individuals independent from the activities being audited.

   HIPAA: 164.308(a)(1)(D), ISO: 15.3.1

b. All audit activities must be logged and monitored by authorized individuals as designated by Information Security Office and/or Internal Audit. Persons performing audit activities must provide documentation of tasks performed, audit procedures, findings and recommendations.

   HIPAA: 164.308(a)(1)(D), ISO: 15.3.1

c. All audit activities must undergo proper audit planning and execution, including:

   - Minimizing any disruption or interruption of business operations
   - Agreeing on all audit activities and objectives with
   - Limiting scope of assessment to a controlled environment ensuring no improper access is given to perform the audit tasks
   - Identifying resource and skill needs for any technical tasks

   HIPAA: 164.312(b), ISO: 15.3.1

13.3.2 Protection of System Audit Tools

System audit tools may contain sensitive information. As such, specific measures must be taken to ensure that access to audit tools and audit results are provided only to those with a specific business requirement.

a. Access to all tools (e.g., software, applications, documentation, work papers) required for system audits must be restricted to authorized individuals. Any resulting compliance information must be restricted to authorized individuals.

   HIPAA: 164.312(b), ISO: 15.3.2

13.4 Revision History

Date	Version	Description	Author
01/15/2013	0.5	Initial Draft	ISO
07/26/2013	1.0	Approved & Released	CISO

Information Security and Technology Policy	Number 14.0		Policy Owner
	Third Party Security		Department of Innovation and Technology
	Effective	**07/26/2013**	
	Last Revision	**07/26/2013**	

14. Third Party Security

The City of Chicago often utilizes third parties in support of delivering business services. When, as a result, these arrangements extend the City's information technology enterprise or business processes into the third parties' computing environments the third parties must abide by this Policy, as applicable, unless specific additional provisions have been established through contractual agreements.

City of Chicago must ensure that contracted third parties apply equally stringent controls in managing and protecting all City of Chicago confidential data shared with them. As such, adequate contracts and due diligence processes protecting the City of Chicago brand and its members must be in place. In addition, information shared with third parties must be limited to the minimum amount necessary in order to complete the contracted task.

This policy reviews the following policy areas:

14.1 External Parties

Risk identification steps must take place to determine and ensure understanding of the risks associated with specific third parties. Standard contractual language must exist specifically ensuring that third party vendors place the same or more rigorous controls around City of Chicago information assets and systems.

14.1.1 Identification of Risks Related to External Parties

All inbound and outbound connections to external parties should be managed to ensure adequate security controls are in place. Additionally, appropriate risk assessment activities should take place for all inbound and outbound connections to City of Chicago.

a. Where there is a business need for a direct connection between City of Chicago and a third party network, Information Security Office must be involved to determine security implications and control requirements. An adequate control strategy must be agreed upon and defined in a contract with the third party.

   HIPAA: 164.308(b)(4), ISO: 6.2.1

b. Information Security Office must ensure that all inbound connections from external organizations are limited to specific hosts and specific applications on those hosts. If possible, each specific host and application must be physically or logically segmented from production networks. External parties must not be granted unlimited access to City of Chicago computers or networks.

   HIPAA: 164.312(e)(1), ISO: 6.2.1

c. Information Security Office and the HR Department must ensure that all contract personnel sign a Non-Disclosure agreement including a statement indicating that they understand the importance of information security. For third party service providers, a blanket confidentiality agreement must be signed and retained. The Business Owner representative responsible for the contract must ensure that vendors sign Non-Disclosure and/or Confidentiality Agreements.

   ISO: 6.2.1

d. Information Security Office must ensure that all third party personnel who require access to information resources have a manager sponsoring them. Access will not be granted until formal authorization is obtained from the sponsor.

   ISO: 6.2.1

e. Information Security Office must set a minimum requirement that third party service providers adhere to the same access restrictions as internal users. Access to information must be limited according to the principle of least privilege. Access restrictions must include both physical access to the City of Chicago facilities and logical access to its information systems.

f. Information Security Office must ensure that vendors requiring remote access to City of Chicago information systems have access based on the principle of least privilege. Access must be disabled until they are required for use and disabled after they are no longer needed. If a vendor requires access for maintenance purposes, any opened ports must be disabled upon completion of service. Business owners are responsible for providing notification when access is no longer needed.

   HIPAA: 164.308(a)(4), ISO: 6.2.1, PCI: 12.3.9

g. Information Security Office must maintain a program to monitor service providers' PCI DSS compliance status. As a component of this program, a list of current third-party vendors and their specific roles must be maintained.

   PCI: 12.8.4

14.1.2 Addressing Security in Third Party Agreements

All contracts between City of Chicago and vendors or third parties must include specific Information Security provisions and the right to audit.

a. Third parties with whom cardholder data is shared are subject to all applicable PCI-DSS Requirements for third party service providers, which include:

- Identification on a list of City service providers with whom confidential and sensitive data is shared
  PCI 12.8.1
- A written agreement acknowledging responsibility for securing confidential and sensitive data
  PCI 12.8.2
- Complying with any and all due diligence procedures prior to engagement
  PCI 12.8.3
- Complying on an annual basis with PCI DSS and other regulatory requirements
  PCI 12.8.4

b. If a third party is managing any non-public data, maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the private data they possess.

   PCI: 12.8.2

c. To the extent possible, all contracts must include a "Right to Audit" clause ensuring that Management and/or an authorized representative may physically and logically evaluate a third party's control environment at any time.

   ISO: 6.2.3

d. Any vendor or third party working under contract for City of Chicago must immediately notify the manager responsible for the contract if a security incident occurs. A security incident is any event that has the potential to impact the confidentiality, integrity or availability of City of Chicago data or computing resources. Additionally, any employee who is aware of security violations by vendors must report them to Information Security Office and the Legal Department.

   HIPAA: 164.314(a)(1)(i)(C), ISO: 6.2.3

e. All outsourcing contracts must include an agreement on acceptable security controls and a requirement that the outsourcer provide a SAS70 or equivalent document on an annual basis.

   HIPAA: 164.314(a)(1)(i)(A), ISO: 6.2.3

f. Depending on the sensitivity and criticality of the services or data provided, City of Chicago must consider commissioning or requesting an independent review of the service provider's internal control structure.

   ISO: 6.2.3

g. Ownership of software developed by third parties must be defined in the contract agreement.

   ISO: 6.2.3

h. The department responsible for the selection and approval of third party services and a representative from the Legal Department must review all contracted information services agreements. Approval from City of Chicago Compliance Office must also be obtained if the services provided affect the security or integrity of City of Chicago networks or information, such as the sharing of information classified as confidential or above, or network connectivity for third party employees.

   HIPAA: 164.314(a)(1)(i), ISO: 6.2.3

i. Users must not copy, alter, modify, disassemble, or reverse engineer the City's authorized software or other intellectual property in violation of licenses provided to or by the City. Additionally, Users must not download, upload, or share files in violation of U.S. patent, trademark, or copyright laws. Intellectual property that is created for the City by its employees, vendors, consultants and others is property of the City unless otherwise agreed upon by means of third party agreements or contracts.

14.2 Revision History

Date	Version	Description	Author
01/15/2013	0.5	Initial Draft	ISO
07/26/2013	1.0	Approved & Released	CISO