City of Chicago

Information Security Policy

Seal of the City of Chicago

Department of Innovation and Technology
Table of Contents

I. Introduction ........................................................................................................................................... 3
II. Purpose ................................................................................................................................................ 3
III. Scope .................................................................................................................................................. 3
IV. Definitions .......................................................................................................................................... 3
V. Organizing Information Security ........................................................................................................ 4
VI. Asset Management ............................................................................................................................ 4
VII. Human Resources Security ................................................................................................................ 7
VIII. Communications and Operations Management ............................................................................... 8
IX. Access Control ................................................................................................................................... 10
X. Information Security Incident Management ...................................................................................... 12
XI. Compliance ......................................................................................................................................... 13
Appendix A – Common Terms and Definitions ....................................................................................... 14
Appendix B – Change Control ................................................................................................................... 15
I. **Introduction**

A. The City of Chicago (City) intends to manage its information technology and information assets to maximize their efficient, effective, and secure use in support of the City’s business and its constituents.

B. This document, the Information Security Policy (Policy), defines the governing principles for the secure operation and management of the information technology used, administered, and/or maintained by the City and for the protection of the City’s information assets.

C. Violations of the City’s Information Security Policy must be reported to Department Management or the Department of Innovation and Technology’s (DoIT) Chief Information Officer.

II. **Purpose**

A. To define the responsibilities of the City’s officers, employees, agents, departments, commissions, boards, offices, and agencies with respect to appropriate use and protection of the City’s information assets and technology.

B. To ensure that the City’s information assets and technology are secure from unauthorized access, misuse, degradation, or destruction.

III. **Scope**

A. This Information Security Policy applies to the City of Chicago, its departments, commissions, boards, offices, and agencies, and all officers, employees, temporary employees, interns, vendors, consultants, contractors and agents thereof—collectively referred to as “User(s)”. The principles set forth in this Policy are applicable to all information technology and assets, in all formats, used by the City.

B. This Policy does not create any rights, constitute a contract, or contain the terms of any employment contract or other contract between the City of Chicago, any employee or applicant for employment, or any other person. Rather, this Policy details certain purposes, procedures, guidelines, responsibilities, and other matters the City of Chicago deems relevant to its management of information assets. The City reserves the right to amend this Policy or any part or provision of it.

IV. **Definitions**

Please familiarize yourself with the definitions in appendix A as part of your understanding of this Information Security Policy.
V. Organizing Information Security

A. Information Security Co-ordination
The Department of Innovation and Technology is responsible for designing, implementing and maintaining a City-wide information security program--in conjunction with other departments--and for assisting all City departments, agencies, offices, boards, and commissions in implementing and maintaining information management practices at their respective locations.

B. Allocation of information security responsibilities
The City’s Chief Information Officer (CIO) 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.

C. Confidentiality Agreements
Employees, consultants, or contractors who use the City’s information technology are required to read, understand, and agree to the City's Confidentiality and Acceptable Use Agreement regarding their responsibilities and conduct related to the protection of the City’s information assets and technology.

D. Third Parties
The City 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—for example, in cases of Application Service Providers (ASPs)—the third parties must abide by this Policy, as applicable, unless specific additional provisions have been established through contractual agreements.

VI. Asset Management

A. Information Classification
The City’s information, whether in electronic or physical form, can be categorized into three classifications. Due care must be taken to protect the City’s information assets in accordance with the three classifications, as described within this Policy.

1. Confidential – Sensitive personally identifiable information (PII) used for business purposes within the City which, if disclosed through unauthorized means, could adversely affect the City’s personnel, including employees and constituents, and could have legal, statutory, or regulatory repercussions. Examples include: information exempt from disclosure under the Illinois Freedom of Information Act (FOIA), information protected from disclosure under the federal Health Insurance Portability and Accountability Act (HIPAA), other personnel information including Social Security numbers, and personal financial information including
credit card data protected by the Payment Card Industry’s Digital Security Standard (PCI DSS).

2. **Internal** – Information related to the City’s business that if disclosed, accessed, modified or destroyed by unauthorized means, could have limited or significant financial or operational impact on the City. Examples include: strategic plans, vendors’ proprietary information, and responses to Requests for Proposals (RFPs), information protected by intergovernmental non-disclosure agreements or other non-disclosure agreements, and design documents. Other information related to the City’s information technology that is considered Internal includes dial-up modem phone numbers and access point Internet Protocol (IP) addresses.

3. **Public** – Information intended for unrestricted public disclosure in the course of the City’s business. Examples include: press releases, public marketing materials, and employment advertisements.

B. Responsibility for Assets

1. **Ownership of Assets**

   All information stored and processed over the City’s technology systems is the property of the City. 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.

2. **Acceptable and Unacceptable Use of Assets**

   a. To effectively conduct the City’s business and operations, the City makes available to authorized employees and third parties various information technology resources, including e-mail, the City’s Intranet, the Internet, and other communication and productivity tools. Use of these resources is intended for business purposes in accordance with Users’ job functions and responsibilities, with limited personal use permitted only in accordance with the City’s Ethics Ordinance, personnel rules, this policy, and other applicable City policies. 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.

   b. Users must not allow any consultant, visitor, friend, family member, customer, vendor or other unauthorized person to use their network account, e-mail address or other City-provided computer facilities. Users are responsible for the activities performed by and associated with the accounts assigned to them by the City.

   c. No User may use City-provided Internet or Intranet access or the City’s Confidential or Internal information to solicit or conduct any personal commercial activity or for personal gain or profit or non-City approved solicitation.
d. Users must not make statements on behalf of the City or disclose Confidential or Internal City information unless expressly authorized in writing by their Department Management. This includes Internet postings, or bulletin boards, news groups, chat rooms, or instant messaging.

e. Users must protect Confidential or Internal information being transmitted across the Internet or public networks in a manner that ensures its confidentiality and integrity between a sender and a recipient. Confidential information such as Social Security numbers, credit card numbers, and electronic Protected Health Information (ePHI) must be transmitted using encryption software.

f. Internal information such as email lists must not be posted to any external information source, listed in telephone directories, placed on business cards, or otherwise made available to third parties without the prior express written permission of the User’s Department Management.

g. Users must not install software on the City’s network and computer resources without prior express written permission from the Department of Innovation and Technology. Person-to-person (P2P) applications, Voice over IP (VOIP), instant messenger (IM) applications, and remote access applications pose an especially high risk to the City and their unauthorized use is strictly prohibited. City business must not be conducted on any device that allows P2P communication (such as file sharing music applications) without explicit approval from the Department of Innovation and Technology.

h. 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.
i. Users must not access the Internet, the Intranet or e-mail to use, upload, post, mail, display, or otherwise transmit in any manner any content, communication, or information that, among other inappropriate uses:

   i. interferes with official City business;
   ii. is hateful, harassing, threatening, libelous or defamatory, pornographic, profane, or sexually explicit;
   iii. is deemed by the City to offend persons based on race, ethnic heritage, national origin, sex, sexual orientation, age, physical or mental illness or disability, marital status, employment status, housing status, religion, or other characteristics that may be protected by applicable civil rights laws;
   iv. impersonates a person (living or dead), organization, business, or other entity;
   v. enables or constitutes gaming, wagering or gambling of any kind;
   vi. promotes or participates in unauthorized fundraisers;
   vii. promotes or participates in partisan political activities;
   viii. promotes or participates in unauthorized advertising of City projects and any advertising of private projects;
   ix. compromises or degrades the performance, security, or integrity of the City's technology resources and information assets;
   x. contains a virus, logic bomb, or malicious code;
   xi. Constitutes participation in chain letters, unauthorized chat rooms, unauthorized instant messaging, spamming, or any unauthorized auto-response program or service.

VII. Human Resources Security

A. Prior to Employment

   All employees, consultants, and contractors who use of the City’s information technology as part of their job function are required to sign the City’s Confidentiality and Acceptable Use Agreement. Consultants and contractors who are hired to support the City’s information technology infrastructure must be able to provide proof of background checks (including a statement of what checks are conducted and how they are conducted) prior to accessing the City’s information technology infrastructure. The background checks must include a criminal background check.

B. During Employment

   1. Information Security Awareness, Education, and Training

      Security Awareness begins during the hiring process and it is the responsibility of the User to remain aware of current security policies. The City's Intranet site contains the City’s Security
Information Security Policy

Policies as well as educational materials such as the “Security First” presentation. Users should read the Security Reminders that are periodically distributed by email. Users must also respond to the Information Security Notice that is displayed while logging on to City related systems.

2. Disciplinary Process

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.

C. Termination or Change of Employment

1. Return of Assets

When a User leaves the City, all Information Assets remain the property of the City. A User 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.

2. Removal of Access Rights

Upon termination of an employee or vendor, 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 vendor. The City may automatically disable or delete accounts where termination is suspected even if formal notification was by-passed.

VIII. Communications and Operations Management

A. Protection Against Malicious Code

1. 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.

2. All servers and workstations (networked and standalone) must have the City’s approved antivirus protection software installed, properly configured, and functioning at all times. Additionally, systems that have not been issued by the City but that use the City’s network must also be protected by antivirus software.

3. All incoming and outgoing e-mails must be scanned for viruses.

4. Users are responsible for ensuring that software, files, and data downloaded onto the City’s workstations are properly scanned for viruses.

5. Users must conduct virus scans on all external media received or used by the City.

6. Users must ensure that all workstations (networked and standalone) have the most current antivirus signature files loaded.
B. Back-Up

1. 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.

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

C. Media Handling

1. Disposal of Media
   
   Except as otherwise provided by law or court order, electronic information maintained in a department's office will be destroyed by department staff or the Department of Innovation and Technology when the retention period expires, in compliance with the City's implementation of the State of Illinois Local Records Act.

D. Monitoring

1. Monitoring System Use
   
   a. 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.

   b. All information technology administrators, technicians and any other employees who by the nature of their assignments have privileged access to networks or computer systems must obtain written approval from the Department of Innovation and Technology to monitor User activity.

2. Clock Synchronization
   
   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.
IX. Access Control
A. User Access Management

1. User Account Management

a. Access to Confidential and Internal data must be made using a formal Access Request Form.

b. 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.

c. Departments must use the access request process to 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.

B. User Responsibilities

1. 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, handhelds (e.g. Blackberries) 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; and,

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.

d. Passwords must not be disclosed to anyone. All passwords are to be treated as Confidential information.
2. Screen Savers
   Use of password-protected screen savers is recommended to prohibit unauthorized system access. Screen savers should initiate after 15 minutes of inactivity. Password-protected screen savers are required on workstations that access Confidential information such as electronic Protected Health Information. Password-protected screen savers are also required on workstations that access Internal information if the workstation is not in an area that has restricted access.

C. Mobile Computing and Remote Access
   1. Laptops, off-site computers, and mobile media that contain Confidential information must be encrypted using an encryption technique approved by the Department of Innovation and Technology. Mobile media that contain Internal information must be protected using an encryption technique approved by the Department of Innovation and Technology, a strong logon password, or restricted physical access in order to protect the data. Examples of mobile media include flash drives, DVDs, CDs, and external hard drives.
   2. Personal media devices (for example, MP3 players such as iPods) must not be used as peripheral devices on City-issued workstations.
   3. 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 the Department of Innovation and Technology.
   4. 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 the Department of Innovation and Technology. Remote access through unapproved entry points will be terminated when discovered.
   5. 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.
   6. Users 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.
X. Information Security Incident Management

A. Reporting Information Security Events and Weaknesses

1. Violations of the City’s Information Security Policy or any or all parts or provisions of this Policy must be reported to Department Management or to the Department of Innovation and Technology.

2. Users must ensure that a Help Desk 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.

3. 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.
XI. **Compliance**

A. **Compliance with Legal Requirements**

1. **Intellectual Property Rights**
   
   a. 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.
   
   b. 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.

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.

3. **Compliance with Relevant Laws and Regulations**
   
   By virtue of the City’s services to its constituents and the nature of its legal status, the City is covered by certain laws and regulations dealing with security and privacy of information, most notably the Illinois Personal Information Protection Act (PIPA), the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry’s Digital Security Standard (PCI DSS). These laws and regulations, in some circumstances, may require additional safeguards for protection the City’s information beyond the stipulations of this Policy. (For example, when accessing credit/debit cardholder data remotely, it is never to be stored on local hard drives, floppy disks, or external media. Furthermore, cut-and-paste and print functions are prohibited during remote access sessions.) Accordingly, Users with access to Protected Health Information (PHI) must abide by HIPAA and Users with access to credit/debit card information must abide by PCI, as applicable.

4. **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.
Appendix A – Common Terms and Definitions

1. **Computer Resources** - All related peripherals, components, disk space, system memory and other items necessary to run computer systems.

2. **Credit Card Data** - The Primary Account Number (PAN), Card Verification Value (CVV—the 3-4 digit code on the signature block on the back of a Credit Card), track data (the data read directly from the magnetic stripe of a Credit Card) and PIN Block data (also read from the magnetic stripe). The PCI DSS can be found at https://www.pcisecuritystandards.org.

3. **Department Management** - A supervisor, manager, director, commissioner, or other officer or employee of the City designated by a City agency, board, commission, department, or office to be responsible for implementation of this Policy by his/her City agency, board, commission, department, or office.

4. **Electronic Mail (E-mail)** - The transmission of messages through electronic means in a body or attachment using the City’s network or other information technology.

5. **Information Assets** - Information and data created, developed, processed, or stored by the City that has value to the City’s business or operations.

6. **Information Technology or Network and Computer Resources** - Computer hardware and software, network hardware and software, e-mail, voice mail, video conferencing, facsimile transmission, telephone, remote access services, printers, copiers, and all other printed and electronic media.

7. **Intranet** - The suite of browser-based applications and HTML pages that are available for use only with access to the City’s internal network.

8. **Internet** - The worldwide ‘network of networks’ connected to each other using the IP protocol and other similar protocols. The Internet enables a variety of information management services, including, but not limited to, e-mail, instant messaging, file transfers, file uploads, file downloads, news, and other services.

9. **Internet Services** – Any service in which its primary means of communication is the Internet. For example e-mail, web browsing and file transfers.

10. **Mobile Computing Devices** – Mobile devices and Mobile media. Mobile data processing devices are used as business productivity tools. Examples include: laptops, personal digital assistants (PDAs), smart phones, handhelds (e.g. Blackberries), and off-site desktops. Mobile media are devices typically used to transport data. Examples include: flash drives, DVDs, CDs, and external hard drives.

11. **Network** - The linking of multiple computers or computer systems over wired or wireless connections.

12. **P2P** – Peer-to-Peer network. A network where nodes simultaneously function as both “clients” and “servers” to other nodes on the network. P2P may be used for a variety of uses, but it is typically used to share files such as audio files. Examples of P2P networks include Napster, KaZaA, and LimeWire. If a node is not properly configured, any file on the device may potentially be accessed by anyone on the network.

13. **Protected Health Information** – Individually identifiable health information about an individual that relates to the past, present, or future physical or mental health or condition, provision of health care, or payment for health care.

14. **Remote Access Services** – A service that enables off-site access to the City information technology and assets. Examples include the City’s telephone exchanges, internal phone switches, wireless access points (WAP), and Virtual Private Network (VPN) connections. Remote access includes, but is not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems.

15. **Security Incident** – An event that has an adverse impact on the confidentiality, integrity, and availability of computer systems, computer networks, electronic information assets, or physical information assets.

16. **User(s)** – The City’s departments, commissions, boards, offices, officers, employees, temporary employees, interns, vendors, consultants, contractors, and authorized agents who utilize the City’s information assets and technology.

17. **World Wide Web (WWW)** – Browser-based applications and HTML pages that are available for access and use across the Internet.
# Appendix B – Change Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>01/2006</td>
<td>Unknown author.</td>
<td>Changed version and day on page 7, added the sentence that begins with “Passwords must not be shared…” on page 14, removed potential implication that passwords may be shared with authorization on page 14.</td>
</tr>
<tr>
<td>3.0</td>
<td>10/2007</td>
<td>BIS</td>
<td>The Information Management Policy V 2 was modified and renamed to Information Security Policy V 3. Information Management Policy and Information Security Policy are used as synonyms within the City of Chicago. In Version 3, there have been numerous document updates including re-arrangement of content and removal of duplicate or outdated language. Version 3 is the official policy used by BIS as of 10/2007.</td>
</tr>
<tr>
<td>3.1</td>
<td>01/2008</td>
<td>DoIT</td>
<td>Changed BIS references to DoIT.</td>
</tr>
<tr>
<td>3.2</td>
<td>01/2008</td>
<td>DoIT</td>
<td>Minor corrections (spelling etc.).</td>
</tr>
<tr>
<td>3.3</td>
<td>01/2008</td>
<td>DoIT</td>
<td>Edited VI B 2 a and i for Internet Acceptable Use and small format changes including TOC.</td>
</tr>
<tr>
<td>3.4</td>
<td>01/2008</td>
<td>DoIT</td>
<td>Removed newsgroup and mail list blanket constraint.</td>
</tr>
<tr>
<td>3.5</td>
<td>02/2008</td>
<td>DoIT</td>
<td>General cleanup and removed reference to raffles.</td>
</tr>
<tr>
<td>4.0</td>
<td>02/2008</td>
<td>DoIT</td>
<td>Citywide Review Completed. Only small format change was made.</td>
</tr>
<tr>
<td>4.1</td>
<td>10/2/2009</td>
<td>DoIT (and Compliance)</td>
<td>Screen savers should initiate after 10 minutes of inactivity” was changed to “Screen savers should initiate after 15 minutes of inactivity”</td>
</tr>
<tr>
<td>4.1</td>
<td>03/15/2010</td>
<td>DoIT</td>
<td>Document was changed to provide improved accessibility. For example, labels were added to figures. Tables were removed. Policies reviewed but remained the same.</td>
</tr>
<tr>
<td>5.0</td>
<td>12/08/2010</td>
<td>DoIT</td>
<td>The name of the CIO was removed from the document. Policies were reviewed but no policy changes were made.</td>
</tr>
<tr>
<td>5.1</td>
<td>04/04/2011</td>
<td>DoIT</td>
<td>The label for the seal of the City of Chicago was changed on the cover page. Two sentences regarding background checks were added in the Human Resources Security Section.</td>
</tr>
</tbody>
</table>