# INFORMATION SECURITY AND TECHNOLOGY POLICY

## Department of Technology and Innovation


**Latest Revision Release Date:** 05-07-2024 | **Initial Release Date:** 10-20-2014

2.1 | ISTP-Revision-21-05072024

**Classification:** Public

# Table of Contents

Policy Set Overview

1. Policy Responsibilities & Oversight
2. Physical and Environmental Security
3. Acceptable Use and Personnel Security
4. Device Build and Configuration Management
5. Application Development
6. Asset Management
7. Access Control
8. Network Security
9. Communications Management
10. Operations Management
11. Information Security Incident Management
12. Business Continuity Management
13. Compliance
14. Third-Party Security
15. Social Media and Internet Postings

Policy Set Overview

## Purpose

The Information Security and Technology Policy ("Policy") is dedicated to the following purposes. First, the Policy is to convey the highest directive of cybersecurity posture of the City of Chicago ("City") which stems to a subset of administrative, operational, and technical controls. Second, the Policy is developed, reviewed, updated, and implemented to mitigate imminent and potential cybersecurity risks to employees and affiliated third parties on data, network and information system owned by the City. Third, the Policy guides how the City complies with applicable industry standards and regulations including the Health Information Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, the Freedom of Information Act (FOIA), the Illinois State Local Records Act (LRA), the Illinois State Breach Disclosure Laws, and the Payment Card Industry Data Security Standards (PCI-DSS), Criminal Justice Information System (CJIS), American Water Works Association (AWWA).

## Policies, Standards, Guidelines and Procedures Defined

- A Policy consists of high-level statements relating to the protection of information across the organization and should be produced and ratified by senior management. A documented policy is frequently a requirement to satisfy regulations or laws, such as those relating to privacy and finance. It is an organizational mandate.
- Standards consist of specific low level mandatory controls that help enforce and support the information security policy. Standards help to ensure security consistency across the business and usually contain security controls relating to the implementation of specific technology, hardware, or software.
- Guidelines consist of recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place. Guidelines should be viewed as best practices that are not usually requirements but are strongly recommended. They could consist of additional recommended controls that support a standard or help fill in the gaps where no specific standard applies.
- Procedures consist of step-by-step instructions to assist workers in implementing the various policies, standards, and guidelines. While the policies, standards and guidelines consist of the controls that should be in place, a procedure gets down to specifics, explaining how to implement these controls in a step-by-step fashion.

## Policy Set Structure

To ensure that best practices are woven into the City's technology infrastructure, the policy set is built off industry standard framework: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5.

Furthermore, to satisfy multiple external legal and industry requirements, such as Payment Card Industry Data Security Standard (PCI-DSS), the Federal Health Insurance Portability and Accountability Act (HIPAA), Criminal Justice Information Systems (CJIS), SWIFT, Transportation Security administration (TSA) Standards and the State of Illinois Local Records Act, specific requirements have been included.

Each Policy Standard has been noted with the specific framework requirements to enable rapid cross reference of City Policy against compliance requirements.

Each document consists of four levels of hierarchical statements: Policy Number (Chapter, Numeric) – Article (Numeric) – Clause (Numeric) – Item (Alphabetic).

## Applicability

The polices apply to all City of Chicago information technology systems and networks, those entrusted to third-parties, City employees and others including but not limited to contractors, vendors, and consultants.

Not all departments in the City have the same technological implementations. While the policies reflect current technology and security advances, implemented technologies in some departments may not be of immediate compliance with the policy. The use of such technologies must be reviewed by the Chief Information Security Officer and approved by the Chief Information Officer through a policy exception process.

These policies do not foresee any exceptional situations like new legal or regulatory obligations, best practices, or emergencies that require actions that might conflict with policy statements. Should that occur, it is the responsibility of the individual who has identified such a situation to report to the Chief Information Security Office.

| Policy 1 | | Policy Owner |
|---|---|---|
| **Policy Responsibilities & Oversight** | | |
| Effective | **10-20-2014** | Department of Technology and Innovation |
| Last Revision | **05-06-2024** | |

# 1. Policy Responsibilities & Oversight

## I. Purpose

The purpose of the Information Security Policy is to formalize the Security and Internal Control standards that the City of Chicago ("City") has adopted to mitigate security risks to employee and constituent data. The requirements and standards within this policy comply with applicable external controls and regulations, including the Health Information Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act, the Payment Card Industry's Data Security Standards (PCI-DSS), the Freedom of Information Act (FOIA), the Illinois State Local Records Act (LRA) and the Illinois State Breach Disclosure Laws.

In addition, this policy defines the requirements for how computing and communication assets, systems and resources should be accessed, configured, used, and protected. These requirements, along with monitoring activities of City personnel's internet use help maintain the security of the City's technology environment.

This document is published under the authority of the Chief Information Officer, and provides a framework for safeguarding data, including personally identifiable information (PII), protected health information (PHI) and payment cardholder data (CHD), throughout the information lifecycle within the City of Chicago.

All City Departments are subject to the provisions within. Exceptions to any provision can only be granted by the Chief Information Officer, the Chief Information Security Officer, or their delegates.

The Commissioner of the Department of Assets, Information, and Services (AIS) holds the Chief Information Officer (CIO) designation. The Chief Information Security Officer (CISO) leads the Information Security Office (ISO

## II. Policy Statements

### 1.1. Roles and Responsibilities

City of Chicago employees, contractors and agents should support the information security program detailed herein.

#### 1.1.1. Management Commitment to Information Security & Sponsorship

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

a. Ultimately, the Chief Information Officer should be responsible for the establishment of the Information Security Policy. The Information Security Office should be responsible for driving day-to-day activities and enforcement.
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 information security policies, standards, and guidelines.
- Managing a data and asset classification program, which includes the identification of information and application owners.
- 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.
- Reporting on a regular basis to the Chief Information Officer.

### 1.1.2. Allocation of Information Security Responsibilities

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

a. The City's Chief Information Officer is responsible for the security of information assets and technology in the City. The Chief Information Officer 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 knowledgeable member of management by the Chief Information Officer.
   - 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 knowledgeable member of management by the Chief Information Officer.
   - 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 knowledgeable member of management by the Chief Information Officer.
   - 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 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.
   - The responsibility to monitor and control access to data is assigned to the Head of Technical Operations and Enterprise Network Architecture for file, print, email, and network access. Should that position become vacant, this responsibility will be assigned to a 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 access to data is assigned to the Information Owner responsible for that program or their delegate.

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

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.

d. An Information Owner is a manager responsible for the City's information assets. Individual Information Owners reside within Business Units or Departments, not the Department of Technology and Innovation. 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.

e. An Information Custodian is any 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 Data and Asset Classification Policy); and
   - Operationally provide assurance for the confidentiality, integrity, and availability of information.

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 should be provided by the 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.

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's technology environment. These risks must be communicated appropriately so suitable mitigating controls can be put in place and subsequently reviewed by the Internal Audit function.

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 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. Additional responsibilities include:
   - Configuring and maintaining the City network.
   - Network segmentation.
   - Providing network access control.

#### 1.1.3. Review of Information Security

A review of the City environment must be conducted by either the Information Security Office, a designated Internal Audit team, or an independent third party. The goal of the review should be to ensure proper security controls are in place throughout the organization.

The City's security policy, standards and security environment should 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.

## 1.2. Information Technology and Security Policy Maintenance

The City of Chicago Information Security Policy is approved, maintained, and annually reviewed to ensure its effectiveness.

### 1.2.1. Security Policy Approval

The Information Security Policy is approved by management. Based on the review being conducted, approvals 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 security practices, policies, and standards.
b. The Information Security Office is responsible for ensuring that the security practices and standards are reviewed and approved on an annual basis.

### 1.2.2. Additions and Changes to Policy

Any additions or changes to the Information Security Policy are managed and approved. All additions to the information security policy 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.
b. The Information Security Office is responsible for ensuring that 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 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 may be conducted or coordinated by the Information Security Office prior to 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.

### 1.2.3. Review of the Information Security Policy

An annual review of the Information Security Policy is 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.
b. The Information Security Office must perform a technical review to ensure standards remain in sync with business requirements, vendor, and industry-recommended practices, current technology, and regulatory requirements.
c. The annual review must include a review of any impacting legal changes to ensure practice compliance with applicable municipal, state, and federal laws.
d. The annual review results must be presented to the City's Chief Information Officer. Comments and requests and modification suggestions are made via the Information Security Policy Change Procedures processes outlined by the Information Security Office.

## III. Exceptions

Any exception to the policy must be submitted through a "Policy Exception form" for review and approval by the Information Security Office in advance.

## IV. Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 08/07/2012 | 5.2 | Last update of prior "Information Security Policy document. All future versions are in the "New" format." | |
| 01/15/2013 | 0.0 | Initial Draft of new format | CISO |
| O7/26/2013 | 0.1 | Approved as Release Candidate v1 | CISO |

| | | | |
|---|---|---|---|
| 12/30/2013 | 0.2 | Approved as Release Candidate v2 | CISO |
| 03/20/2013 | 0.3 | Approved as Release Candidate v3 | CISO |
| 06/19/2014 | 0.4 | Approved as Release Candidate v4 | CISO |
| 10/20/2014 | 0.5 | Released for Final Review | CISO |
| 03/22/2022 | 2.0 | Revised to include CJIS and AWWA frameworks; document layout reformatted. Technical requirements removed from policy statements. Takes into consideration the NIST 800-53 Rev5 | GRC Unit |
| 05/07/2024 | 2.1 | Editorial changes for content and clarity. Changed Policy owner to Department of Technology and Innovation. Hyperlinks updated. | GRC Unit |

| Policy 2 | | Policy Owner |
|---|---|---|
| **Physical and Environmental Security** | | |
| Effective | **10-20-2014** | Department of Technology and Innovation |
| Last Revision | **05-07-2024** | |

# 2. Physical and Environmental Security

## I. Purpose

Robust physical and environmental controls 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 are limited to individuals with an approved and demonstrated business need. Users are prohibited from using the City of Chicago's ("City") Data and Information facilities in any way that violates this policy, Federal, State, Municipal Law, and Personnel Rules. A list of authorized personnel must be established and maintained regularly to reflect changes in personnel access privileges.

## II. Policy Statements

### 2.1. Equipment Security

City of Chicago ("City") information systems should be properly protected from potential physical and environmental threats to ensure the confidentiality, integrity, and availability of the data contained within. This section covers Network Jacks and Cabling Security, Equipment Maintenance, Data Center Environmentalism, Data Supporting Utilities, Removal of Property, and Security of Off-Site Equipment. Detailed control measures are stated in Technical Process 2 – Physical and Environmental Security.

#### 2.1.1. Network Jacks and Cabling Security

Network Jacks and cables should be properly secured from unauthorized physical access and environmental threats.

#### 2.1.2. Equipment Maintenance

City of Chicago information systems should be properly maintained by authorized individuals.

#### 2.1.3. Data Center Environmentalism

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

#### 2.1.4. Data Center Supporting Utilities

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

#### 2.1.5. Removal of Property

Removal of City property from City premises is to be authorized and logged.

#### 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 Information Security and Technology Policy apply to City technical equipment and information regardless of physical location.
y facilities should have controls in place to protect the assets contained within from physical and environmental threats. Access to facilities should be controlled at defined access points. This section covers Physical Security Perimeter,

Physical Entry Controls, Securing Data Center Facilities, Working in Secure Areas, and Protecting Against External and Environmental Threats. Detailed control measures are stated in Technical Process 2 – Secure Areas.

### 2.2.1. Physical Security Perimeter

A security perimeter should be established for all non-public City facilities. Visitors to non-public City facilities should be logged and escorted as required.

a. Facility Management personnel ensure that a security perimeter is established for non-public City facilities. The strength of the security perimeter will be determined by an assessment of the risks and threats to the physical environment. Technical Operations and Enterprise Architecture is responsible for coordinating additional security perimeter controls around data center facilities.
b. The security perimeter for the City's sensitive facilities should have a staffed reception area to control access to the main entry of the facility and appropriate controls to access secondary entrances. For facilities without a staffed reception area, the perimeter should be controlled via access controls on doors and windows, and doors and windows must be always locked. Facility Management personnel should ensure that access is properly maintained.
c. Technical Operations and Enterprise Architecture ensures that City buildings are separated into secure areas based on sensitivity. Based on the sensitivity of the secure area, additional physical security measures may be implemented to provide adequate protection.
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.

### 2.2.2. Physical Entry Controls

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

a. The Information Security Office ensures that access rights to data center facilities are reviewed at least quarterly and approved by an appropriate party. Those identified as having separated from the City or no longer having a business need to access the facility shall be terminated.
b. Technical Operations and Enterprise Architecture ensures that physical access to non-public areas is tightly controlled. Doors must be secured, and only authorized personnel may have access.
c. Badges must be worn by employees, contractors, third party users and visitors and should clearly distinguish between visitors and employees. Temporary badges must expire after a set period. Badges must always be visible while in City non-public facilities.
d. Employees, contractors, vendors, and visitors are to report any lost identification badges immediately.
e. Employees, contractors, vendors, and visitors should be authorized by an authorized member of the Technical Operations and Enterprise Architecture, Information Security Office, Human Resources, or an appropriate approving party for physical entry into non-public City facilities.
f. Authorized employees must not allow unknown or unauthorized individuals into restricted areas without an escort. Employees should notify Human Resources, Building Security and/or the Information Security Office of any unrecognized and unescorted personnel within a non-public area. Human Resources is responsible for escalating the situation, as appropriate and notifying the appropriate parties, including the Information Security Office.
g. Visitor log information should be retained for a minimum of 90 days and reviewed by the Information Security Office.
h. Employees hosting visitors ensure that their visitors are escorted when on premises containing secure facilities.

### 2.2.3. Securing Data Center Facilities

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

a. Technical Operations and Enterprise Architecture ensures that Data Center access is limited to only those people with a valid business reason for access. Access should be reviewed quarterly and revoked immediately since it is no longer needed.
b. Information Owners ensure that directories and internal documents identifying locations of the City's information processing facilities, or any other sensitive or secure area are not accessible to the public.
c. Technical Operations and Enterprise Architecture ensures that unauthorized users are not permitted

unsupervised access to the data center.

d. Technical Operations and Enterprise Architecture ensures 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.

#### 2.2.4. Working in Secure Areas

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 are to follow. The manager is also responsible for implementing and communicating additional physical or procedural security requirements needed to protect information stored in the secure area.

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

c. During any relocation of an employee's workspace, the relocating employee should take reasonable measures to ensure that information assets are protected during the moving process. This includes, but is not limited to, computer and hard copy files.

d. Employees must collect 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.

e. Employees should ensure that information on whiteboards or work boards is wiped after use in unsecured areas.

#### 2.2.5. Protecting Against External and Environmental Threats

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

a. Facility Management personnel should ensure that hazardous or combustible materials are stored at a safe distance from secure areas in accordance with local safety regulations and manufacturer specifications.

b. Facility Management personnel should ensure that appropriate firefighting equipment is available at City sites. Equipment should be checked periodically. Firefighting equipment location and maintenance should follow local fire regulations.

c. Technical Operations and Enterprise Architecture ensures that backup and recovery media and facilities are located at a safe distance from main facilities. The backup facilities should be at a distance that would protect them from damage from any incident at the main site(s).

## 2.3. Auditing, Review, Certification and Termination of Access

The Information Security Office reviews swipe card usage for the Data Center monthly. Any questionable access should 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 is granted by way of a HID swipe card and is 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 should be accompanied by a person with Authorized Access and sign in and out via 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 access based on 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 clearly sign the access log upon entering and leaving the Data Center. Maintenance staff are to 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 should 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 should request immediate termination of access rights of employees or vendors leaving the department. The Human Resources Department or Approved vendors will notify the Information Security Office as part of an employee separation procedure.

d. Managers and Vendors should 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.

## III. Exceptions

Any exception to the policy must be submitted through a "Policy Exception form" for review and approval by the Information Security Office in advance.

## IV. Related Technical References and Standards

Information Security Office (2021), "*Technical Control Process for Physical and Environmental Security*"

## V. Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 08/07/2012 | 5.2 | Last update of prior "Information Security Policy document. All future versions are in the "New" format." | DoIT |
| 01/15/2013 | 0.0 | Initial Draft of new format | CISO |
| O7/26/2013 | 0.1 | Approved as Release Candidate v1 | CISO |
| 12/30/2013 | 0.2 | Approved as Release Candidate v2 | CISO |
| 03/20/2013 | 0.3 | Approved as Release Candidate v3 | CISO |
| 06/19/2014 | 0.4 | Approved as Release Candidate v4 | CISO |
| 10/20/2014 | 0.5 | Released for Final Review | CISO |
| 04/07//2022 | 2.0 | Format and headings changed, internal cross references; technical statements separated from policy statements. | GRC Unit |
| 05/07/2024 | 2.1 | Editorial changes for content and clarity. Changed Policy owner to Department of Technology and Innovation. Hyperlinks updated. | GRC Unit |

| Policy 3 | | Policy Owner |
|---|---|---|
| **Acceptable Use and Personnel Security** | | Department of Technology and Innovation |
| Effective | **10-20-2014** | |
| Last Revision | **05-07-2024** | |

# 3. Acceptable Use and Personnel Security

## I. Purpose

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

## II. Policy Statements

### 3.1. Acceptable Use

Information security, confidentiality, and copyright protection are matters of concern for employees of the City and for 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 obligated to take reasonable and customary precautions to prevent unauthorized disclosure or use of these information assets.

#### 3.1.1. Obligations

A position of trust has been conferred upon every authorized person who handles data and information to keep it secure and private. City employees, contractors, vendors, and contingent workers are obligated to recognize and adhere to these responsibilities while on or off the job.

Therefore, employees, contractors, vendors, contingent workers, and persons with access to City facilities and information are required to satisfy the following:

a. Abide by the policies and standards as documented in the *Information Security and Technology policies*, *City Employee Code of Conduct, City Employee Code of Ethics*, the *City Personnel Rules Handbook,* and published department specific requirements.
b. Protect City of Chicago assets, both physical and logical, from compromise of confidentiality, integrity, or availability.
c. Manage sensitive and confidential data in full compliance with City-wide Information Security and Technology Policies and department specific requirements. Some of these include the following:
    - Not to permit access to any sensitive or confidential data to unauthorized individuals. For example, confidential data includes but is not limited to social security numbers, driver's license numbers, credit card data or account information.
    - To maintain credit card data confidential and in full compliance with the current Payment Card Industry (PCI) Data Security Standards.
    - Not to expose health information (such as an individual's diagnosis or treatment) as protected by HIPAA

privacy and security rules.
See "*Policy 06 - Data and Asset Classification*" for data classification examples.

d. Maintain confidentiality of information outside of work and in remote access situations.
e. Report any security incidents, potential security risks or vulnerabilities to the Information Security Office (ISO) which is part of the Department of Assets, Information and Services (AIS).
f. Acknowledge that 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. All information on and transmitted to or from any computer system or network may be intercepted, recorded, read, copied, and disclosed by, and to authorized personnel, for official purposes, including criminal investigations. Access or use of any computer system by any person, whether authorized or unauthorized, constitutes consent to these terms.
g. Not to engage in or permit unauthorized use of any information in files or programs maintained by the City.
h. Not to seek to benefit personally or permit others to benefit personally through the release of City owned or managed information.
i. 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.
j. 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.
k. Not to disclose the specifics of non-public City related business to unauthorized personnel.
l. 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.
m. Not to use or request others to use the City's information technology for personal reasons beyond limited personal use.
n. 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), tablets and off-site desktops.
o. To treat all passwords as *Confidential* information.
p. Not to conduct City business on devices that allow peer-to-peer (P2P) communications (such as music file sharing) without explicit approval from the Department OF Assets, Information and Services (AIS), Information Security Office (ISO).
q. Not to use any system, application, or cloud-based product (such as Amazon S3, Dropbox, Google Docs/Drive/Hangouts, Microsoft Messenger/Windows Azure, Mozy, Rackspace, etc.) for communication, data sharing, processing, or storage without explicit approval from the Commissioner of the Department of AIS or their designate.
r. Not to aid, abet, or act in conspiracy with another to violate any part of this or any other policy.
s. Accept that they are responsible for all actions taken by them or through their assigned access accounts.
t. To report any violation of this code by anyone to his/her supervisor immediately.
u. Human Resources will provide a copy of instructions on how to access the Information Security and Technology Policies and Security Awareness materials to new employees appropriate for their position and role within the City of Chicago. New employees will acknowledge in writing that they understand their responsibilities as stated in the policies.

### 3.1.2. Disciplinary Process

Violations of an *Information Security and Technology Policy* will result in disciplinary actions, coordinated through Human Resources as defined by the *Employee Personnel Rules Handbook*. Any violation may result in disciplinary action, including termination and/or civil action and/or criminal prosecution.

a. For City employees or contractors, disciplinary action because of a *Policy* violation should 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 Rules Handbook*.

## 3.2. Prospective Employees

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

### 3.2.1. Screening

A pre-employment screening, to include a criminal background check process will 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.
b. Information gathered on potential employees or contractors must be secured in accordance with all applicable laws and regulations and be limited to a 'need to know' basis.

### 3.2.2. Terms and Conditions of Employment

New employees are responsible for reviewing and understanding all *Information Security and Technology Policies*. Employees must agree in writing to accept and abide by the Policies 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 a person under a third party's responsibility will have access to confidential information, an individual confidentiality agreement must be signed by that individual.
b. Human Resources must ensure that employees and relevant non-employees meet *Information Security and Technology Policy* requirements prior to accessing any City facility that houses confidential information.
c. Before gaining access to City information systems, employees must:
    - Review all *Policies*, or a synopsis thereof, and acknowledge their understanding and agreement to accept and abide by the standards as set forth in the *Policies*.
    - Acknowledge their understanding of the City's *Acceptable Use and Personnel Security* policy and sign appropriate confidentiality and non-disclosure agreements as required by the *Personnel Rules Handbook*.

## 3.3. 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 processes, based on the circumstances, to terminate access.

### 3.3.1. Removal of Access Rights

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

a. Employee Managers are required to immediately notify Human Resources upon the resignation or termination of any employee.
b. Upon notification of termination, user provisioning processes 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. The Information Security Office is responsible for performing periodic audits ensuring this process is adequately functioning.
c. Upon termination of an employee or contractor, the person who requested access to technology resources may request the termination of that access using the City's access request procedure. If the requestor is not available or

known, 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 bypassed.

#### 3.3.2. Return of Assets

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.
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.

### 3.4. User Training

City employees may 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 Technology and Security Policies* and educational materials. Employees should read all Security Reminders that are distributed periodically. System users are expected to respond to any Information Security Notice that is displayed while logging on to City systems.

#### 3.4.1. Information Security Awareness, Education, and Training

Responsibility for training City employees on an annual basis should be assigned to ensure all employees are properly educated in 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 should create a security awareness, education, and training program to promote constant security awareness to all employees. The security awareness program may consist of training, continuous awareness briefings, links to relevant information and other forms of communicating information.
b. New employees should be briefed on the *Policies* and related procedures. A written summary of the basic information security measures may also 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.
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 information about the proper use of City resources.
d. The Information Security Office is responsible for posting security advisories for system users who may be affected by security issues. Security advisories may include warnings about viruses, social engineering, new technical vulnerabilities, and other specifics security risks to City as well as their associated counter measures.
e. Employees and contractors should receive and acknowledge information security awareness information at least annually.

## III. Exceptions

Any exception to the policy must be submitted through a "Policy Exception form" for review and approval by the Information Security Office in advance.

## IV. Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 08/07/2012 | 5.2 | Last update of prior "Information Security Policy document. All future versions are in the "New" format." | DoIT |
| 01/15/2013 | 0.0 | Initial Draft of new format | CISO |

| | | | |
|---|---|---|---|
| O7/26/2013 | 0.1 | Approved as Release Candidate v1 | CISO |
| 12/30/2013 | 0.2 | Approved as Release Candidate v2 | CISO |
| 03/20/2013 | 0.3 | Approved as Release Candidate v3 | CISO |
| 06/19/2014 | 0.4 | Approved as Release Candidate v4 | CISO |
| 10/20/2014 | 0.5 | Released for Final Review | CISO |
| 04/07/2022 | 2.0 | Revised to include CJIS and AWWA frameworks; document layout reformatted. Technical requirements removed from policy statements. Takes into consideration the NIST 800-53 Rev5. | GRC Unit |
| 05/07/2024 | 2.1 | Editorial changes for content and clarity. Changed Policy owner to Department of Technology and Innovation. Hyperlinks updated. | GRC Unit |

| Policy 4 | | Policy Owner |
|---|---|---|
| **Device Build and Configuration Management** | | |
| Effective | **10-14-2014** | Department of Assets, Information & Services |
| Last Revision | **05-07-2022** | |

# 4. Device Build and Configuration Management

## I. Purpose

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

## II. Policy Statements

### 4.1. Security Requirements of Systems

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

#### 4.1.1. Management Commitment to Information Security & Sponsorship

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

a. Software Development ensures that security requirements are determined prior to the application development phase for systems. Application Development Management ensures that these requirements are implemented during testing. System requirements include specifications for:
   - Access control
   - Authorization
   - System criticality
   - Information classification
   - System availability
   - Information confidentiality and integrity

b. Software Development ensures that a security assessment is conducted, and control requirements are documented.

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

#### 4.1.2. Platform/Device Build Standards

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

a. Technical Operations and Enterprise Network Architecture ensures that technical build standards exist for critical platforms and contain clearly defined, required security parameters. Such build standards 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.
- unnecessary and insecure services are disabled.
- Technical Operations and Enterprise Network Architecture, and Software Development ensure that a common configuration management standard, which complies with the requirements set forth in this information security policy, is enforced across devices and includes but is not limited to, network devices, City PCs, and Point of Sale systems.

## III. Exceptions

Any exception to the policy must be submitted through a "Policy Exception form" for review and approval by the Information Security Office in advance.

## IV. Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 08/07/2012 | 5.2 | Last update of prior "Information Security Policy document. All future versions are in the "New" format." | DoIT |
| 01/15/2013 | 0.0 | Initial Draft of new format | CISO |
| O7/26/2013 | 0.1 | Approved as Release Candidate v1 | CISO |
| 12/30/2013 | 0.2 | Approved as Release Candidate v2 | CISO |
| 03/20/2013 | 0.3 | Approved as Release Candidate v3 | CISO |
| 06/19/2014 | 0.4 | Approved as Release Candidate v4 | CISO |
| 10/20/2014 | 0.5 | Released for Final Review | CISO |
| 04/07/2022 | 2.0 | Revised to include CJIS and AWWA frameworks; document layout reformatted. Technical requirements removed from policy statements. Takes into consideration the NIST 800-53 Rev5 | GRC Unit |
| 05/07/2024 | 2.1 | Editorial changes for content and clarity. Changed Policy owner to Department of Technology and Innovation. Hyperlinks updated. | GRC Unit |

| Policy 5 | | Policy Owner |
|---|---|---|
| **Application Development** | | |
| Effective | **10-20-2014** | Department of Technology and Innovation |
| Last Revision | **05-07-2024** | |

# 5. Application Development

## I. Purpose

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

## II. Policy Statements

### 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, should be followed. Clear segregation of duties should be established between release managers, testers, and developers to effectively manage viewing, changing, and migration of source code. Additionally, a technical review should 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 are to be in place requiring the physical separation of development, test, and production environments.

a. Technical Operations and Enterprise Network Architecture ensures that the production, test, and development environments are physically and/or logically separated.
b. Technical Operations and Enterprise Network Architecture ensures 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.
c. Technical Operations and Enterprise Network Architecture ensures 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.

#### 5.1.2. Segregation of Duties

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

a. Application Development should ensure that specific segregation of duties controls is in place and that distinct, separate roles exist for developers, release managers, and testers.
d. Application Development and the Information Security Office ensures that directories or repositories containing application source code are secured from unauthorized access.
e. Application Development ensures 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.

#### 5.1.3. Information Leakage

See Technical Control Reference for controls should be implemented to prevent information leakage at system runtime.

#### 5.1.4. Outsourced Software Development

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

a. Contracts for outsourced development must be reviewed by the Department of Law and Application Development.
b. Code, software, or infrastructure provided by an outsourced development contractor should be reviewed and accepted in writing by Application Development in conjunction with the Information Security Office.
c. The Department of Law ensures that outsourced software development contracts provide protections for the City including the following:
d. Application Development is responsible for monitoring activity performed by software development firms engaged by the City.
e. Application Development or any Department or Business Unit seeking to contract for outsourced software development must notify the Department of Technology and Innovation prior to the release of any requests for proposal or information.

#### 5.1.5. Technical Review of Applications After changes

a. After changes (e.g., patches, upgrades, or new versions), Application Development ensures that applications and support processes are reviewed and tested as deemed necessary. These processes include but are not limited to the following.
b. Application Development must ensure that 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.
c. Code changes should 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 and Information Security. 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.
d. Application Development ensures that 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 should be conducted in a separate, independently controlled environment.
e. Application Development ensures that 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 includes tests of major functions, processes, and interfacing systems, as deemed necessary.

### 5.2. Secure Coding Standards

#### 5.2.1. Secure Coding Requirements

A secure coding standard should be utilized as part of the software development methodology. Detailed guidelines can be found on Process 5.

#### 5.2.2. Input Data Validation

Data entered into City application systems should be validated where possible to ensure information quality and mitigate the impacts of web-based attacks. Detailed guidelines can be found on Process 5.

a. Application Development implements data checks within information systems and applications to validate business transactions, standing/master data, or parameter tables.

#### 5.2.3. Developer Training

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.

### 5.3. Security of System Files

Operational systems should 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

Operational software should be an authorized version supported by the vendor, where applicable, and configured securely. Detailed controls guidelines can be found on Process 5.

#### 5.3.2. Protection of Live Data in Test Environments

Data classified as private or higher used in any non-production environment should be altered or obfuscated. Detailed guidelines can be found on Process 5.

## III. Exceptions

Any exception to the policy must be submitted through a "Policy Exception form" for review and approval by the Information Security Office in advance.

## IV. Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 08/07/2012 | 5.2 | Last update of prior "Information Security Policy document. All future versions are in the "New" format." | DoIT |
| 01/15/2013 | 0.0 | Initial Draft of new format | CISO |
| O7/26/2013 | 0.1 | Approved as Release Candidate v1 | CISO |
| 12/30/2013 | 0.2 | Approved as Release Candidate v2 | CISO |
| 03/20/2013 | 0.3 | Approved as Release Candidate v3 | CISO |
| 06/19/2014 | 0.4 | Approved as Release Candidate v4 | CISO |
| 10/20/2014 | 0.5 | Released for Final Review | CISO |
| 04/07/2022 | 2.0 | Revised to include CJIS and AWWA frameworks; document layout reformatted. Technical requirements removed from policy statements. Takes into consideration the NIST 800-53 Rev5. | GRC Unit |
| 05/07/2024 | 2.1 | Editorial changes for content and clarity. Changed Policy owner to Department of Technology and Innovation. Hyperlinks updated. | GRC Unit |

| Policy 6 | Policy Owner |
|---|---|
| **Data and Asset Classification** | |
| Effective **10-20-2014** | Department of Technology and Innovation |
| Last Revision **05-07-2024** | |

# 6. Data and Asset Classification

## I. Purpose

A risk-based information data and computer asset classification scheme has been established to ensure that data is handled and managed appropriately. Data and computer assets are to 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.

## II. Policy Statements

### 6.1. Responsibility for computer and Information Assets

Computer and information ("data") assets are to be accounted for and have an assigned owner. Acceptable use of City assets should be understood by employees and contingent staff.

#### 6.1.1. Ownership of Computer Assets and Data

Unless specifically identified and approved by the Department of Law, information possessed or used by a particular department and information stored and processed over the City's technology and information systems are the property of the City and are to have a designated Data Owner. City employees and contingent staff 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. Physical computing assets should have an assigned Asset Owner.
b. Production information possessed or used by a particular organization or business unit within the organization is to have a designated Data Owner. Ownership and custodianship of assets is to be documented.

#### 6.1.2. Data Governance

The accountability and responsibility for ensuring the confidentiality, integrity and availability of City owned and managed data should be defined.

a. The below Table 1 provides definitions of the three defined data roles. The Department of Technology and Innovation and the Department of Law are responsible for developing the roles and responsibilities for proper data handling procedures.

*Table 1 Data Roles and Responsibilities Definition*

| | |
|---|---|
| Data Owner | The individual(s), normally a manager or director, who has accountability and responsibility for the integrity, accurate reporting, and use of computerized data. This individual(s) typically exists within the department that generated the data and is ultimately accountable for its accuracy and proper handling. |
| Data Custodian | The individual(s) and department(s) responsible for the storage, safeguarding and availability of computerized data. The Department of Technology and Innovation is a primary Custodian within the City. |
| Data Consumer | The individual(s) and department(s) that use provided data to perform a job responsibility including the possible generation of new data. A data consumer may also be a data custodian if that person transfers data from its original location.<br><br>*Example*: If an employee or contingent worker transfers data from a server or website to their workstation, that individual is not only a consumer but also a custodian of that data and is responsible for its proper handling. |

### 6.1.3. Acceptable use of Computer Assets

The acceptable use of resources, information and assets should be documented and understood by staff (see *Acceptable Use and Personnel Security Policy*). The 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, Data Owners and Department Management are primarily responsible for developing recommendations and minimum standards.
b. An up-to-date list of technologies as approved/coordinated by Technical Operations and Enterprise Network Architecture should be maintained and readily available.

### 6.1.4. Inventory of Computer Assets

An inventory of information assets, including systems, software, and service providers, is to be always kept current.

a. Technical Operations and Enterprise Network Architecture should compile and maintain a data repository catalog on third party software-related assets (e.g., application software, development tools and third party purchased software). This catalog should 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 to assist in maintaining this catalog and should communicate any changes or additions.
b. Technical Operations and Enterprise Network Architecture should compile and maintain a data repository catalog of physical assets owned by the City. This catalog should be reviewed and updated annually. The catalog should contain descriptive asset information. Business unit managers should assist Technical Operations and Enterprise Network Architecture in maintaining this catalog and should communicate changes or additions in a timely manner.

## 6.2. Information and Data 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, should be used to ensure appropriate security protections are placed around information during handling.

### 6.2.1. Information and Data Classification Guidelines

An information classification scheme should be used throughout the organization to protect the 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 information assets and should define procedures for proper data identification and handling.
c. Data Owners or an assigned Data Custodian is responsible for defining the classification of an information asset.
d. It is the Data Owner or delegated Data Custodian's responsibility to monitor information assets and continuously review the information's classification. The Data Owner or delegated Data Custodian should sponsor a formal declassification effort before information can be downgraded to a lower classification, based upon the definitions of the classification.
e. Employees, contractors, and vendors should protect all the City's information in any format (e.g., hard copy, disk, tape, flash drive) at a level commensurate with its value as determined by its information classification. These standards mitigate the risk that information of different classification levels is inadvertently combined and released. Correctly classified information with proper controls can be instituted to manage the dissemination of information throughout the City's environment.

### 6.2.2. Information and Data Classification Scheme

The City has a four-tier classification system consisting of "Public," "Internal", "Sensitive" and "Confidential" levels of classification.

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, employment advertisements, press releases and marketing materials.*

b. **Internal** Information is defined as information that is related to the day-to-day operations of City departments and services. All data classified as Internal is subject to the Illinois Freedom of Information Act (FOIA) and if disclosed would have minimal to no impact on the confidentiality, integrity or availability of City data or computer assets.
   - *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 by the Department of Law.
   - *Examples include internet protocol (IP) addresses of computer assets, design, and 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 Department of Law. Confidential information may be exempt from disclosure under the Freedom of Information Act (FOIA).
   - *Examples include information related to the City's Information Security (aka Cyber Security) controls, strategic planning, operational means and methods, network diagrams, passwords, Card Holder Data (CHD) as defined under PCI, Personal Health Information (PHI), Personally Identifiable Information (PII) and all other legally protected material.*

### 6.2.3. Information and Data Labeling and Handling

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

a. Data Owners are responsible for ensuring that removable media containing *non-Public* data is labeled with its information classification, owner, contact information and purpose.

b. Technology Operations and Enterprise Network Architecture is responsible for ensuring that efforts are made to separate C*onfidential* information from other information with specific security or control requirements.

c. Employees are responsible for ensuring that any electronic information approved for deletion 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.

d. Data Owners or designated Data Custodians are responsible for ensuring that *Confidential* information is secured in one of the following ways:
   - 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
   - Electronic information must be encrypted using an Information Security Office approved method when stored on any portable device or media (e.g., laptop, hard drive, tape, compact disc, flash drive).

### 6.2.4. Information and Data Management

To help ensure legal and information security control of City and constituent information, data at rest must remain within the physical boarders of the United States.

a. Data Owners are responsible to ensure that no City owned data is forwarded to non-US locations unless as part of approved business operations which has prior approval from the Information Security Office.
   NIST 800-53, FedRAMP

b. Data Owners, in partnership with the Departments of Innovation and Technology, Procurement Services, and Legal must ensure that contracts with third parties, who may handle City data, meet, or exceed NIST 800-53 and/or FedRAMP-moderate level security controls.

## III. Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 08/07/2012 | 5.2 | Last update of prior "Information Security Policy document. All future versions are in the "New" format." | DoIT |
| 01/15/2013 | 0.0 | Initial Draft of new format | CISO |
| O7/26/2013 | 0.1 | Approved as Release Candidate v1 | CISO |
| 12/30/2013 | 0.2 | Approved as Release Candidate v2 | CISO |
| 03/20/2013 | 0.3 | Approved as Release Candidate v3 | CISO |
| 06/19/2014 | 0.4 | Approved as Release Candidate v4 | CISO |
| 10/20/2014 | 0.5 | Released for Final Review | CISO |
| 04/07/2022 | 2.0 | Revised to include CJIS and AWWA frameworks; document layout reformatted. Technical requirements removed from policy statements. Takes into consideration the NIST 800-53 Rev5. | GRC Unit |
| 05/07/2024 | 2.1 | Editorial changes for content and clarity. Changed Policy owner to Department of Technology and Innovation. Hyperlinks updated. | GRC Unit |

| Policy 7 | Policy Owner |
|---|---|
| **Access Control** | |
| Effective **10-20-2014** | Department of Technology and Innovation |
| Last Revision **05-07-2024** | |

# 7. Access Control

## I. Purpose

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

## II. Policy Statements

### 7.1. Business Requirements for Access Control

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

#### 7.1.1. Access Control Policy

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

a. Technical Operations and Enterprise Network Architecture is responsible for ensuring that physical and logical access controls are established.

b. Technical Operations and Enterprise Network Architecture is responsible for ensuring that access rights granted and revoked from systems are approved using an authorization form signed by Application Owners. Access rights granted to systems must be limited to the minimum access rights necessary for the user to fulfill their responsibilities as determined by their role. Technical Operations and Enterprise Network Architecture should 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.

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

d. For users with similar duties, groups, or role-based access controls (RBAC) should be used to assign access to individual accounts based on job descriptions, duties, or function.

e. The Information Owner should 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.

f. Technical Operations and Enterprise Network Architecture should ensure that access to confidential data is administered via an automated access control system.

g. Technical Operations and Enterprise Network Architecture should ensure that access to computer systems is controlled by an authentication method involving a minimum of a username and password combination. The username and password combination provides verification of the user's identity. Based on risk and compliance

requirements, two-factor authentication or better should be implemented.

h. Technical Operations and Enterprise Network Architecture should 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.

i. Technical Operations and Enterprise Network Architecture should ensure that there is a default "deny-all" setting on technical platforms. Administration accounts or accounts that can override system or application controls must be based upon job function and necessity. These privileges should only be allocated on a need-to-have basis.

j. Departments should use the access request process to immediately notify the Department of Technology and Innovation 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

City employees and all third parties working on behalf of the City 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 portable desktop equipment).

a. Users should ensure that private hardcopy information is kept in a secure, locked location when unattended.

b. Users should ensure that incoming and outgoing mail points, facsimile machines, and photocopiers are protected against unauthorized use or interception.

c. Users should 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.

### 7.2.2. Password Use

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

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

c. Passwords should not be disclosed to anyone.

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

e. All passwords are to be treated as *Confidential* information.

## 7.3. User Identification

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

### 7.3.1. User Registration

Users should 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 should ensure that user registration, modification, and de-registration procedures are implemented for user access rights on information systems.

b. Technical Operations and Enterprise Network Architecture should ensure the initial passwords are unique. Initial passwords should meet City password composition standards. The user should 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.)

#### 7.3.2. User Identification

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

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

b. Technical Operations and Enterprise Network Architecture should ensure that 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.

c. Technical Operations and Enterprise Network Architecture should 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 the risks associated with using group IDs such as the loss of individual accountability.

d. Technical Operations and Enterprise Network Architecture should 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, should be approved by the Information Security Office.

e. Technical Operations and Enterprise Network Architecture should ensure that 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 should not be logged into directly if their usage cannot be tracked.

#### 7.3.3. Default Accounts

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

a. Technical Operations and Enterprise Network Architecture should ensure the default vendor passwords are changed immediately following installation.

#### 7.3.4. Third Party Account

Additional security measures should 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 should ensure that any accounts used by contractors or vendors are only activated during the period needed to complete the current maintenance task.

### 7.4. Authentication

Authentication to City information systems should be governed by strong password composition guidelines in addition to strong session level controls, logging, and audit capabilities.

#### 7.4.1. Password Standards

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

a. Security awareness training should communicate password procedures and policies to City of Chicago employees.

b. Technical Operations and Enterprise Network Architecture and Application Development should 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.

c. Technical Operations and Enterprise Network Architecture should ensure that computers, databases, and applications that store user account and password information restrict access only to authorized operations personnel and that password information is rendered unreadable during transmission and storage on system components using strong cryptography based on approved standards.

d. Technical Operations and Enterprise Network Architecture should ensure that information systems use password history techniques to maintain a password history of users. The history file should contain the

last 4 passwords of users and store them in an encrypted form. Users should not be allowed to use a password contained within a specific user's password history.

e. Users should be forced to change passwords at least every ninety (90) days. Technical Operations and Enterprise Network Architecture should enforce this through technical means by enabling password aging controls on systems.

#### 7.4.2. Inactive Accounts

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

#### 7.4.3. Session Restrictions

Computer sessions that are not being actively used automatically terminate or lockout.

#### 7.4.4. Secure Network Controls

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

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

b. Technical Operations and Enterprise Network Architecture should implement network access control technologies within the PCI environment to limit access to the City of Chicago Network to only authorized systems and processes.

#### 7.4.5. Secure System Login

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

### 7.5. Authorization

Authorized users should be authenticated before granting access to any City system. Information systems should be reviewed regularly 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 are to promptly revoke or amend privileges no longer required by users.

a. Technical Operations and Enterprise Network Architecture and Information Owners should ensure that privileges assigned to employees transferring or changing job responsibilities are reviewed and re-allocated as determined by their new role.

b. Technical Operations and Enterprise Network Architecture and Information Owners should ensure that special or privileged access to systems (such as administrative or supervisor accounts) are reviewed quarterly. Any changes made to privileged accounts should be logged and periodically reviewed.

c. Information Owners are responsible for reviewing system privileges on a periodic basis and should promptly revoke or amend privileges no longer required by users. Reviews should be conducted twice yearly. It is the responsibility of the Technical Operations and Enterprise Network Architecture to ensure that Information Owners are provided with the proper reports to review current user access.

### 7.6. Remote Access

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

#### 7.6.1. Mobile Computing and Remote Access

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

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 Technical Operations and Enterprise Network Architecture and the Information Security Office.

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 Technical Operations and Enterprise Network Architecture and the Information Security Office. Remote access through unapproved entry points or methods (e.g. LogMeIn, GoToMyPC, TeamViewer) is not permitted and will be terminated without notice 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.

## III. Exceptions

7.2.3.E. Exceptions:

- "Service-Accounts" are exempt from password change frequency requirements. Service-Accounts are user accounts that are configured for use solely by inter or intra computer or application processes. Only the Department of Technology and Innovation may authorize their use as part of an approved computer or application system.
- "External-Accounts" are exempt from the password change frequency requirements. External Accounts are typically application-level user accounts provided to users to access external services such as web sites. These users are typically residents or other constituents.

Any exception to the policy must be submitted through a "Policy Exception form" for review and approval by the Information Security Office in advance.

## IV. Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 08/07/2012 | 5.2 | Last update of prior "Information Security Policy document. All future versions are in the "New" format." | DoIT |
| 01/15/2013 | 0.0 | Initial Draft of new format | CISO |
| O7/26/2013 | 0.1 | Approved as Release Candidate v1 | CISO |
| 12/30/2013 | 0.2 | Approved as Release Candidate v2 | CISO |
| 03/20/2013 | 0.3 | Approved as Release Candidate v3 | CISO |
| 06/19/2014 | 0.4 | Approved as Release Candidate v4 | CISO |
| 10/20/2014 | 0.5 | Released for Final Review | CISO |
| 04/07//2022 | 2.0 | Format and headings changed; internal cross references removed; technical statements separated from policy statements. | GRC Unit |
| 05/07/2024 | 2.1 | Editorial changes for content and clarity. Changed Policy owner to Department of Technology and Innovation. Hyperlinks updated. | GRC Unit |

| Policy 8 | Policy Owner |
|---|---|
| **Network Security** | |
| Effective **10-20-2014** | Department of Technology and Innovation |
| Last Revision **05-07-2024** | |

# 8. Network Security

## I. Purpose

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

## II. Policy Statements

### 8.1. Network Administration/Security Management

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

#### 8.1.1. Device Configuration

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

a. Technical Operations and Enterprise Network Architecture management should 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.
b. Technical Operations and Enterprise Network Architecture should ensure that external firewalls employ stateful inspection or dynamic packet filtering to allow only established connections into the City network.
c. Technical Operations and Enterprise Network Architecture management should ensure that routers are governed by a router technical configuration standard, and that security hardening of the routers is a component of the standard.
d. Technical Operations and Enterprise Network Architecture management should ensure that a common router and firewall configuration files are synchronized across devices and that they are not managed in a one-off fashion.

#### 8.1.2. Network Documentation

Network configuration and topology should be adequately documented.

e. Technical Operations and Enterprise Network Architecture management should maintain appropriate network documentation, including a high-level network diagram specifically noting inbound and outbound network connections into areas containing Confidential data, including wireless network components.
f. Application Owners are responsible for maintaining network documentation specific to the Confidential data environment, including transaction level detail highlighting the points at which Confidential data is transferred throughout the City of Chicago network and to external organizations. This documentation should be kept current to reflect any changes to network infrastructure or business processes associated with the confidential and sensitive data environment.

### 8.2. Networks

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

### 8.2.1. Connection Approval

Devices connected to and any connections, inbound or outbound, should be properly documented by Technical Operations and Enterprise Network Architecture

a. Technical Operations and Enterprise Network Architecture should 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 should manage and implement a formal process for testing and approving changes to external firewalls and routers. This process should clearly define the steps and requirements for adequate testing of the change and set forth a structure of approvals required to implement various changes.
c. Only City managed and approved computer assets may be connected to the City network. Exceptions are only 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 should be used to separate trusted and untrusted networks and networks of different levels of trust.

a. Technical Operations and Enterprise Network Architecture management should ensure that a DMZ has been implemented to limit traffic into the City network only necessary business services, ports, and protocols.
b. Technical Operations and Enterprise Network Architecture management should 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.
c. Technical Operations and Enterprise Network Architecture should ensure that internal addresses cannot pass through the Internet into the DMZ.
d. Technical Operations and Enterprise Network Architecture management should ensure that any database containing cardholder data is placed securely on the internal network, properly segmented from the DMZ.

## 8.3. Firewalls

Firewalls and their associated rules within the City of Chicago network should be documented, approved, and managed. Firewalls should be installed, and firewall configurations must be documented, approved, and maintained.

### 8.3.1. Use of Firewalls

Firewalls should be deployed to restrict inbound and outbound connections to the City of Chicago corporate network. Firewall configuration requirements should be put in place that restrict connections between networks that are not managed by the Department of Technology and Innovation (DTI) and any system or components that contain sensitive or confidential data.

a. Technical Operations and Enterprise Network Architecture should ensure that firewalls are placed at each Internet connection and between any DMZ and the internal network.
b. Technical Operations and Enterprise Network Architecture should ensure that personal firewalls are implemented on a laptop or employee-owned computers with direct access to the Internet and the City network, and the firewall configurations cannot be altered by the end users.
c. Technical Operations and Enterprise Network Architecture should ensure that firewalls are installed and configured to deny or control traffic between any wireless networks and systems that store confidential data.

### 8.3.2. Rule Management

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

a. Technical Operations and Enterprise Network Architecture should ensure that traffic inbound and outbound to the

confidential and sensitive data environment is restricted to those connections required by the confidential and sensitive environment. Other traffic must be specifically denied. Enterprise Network and Architecture should ensure that restrictions are appropriately documented.

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

c. Technical Operations and Enterprise Network Architecture should ensure that no insecure protocols are used in any network zone. An insecure protocol is a protocol where an ID and/or its password is not encrypted before transmission.

d. The Information Security Office should ensure that a review of firewalls and routers restricting access to confidential data environments occurs at least every six months. This activity should include a review of the specific ports/services/protocols allowed into the environment and proper documentation of the review.

## 8.4. Wireless Security

Proper security controls, such as authentication, logging, and encrypted transmission should be used for wireless devices. Additionally, processes should 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 should be in place to identify and remove rogue access points connected to the City network.

a. Technical Operations and Enterprise Network Architecture approves the implementation of wireless networks. Ad hoc wireless networks are not permitted.

b. Technical Operations and Enterprise Network Architecture should ensure that rogue access points are not deployed anywhere throughout the City of Chicago network. As such, the Technical Operations and Enterprise Network Architecture should perform quarterly wireless scanning or deploy appropriate tools to identify rogue wireless access points. identified rogue access points must be investigated and disabled.

### 8.4.2. System Configuration

New wireless access points should be configured securely and approved by management to avoid unwanted access to the City network.

a. Technical Operations and Enterprise Network Architecture should ensure that wireless networks with access to the City internal network implement WPA2 or equivalent as defined by the Information Security Office to adequately authenticate wireless systems/users and provide secure transmission of data.

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

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

d. Technical Operations and Enterprise Network Architecture should ensure that proper procedures are followed to ensure that wireless access point firmware is kept up to date.

### 8.4.3. Physically Securing Access Points

Wireless access points should 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).

## III. Exceptions

Any exception to the policy must be submitted through a "Policy Exception form" for review and approval by the Information Security Office in advance.

## IV. Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 08/07/2012 | 5.2 | Last update of prior "Information Security Policy document. All future versions are in the "New" format." | DoIT |
| 01/15/2013 | 0.0 | Initial Draft of new format | CISO |
| O7/26/2013 | 0.1 | Approved as Release Candidate v1 | CISO |
| 12/30/2013 | 0.2 | Approved as Release Candidate v2 | CISO |
| 03/20/2013 | 0.3 | Approved as Release Candidate v3 | CISO |
| 06/19/2014 | 0.4 | Approved as Release Candidate v4 | CISO |
| 10/20/2014 | 0.5 | Released for Final Review | CISO |
| 04/07/2022 | 2.0 | Revised to include CJIS and AWWA frameworks; document layout reformatted. Technical requirements removed from policy statements. Takes into consideration the NIST 800-53 Rev5. | GRC Unit |
| 05/07/2024 | 2.1 | Editorial changes for content and clarity. Changed Policy owner to Department of Technology and Innovation. Hyperlinks updated. | GRC Unit |

| Policy 9 | | Policy Owner |
|---|---|---|
| **Information Exchange Management** | | |
| Effective | **10-20-2014** | Department of Technology and Innovation |
| Last Revision | **05-07-2024** | |

# 9. Information Exchange Management

## I. Purpose

The way that City of Chicago ("City") information is exchanged should be clearly defined and managed. Employees and contractors are responsible for safeguarding their communications, no matter what the form, to adequately protect the confidentiality, integrity and availability of City data and computer assets.

## II. Policy Statements

### 9.1. Exchange of Information

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

#### 9.1.1. Information Exchange Policies and Procedures

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

a. The Information Security Office should 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 using 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.

b. Employees, contractors, and other business partners should 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*, *Data Protection Language* or an equivalent should be formalized between the City and external parties prior to sharing data and establishing network connections to external systems.

a. The Information Security Office should be consulted to make specific considerations prior to interconnecting business information systems. Specific considerations will 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.

b. The Information Security Office, Department of Law, Department of Procurement Services, and the contracting business party should ensure that agreements including 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 and responsibilities for protecting data, copyrights, and licensing.
- Special controls for protecting private information.

#### 9.1.3. Paper-based Information Transfer

Paper-based transfer of information should 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 *Confidential* data should be logged as part of a management-approved business process.
b. Confidential data should 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.
c. Employees should ensure that any media sent via interoffice mail, courier, or other means are clearly labeled with the appropriate recipient information.
d. City information should 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. Confidential information must be stored in locked drawers, cabinets, or rooms specifically designated for that purpose and accessible only by authorized individuals.
e. Hard copy information should be disposed of properly by either shredding the information or leaving the information in secured, designated shredder bins.
f. Departments which are involved in credit card processing should ensure that no more than the last four digits of the credit card number are printed on any receipt or documentation provided to the cardholder at the point of sale or transaction.

#### 9.1.4. Verbal Information Transfer

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

a. Discussions of or including *Confidential* information should 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 should not leave messages containing *Confidential* information on any type of telephone voice message or answering machine or forward voice messages to an external destination.

#### 9.1.5. Electronic Information Transfer

The electronic transfer of information follows information classification guidelines to ensure the confidentiality and integrity of the information is maintained. Detailed controls on electronic information transfer can be found at Process 9.

a. Availability of public records maintained in an electronic format should comply with the State of Illinois Local Records

#### 9.1.6. Removable Media Information Transfer

Transfer of information via removable media should be used on an as-needed basis only and must follow proper handling procedures. Detailed controls on Removable Media Information Transfer can be found at Process 9.

### 9.2. Encryption

A key-based encryption solution should be used by the City to protect *Confidential* data from unauthorized access while stored and in transit. Technical Operations and Enterprise Network Architecture should ensure that cryptographic key management processes and procedures are documented. Detailed controls on Encryption can be found at Process 9.

#### 9.2.1. Usage of Encryption

Encryption technologies should be approved and used where applicable.

a. The Information Security Office is responsible for validating encryption software/algorithms used by the City and maintaining/distributing an updated list of such technologies.
b. The Information Security Office should perform an annual review of the approved encryption algorithms and protocols.
c. Employees and contractors should not install any encryption software that has not been validated and approved by the Information Security Office.
d. Application Development Management and Technical Operations and Enterprise Network Architecture Management should ensure that only encryption software, algorithms and protocols approved by the Information Security Office are used to encrypt data in enterprise systems.
e. The Information Security Office 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.

### 9.2.2. Key Management

Cryptographic keys should be monitored and protected against both disclosure and misuse.

a. Employees and Contractors should treat keys (passwords or private keys) for encrypted data with the same or higher level of confidentiality as passwords for systems or applications.
b. Technical Operations and Enterprise Network Architecture should ensure that hardware (either housing key management applications or used for generation of encryption keys) is protected at the highest level of security controls.
c. Any contractual or third-party agreements involving encryption or key management should be approved by the Information Security Office.
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 include:
    - 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
e. Technical Operations and Enterprise Network Architecture is responsible for implementing monitoring and logging processes for key management activities.
f. Technical Operations and Enterprise Network Architecture should ensure that access to cryptographic keys be restricted to the fewest number of custodians necessary; and cryptographic keys be stored securely in the fewest possible locations and forms.
g. Technical Operations and Enterprise Network Architecture should ensure that dual control of cryptographic keys is in place and that key management staff sign a form stating they understand and accept their key management responsibilities.
h. The keys should be stored in an encrypted format and the key encrypting keys be stored separately from the data encrypting keys.

### 9.2.3. Data in Transit

*Confidential* data must be encrypted while in transit.

a. Employees and staff should ensure that data classified as *Confidential* is encrypted whenever sent over any network.
b. Non-console administrative access should use appropriate encryption techniques/protocols (e.g. SSH, VPN, or

SSL/TLS) to protect the confidentiality of City data.

c. Strong cryptography and security protocols such as SSL/TLS or IPSEC are used to safeguard sensitive cardholder data during transmission over open, public networks.

#### 9.2.4. Data at Rest

*Confidential* data that resides outside of an approved data center or cloud instance should be encrypted while at rest.

a. Storage of *Confidential* data outside of an approved system and/or area (e.g. USB sticks, removable hard drives, CD's, smartphones, tablets, laptops, workstations, etc.) is prohibited without prior authorization from line management and the Information Security Office

#### 9.2.5. Symmetric key Encryption

Keys used for symmetric key encryption, also called secret key encryption, should be protected as they are distributed to all parties that will use them. Detailed controls on Symmetric Key Encryption can be found at Process 9.

#### 9.2.6. 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 is issued. The private key should only be available to the end user to whom the corresponding. Detailed controls on Asymmetric Key Encryption can be found at Process 9.

#### 9.2.7. 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. Detailed controls on Proprietary Encryption Algorithms can be found at Process 9.

## III. Exceptions

Any exception to the policy must be submitted through a "Policy Exception form" for review and approval by the Information Security Office in advance.

## IV. Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 08/07/2012 | 5.2 | Last update of prior "Information Security Policy document. All future versions are in the "New" format." | DoIT |
| 01/15/2013 | 0.0 | Initial Draft of new format | CISO |
| O7/26/2013 | 0.1 | Approved as Release Candidate v1 | CISO |
| 12/30/2013 | 0.2 | Approved as Release Candidate v2 | CISO |
| 03/20/2013 | 0.3 | Approved as Release Candidate v3 | CISO |
| 06/19/2014 | 0.4 | Approved as Release Candidate v4 | CISO |
| 10/20/2014 | 0.5 | Released for Final Review | CISO |
| 04/09/2022 | | Revised to include CJIS and AWWA frameworks; document layout reformatted. Technical requirements removed from policy statements. Takes into consideration the NIST 800-53 Rev5 | GRC Unit |
| 05/07/2024 | 2.1 | Editorial changes for content and clarity. Changed Policy owner to Department of Technology and Innovation. Hyperlinks updated. | GRC Unit |

| Policy 10 | Policy Owner |
|---|---|
| **Operations Management** | |
| Effective **10-20-2014** | Department of Technology and Innovation |
| Last Revision **05-07-2024** | |

# 10. Operations Management

## I. Purpose

Information systems must be appropriately configured, operated, and maintained to ensure their confidentiality, integrity, and availability. Risk Assessments evaluating the confidentiality, integrity, and availability of City of Chicago ("City") information assets and data should be conducted on a regular basis to ensure that appropriate mitigating controls are in place to adequately protect the City's information systems and assets. In addition, monitoring capabilities and technical vulnerability analysis processes should be deployed and managed to detect information risks or incidents related to the confidentiality, integrity, or availability of the City's systems and assets.

## II. Policy Statements

### 10.1. Operational Procedures and Responsibilities

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

#### 10.1.1. Documented Operation Procedures

Operating procedures should be documented for systems and processes in the technical environment.

a. Documented operating procedures should 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

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

c. Technical Operations and Enterprise Network Architecture should ensure that 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 should be available for operations personnel.

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

e. Changes to the formal operating procedures of the technical infrastructure should be approved by Technical Operations and Enterprise Network Architecture.

#### 10.1.2. Change

Changes to computer assets 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,

signoffs, testing and back out plans.

a. System Owners should ensure that the roles and responsibilities for individuals involved in the change process are clearly defined. When defining various roles, properly segregate incompatible responsibilities.
b. Changes should be approved by the System Owner. The requester's manager should approve the business justification of the request, while the technical area manager should determine if the request is technically feasible. Data Owners should approve the request if it involves incorporating data from a different application or has potential impact on any environment containing private data.
c. System Owners should ensure that an audit trail of all changes is maintained via an approved change method.
d. Technical Operations and Enterprise Network Architecture should ensure that system and application software is backed-up before system upgrades or maintenance.
e. Security-related changes (e.g., file permissions, identification and authentication, audit, and discretionary access control) impacting environments containing *Confidential* data should be approved by the Information Security Office. Permanent fixes should be subjected to the normal change standards.
f. Only those persons authorized by Data 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.

#### 10.1.3. Patch

Appropriate patch procedures should be in place for computer assets.

#### 10.1.4. Security of System Documentation

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

a. Non-Public system documentation should be controlled and protected against unauthorized access. Access to the documentation should 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.

#### 10.1.5. Management of Removable Computer Media

All removable media containing *Confidential* data should be stored securely and documented appropriately during transit.

a. Removable media containing City data must minimally satisfy data handling requirements. See *Data and Asset Classification Policy*.

## 10.2. Risk Assessment & Risk Acceptance

Risk assessments are performed periodically across City information system environments to determine, address, and mitigate security threats. Risk assessments are performed upon initial acquisition on an information system if 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 employs risk assessment and analysis techniques to ensure adequate controls are in place.

a. Risk assessments, under the direction or coordination of Internal Audit or Information Security Office, must be performed annually.
b. Internal Audit or Information Security Office is responsible for defining the risk assessment process. The risk assessment process should allow for the systematic identification, prioritization and of information security risks.

## 10.3. System Planning and Acceptance

Information systems are 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.

## 10.4. Electronic Commerce Services

Electronic commerce (e-commerce) initiatives are 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

a. System Owners ensure that information practices treat customers' personal information with care. City e-commerce sites 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.
b. System Owners ensure that the e-commerce privacy policy is easy to find and understand. It should be open, transparent, and meet generally accepted fair information principles. The privacy policy should include details about the following:
    - What personal information is collected, used, and disclosed to other parties
    - The choices the customer has regarding 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
c. System Owners ensure that the City of Chicago accurately describes proper business practices regarding the use of unsolicited e-mail to customers. The City of Chicago posts and adheres to a "Do Not Email" policy. This policy allows customers who do not wish to be contacted online to opt out of future communications from the City of Chicago.

### 10.4.2. Security of Transactions

Online transactions should meet certain requirements in addition to local laws and regulations.

a. The Information Security Office ensures that the level of protection associated with online transactions corresponds to the risk associated with the transaction and complies with applicable laws and regulations. The following requirements should be met for online transactions:
    - Controls are established to ensure the confidentiality and privacy of the transaction and parties involved
    - Communication paths are encrypted for the parties involved whenever private information is transferred over open, public networks
    - Transaction information is stored outside publicly accessible environments

## 10.5. Media Disposal

Except as otherwise provided by law or court order, electronic information is to be destroyed 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) is to be properly documented and followed by employees and contractors.

### 10.5.1. Disposal of Hardware and Removable media

All hardware and removable media containing City of Chicago member information is to be disposed of securely. The detailed process for handling disposal of hardware and removable media is documented in Process 10.

### 10.5.2. Disposal of Paper

Paper containing City of Chicago sensitive or confidential information is to be shredded and disposed of securely. The detailed process for handling disposal of paper is documented in Technical Standards Documentation.

## 10.6. Monitoring

Logging should be enabled for information systems. The logs are to be time-synchronized and monitor system use for 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

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

#### 10.6.2. Audit Logging

Audit logs should be maintained as determined by business requirements.

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

#### 10.6.3. Protection of Log Information

Log files must be protected by security controls to prevent unauthorized manipulation. Technical details on protection of log information are documented in Process 10.

#### 10.6.4. Clock Synchronization

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

### 10.7. Malicious Program Detection

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

#### 10.7.1. Detection Software and Product Configuration

Information Systems within the technical environment should utilize anti-malware solutions. Technical details on detection software and product configuration are documented in Process 10.

#### 10.7.2. Product and Definition Updates

Anti-malware software updates should 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.

### 10.8. Technical Vulnerability

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

#### 10.8.1. Roles and Responsibilities

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

a. The Information Security Office establishes processes to identify, evaluate, prioritize, and resolve security vulnerabilities.
b. The 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 the 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 the maintenance of these distribution lists.
c. The Information Security Office is responsible for maintaining the documentation of the analysis produced by the technical vulnerability processes. The Information Security Office is also responsible for escalating or de-escalating vulnerability classifications and communicating changes, as appropriate.
d. The 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.

e. The Information Security Office establishes the processes to identify, evaluate, prioritize, and resolve security vulnerabilities.
f. The 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 the 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 the maintenance of these distribution lists.
g. The Information Security Office is responsible for maintaining the documentation of the analysis produced by the technical vulnerability processes. The Information Security Office is also responsible for escalating or de-escalating vulnerability classifications and communicating changes, as appropriate.
h. The 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

Vulnerabilities should be properly classified and remediated according to the City of Chicago change process.

a. The Information Security Office ensures that publicly accessible systems are tested for vulnerabilities prior to being made available.
b. Technical Operations and Enterprise Network Architecture ensures that technical vulnerabilities, including vendor supplied patches, are classified. The CVSS system is to be used to classify technical vulnerabilities and their associated patches.
c. Technical Operations and Enterprise Network Architecture ensures that vulnerability remediation efforts, including patch implementations, are coordinated, and processed according to the change standards. This includes meeting testing and documentation requirements.
d. Information Security Office ensures 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.

## 10.9. Backup

Information backup processes are documented and implemented.

#### 10.9.1. Information Backup

a. If backups are performed at the server or host level, the backup schedule of the most critical application on the server determines the backup frequency of the server.
b. Data Owners or an assigned delegated Data Custodian develops off-site backup rotation and retention schedules in conjunction with the Legal Department for each application that they support. This schedule reflects the criticality of the information being backed up.
c. Technical Operations and Enterprise Network Architecture performs an annual review of the off-site tape backup location to verify that the backup media is stored securely.
d. Each System Owner must have documented backup and recovery procedures.
e. Users should backup critical files by transferring or duplicating files onto the local area network, which is backed up on a scheduled basis. This includes user data created on City of Chicago PC's (e.g., files created in Microsoft Office).
f. Technical Operations and Enterprise Network Architecture ensures that backups of critical applications are sent off-site to a remote location on a schedule designed to meet the specific application recoverability requirements. The remote location should have appropriate security controls in place, including physical and environmental protection.

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

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

## III. Exceptions

Any exception to the policy must be submitted through a "Policy Exception form" for review and approval by the Information Security Office in advance.

## IV. Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 08/07/2012 | 5.2 | Last update of prior "Information Security Policy document. All future versions are in the "New" format." | DoIT |
| 01/15/2013 | 0.0 | Initial Draft of new format | CISO |
| O7/26/2013 | 0.1 | Approved as Release Candidate v1 | CISO |
| 12/30/2013 | 0.2 | Approved as Release Candidate v2 | CISO |
| 03/20/2013 | 0.3 | Approved as Release Candidate v3 | CISO |
| 06/19/2014 | 0.4 | Approved as Release Candidate v4 | CISO |
| 10/20/2014 | 0.5 | Released for Final Review | CISO |
| 05/09/2022 | 2.0 | Revised to include CJIS and AWWA frameworks; document layout reformatted. Technical requirements removed from policy statements. Takes into consideration the NIST 800-53 Rev5 | GRC Unit |
| 05/07/2024 | 2.1 | Editorial changes for content and clarity. Changed Policy owner to Department of Technology and Innovation. Hyperlinks updated. | GRC Unit |

| Policy 11 | | Policy Owner |
|---|---|---|
| **Information Security Incident management** | | |
| Effective | **10-20-2014** | Department of Technology and Innovation |
| Last Revision | **05-07-2024** | |

# 11. Information Security Incident Management

## I. Purpose

In the event of a specific incident affecting information systems, the City of Chicago ("City") has pre-planned methods for responding to various threats, including incidents related to data confidentiality, integrity, and application availability. In addition, reporting mechanisms are to be in place to ensure that proper City personnel are informed of incidents. Responsibility for incident handling operations must be assigned to an Incident Management Team, whose trained members will execute the incident response plan.

## II. Policy Statements

### 11.1. Management of Information Security Incidents

An incident management process is to be properly documented, including team responsibilities and data collection procedures.

#### 11.1.1. Documented Operation Procedures

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

#### 11.1.2. Incident Management Team, Roles & Responsibilities

The incident management team is 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
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

c. A librarian is 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 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 incidents for historical documentation

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

e. A representative from the Department of Law is to 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.

f. Key business unit leaders or analysts are to 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.

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

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.

### 11.1.3. Incident Management Procedures

Incident management processes and procedures including escalation, evidence collection, storage of data, and incident closure should 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.

b. The City of Chicago incident response procedures, 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

c. The incident response plan is to be tested at least annually.

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

e. The 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 follow the procedures as directed by Information Security Office. These individuals are not to divulge any information regarding the incident to anyone outside the immediate investigation team, including internal employees and anyone external to City of Chicago.

#### 11.1.4. Collection of Evidence

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

a. Information Security Office and the Department of Law are responsible for ensuring that 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.
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 Department of Law are the only representatives of the City of Chicago that will complete criminal referral procedures to law enforcement or regulatory authorities.

#### 11.1.5. Learning from Information Security Incidents

Security policy violations and security incidents are documented and reviewed.

a. Information Security Office documents reports of security incidents. The Information Security Office also includes a process to review incidents, document "lessons learned", and coordinate training and learning sessions for applicable areas within the City of Chicago.
b. The Information Security Office maintains a database of records containing information about violations of the Information Security and Technology Policy and will report on these violations. The records of policy violations are accessible to only authorized individuals.

## 11.2. Incident Reporting

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

Reporting Information Security Events and Weaknesses

a. Violations of the City's Information Technology and Security Policy or any or parts or provisions of this Policy must be reported to Department Management or to the City's Information Security Office.
b. Users 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. Reports of alleged violations of this Policy, or any part or provision hereof, will be investigated by the appropriate authority. During an investigation, access privileges may be suspended.

#### 11.2.1. Reporting Information Security Events

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

a. The Information Security Office is responsible for defining incident reporting and escalation processes within the City of Chicago and establishing points of contact for security incident reporting. Reporting procedures include proper documentation of resolution of security incidents.
b. The Information Security Office is responsible for communicating incident reporting and escalation processes to employees, contractors, and third-party users.
c. Disciplinary action resulting from a violation of the Information Security Policy should 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 are coordinated through the Human Resources Department.

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

f. The Department of Law must be contacted in the event of an information security event to determine whether legal requirements dictate the necessity of reporting the security incident publicly or to an external party.

## III. Exceptions

Any exception to the policy must be submitted through a "Policy Exception form" for review and approval by the Information Security Office in advance.

## IV. Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 08/07/2012 | 5.2 | Last update of prior "Information Security Policy document. All future versions are in the "New" format." | DoIT |
| 01/15/2013 | 0.0 | Initial Draft of new format | CISO |
| O7/26/2013 | 0.1 | Approved as Release Candidate v1 | CISO |
| 12/30/2013 | 0.2 | Approved as Release Candidate v2 | CISO |
| 03/20/2013 | 0.3 | Approved as Release Candidate v3 | CISO |
| 06/19/2014 | 0.4 | Approved as Release Candidate v4 | CISO |
| 10/20/2014 | 0.5 | Released for Final Review | CISO |
| 04/07/2022 | 2.0 | Revised to include CJIS and AWWA frameworks; document layout reformatted. Technical requirements removed from policy statements. Takes into consideration the NIST 800-53 Rev5 | GRC Unit |
| 05/07/2024 | 2.1 | Editorial changes for content and clarity. Changed Policy owner to Department of Technology and Innovation. Hyperlinks updated. | GRC Unit |

| Policy 12 | Policy Owner |
|---|---|
| **Business Continuity Management** | |
| Effective **10-20-2014** | Department of Technology and Innovation |
| Last Revision **05-07-2024** | |

# 12. Business Continuity Management

## I. Purpose

Business Continuity Management programs and processes ensure the mitigation of unacceptable business losses in the event of a crisis. Such processes include the identification of critical business processes and determination of business process priority, set forth requirements for development of business continuity plans, adequate recovery strategies, potential work-around procedures, and disaster recovery plans. Business continuity and disaster recovery plans 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.

## II. Policy Statements

### 12.1. Information security Aspects of Business Continuity Management

City of Chicago ensures that a 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 should be implemented for those systems resulting in unacceptable business losses in the event of downtime.

#### 12.1.1. Business Continuity Business Impact Analysis

a. A business continuity plan should be executed on a rolling cycle to identify critical business functions, set forth requirements for recovery, and determine overall function priority. The Information Security Office assists the business units and IT Senior Management to identify critical business functions and subsequently identify key systems supporting those critical functions. The analysis includes 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 should clearly define recovery time objectives and minimum acceptable recovery resources for each required supporting system.

b. The business impact analysis prioritizes business functions based on the business impacts associated with the disruption of the process. Processes should 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, the 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 ensures 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 partners with business leaders to create a standard framework for all business continuity plans. A consistent format should be published and communicated to plan owners.
b. IT Senior Management ensures that each business unit develops a business continuity plan consistent with corporate guidelines.
c. IT Senior Management must ensure that 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.
d. An appropriate business leader approves business continuity plans prior to implementation and rollout. The plan contains necessary documentation, have approval by affected business units, and meets necessary requirements, as determined by management.
e. IT Senior Management ensures that business continuity and incident response plans have a training and education schedule and that requirements are set for affected personnel.
f. Business continuity and incident response plans have a maintenance schedule. Each plan should be reviewed annually, at a minimum.

### 12.1.3. Developing and Implementing Continuity Plans

Business continuity plans 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 ensures that business continuity plans are updated and distributed appropriately.

a. IT Senior Management must ensure that 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 should be included in the plan:
    - Failover conditions or requirements necessary to invoke the plan.
    - Emergency and operational procedures for 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.
b. IT Senior Management ensures that business continuity plans are protected and are considered confidential information. Plans must be stored securely, and backups must be stored at off-site locations.
c. IT Senior Management ensures copies of the business continuity plans are distributed appropriately when plans are updated.
d. If alternate temporary locations are used for business continuity planning purposes, security controls are to be consistent with the primary site and approved by the Information Security Office.

### 12.1.4. Testing, Maintaining and Re-Assessing Business Continuity Plans

Business continuity plans should have a documented testing schedule.

a. IT Senior Management ensures that 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.

b. IT Senior Management ensures 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.

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

## III. Exceptions

Any exception to the policy must be submitted through a "Policy Exception form" for review and approval by the Information Security Office in advance.

## IV. Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 08/07/2012 | 5.2 | Last update of prior "Information Security Policy document. All future versions are in the "New" format." | DoIT |
| 01/15/2013 | 0.0 | Initial Draft of new format | CISO |
| O7/26/2013 | 0.1 | Approved as Release Candidate v1 | CISO |
| 12/30/2013 | 0.2 | Approved as Release Candidate v2 | CISO |
| 03/20/2013 | 0.3 | Approved as Release Candidate v3 | CISO |
| 06/19/2014 | 0.4 | Approved as Release Candidate v4 | CISO |
| 10/20/2014 | 0.5 | Released for Final Review | CISO |
| 04/07/2022 | 2.0 | Revised to include CJIS and AWWA frameworks; document layout reformatted. Technical requirements removed from policy statements. Takes into consideration the NIST 800-53 Rev5. | GRC Unit |
| 05/07/2024 | 2.1 | Editorial changes for content and clarity. Changed Policy owner to Department of Technology and Innovation. Hyperlinks updated. | GRC Unit |

| Policy 13 | Policy Owner |
|---|---|
| **Compliance** | |
| Effective **10-20-2014** | Department of Technology and Innovation |
| Last Revision **05-07-2024** | |

# 13. Compliance

## I. Purpose

City of Chicago ("City") employees, contractors and associated business processes are to fully comply with Information Security and Technology Policies in addition to any other City, Department, Internal, Legal, or Industry-specific regulatory requirements applicable to City of Chicago

## II. Policy Statements

### 13.1. Compliance with Security Policies, Standards, and Technical Compliance

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

#### 13.1.1. Compliance with Security Policy

Management verifies that their security responsibilities are being executed. Escalation processes must be followed when exceptions to the Information Security Policy are noted.

a. Incidents of non-compliance or exceptions to the Information Security Policy are to be reported to the Information Security Office.

b. Technical areas 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.

#### 13.1.2. Technical Compliance Verification

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

a. Information Security Office and Internal Audit assign review activities to parties to maintain compliance with City of Chicago security practices. Situations resulting in non-compliance with 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.

b. The Information Security Office ensures 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.

#### 13.1.3. Exception

Exceptions to the Information Security and Technology Policy should 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 the City of Chicago Information Security Office. Exception requests should be formally documented and submitted for review by the 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.

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.

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.

## 13.2. Compliance with Legal Requirements

Obligations must be clearly understood, and appropriate sanctions applied against employees and contingent workforce 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

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

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

Applicable material legal regulations are to be documented and defined by the City of Chicago Department of Law.

a. Applicable material legal, statutory, contractual, or regulatory requirements are to be documented and defined by the City of Chicago Department of Law. 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 with the identified regulations.

### 13.2.5. Data Protection and Privacy of Personal Information

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

a. The Information Security Office and the Department of Law 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.

### 13.2.6. Licensing of Software

The software used is to be appropriately licensed and in compliance with software copyright agreements.

### 13.2.7. Record Retention

Documentation should be retained per legal and regulatory requirements.

a. The Department of Law ensures 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

should 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 Department of Law to determine proper record retention schedules and procedures and work with the Information Security Office to meet any security-related regulatory requirements.

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.

## 13.3. System Audit Consideration

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

### 13.3.1. System Audit Controls

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

a. Audit activities are to be performed by individuals independent of the activities being audited.

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

c. Audit activities 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.

### 13.3.2. Protection of System Audit Tools

System audit tools may contain sensitive information. As such, specific measures are to 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 tools (e.g., software, applications, documentation, work papers) required for system audits should be restricted to authorized individuals. Any resulting compliance information should be restricted to authorized individuals.

# III. Exceptions

Any exception to the policy must be submitted through a “Policy Exception form” for review and approval by the Information Security Office in advance.

# IV. Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 08/07/2012 | 5.2 | Last update of prior “Information Security Policy document. All future versions are in the “New” format.” | DoIT |
| 01/15/2013 | 0.0 | Initial Draft of new format | CISO |
| O7/26/2013 | 0.1 | Approved as Release Candidate v1 | CISO |
| 12/30/2013 | 0.2 | Approved as Release Candidate v2 | CISO |

| | | | |
|---|---|---|---|
| 03/20/2013 | 0.3 | Approved as Release Candidate v3 | CISO |
| 06/19/2014 | 0.4 | Approved as Release Candidate v4 | CISO |
| 10/20/2014 | 0.5 | Released for Final Review | CISO |
| 04/07/2022 | 2.0 | Revised to include CJIS and AWWA frameworks; document layout reformatted. Technical requirements removed from policy statements. Takes into consideration the NIST 800-53 Rev5. | GRC Unit |
| 05/07/2024 | 2.1 | Editorial changes for content and clarity. Changed Policy owner to Department of Technology and Innovation. Hyperlinks updated. | GRC Unit |

| Policy 14 | | Policy Owner |
|---|---|---|
| **Third Party Security** | | |
| Effective | **10-20-2014** | Department of Technology and Innovation |
| Last Revision | **05-07-2024** | |

# 14. Third Party Security

## I. Purpose

The city of Chicago ("City") often utilizes third parties, contractors, and vendors ("third parties") in support of delivering business and technology related 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 City Information Technology and Security policies, as applicable, unless specific additional provisions have been established through contractual agreements.

The City of Chicago ensures that contracted third parties apply equal or more stringent controls in managing and protecting City of Chicago data shared with them. As such, adequate contracts and due diligence processes protecting the City of Chicago, its constituents and its members must be in place. In addition, information shared with third parties should be limited to the minimum amount necessary to complete the contracted task.

## II. Policy Statements

### 14.1. External Parties

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

#### 14.1.1. Identification of Risks Related to External Parties

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 places for all inbound and outbound connections to the City of Chicago.

a. Where there is a business need for a direct connection between the City of Chicago and a third-party network, the Information Security Office should 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.
b. The Technical Operations and Enterprise Network Architecture team ensures that inbound connections from external organizations are limited to specific hosts and specific applications on those hosts. If possible, each specific host and application are to be physically or logically segmented from production networks. External parties are not to be granted unlimited access to City of Chicago computers or networks.
c. The HR Department and the Business Owner representative responsible for the contract ensure that contingent and third-party 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 ensures that vendors sign Non-Disclosure and/or Confidentiality Agreements.
d. The Information Security Office ensures that 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.

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

f. The Information Security Office ensures 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 should be disabled upon completion of service. Business Owners are responsible for providing notification when access is no longer needed.

g. The Information Security Office maintains 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 is to be maintained.

### 14.1.2. Addressing Security in Third Party Agreements

Contracts with a contractor, vendor or third-party, where there is the potential that City of Chicago owned or managed data will be transmitted to or held by such entity, include information security specific provisions that meet or exceed City of Chicago Policies and Standards.

a. The Information Security Office and the Department of Law are responsible for the development, management and updating of these provisions.

b. All such contracts should include an agreement on acceptable security controls and a requirement that the third party provide an attestation document that their security controls meet NIST 800-53 "moderate", SSAE 16 or equivalent on an annual basis. Acceptance of equivalent standards can only be granted by the Information Security Office.

c. 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.
   - A written agreement acknowledging responsibility for securing confidential and sensitive data.
   - Complying with all due diligence procedures prior to engagement
   - Complying on an annual basis with PCI DSS and other regulatory requirements

d. 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.

e. To the extent possible, contracts should 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.

f. Any vendor or third party working under contract for City of Chicago is to 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 the Information Security Office and the Department of Law.

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

h. The Department responsible for the selection and approval of third-party services and a representative from the Department of Law must review all contracted information services agreements. Approval from the Information Security Office must also be obtained if the services provided affect the confidentiality, integrity, or availability of City of Chicago networks, involve network connectivity for third party employees or have the potential to be involved in the transference, creation or management of data classified as sensitive or above.

i. Users are not to 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 are not to 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.

### 14.1.3 Data Protection Requirements for Contractors, Vendors and Third Parties

a. General. Notwithstanding any other obligation of Contractor under this policy, Contractor agrees that it will not lose, alter, or delete, either intentionally or unintentionally, any Protected Information, and that it is responsible for the safe keeping of all such information, except to the extent that the City directs the Contractor in writing to do so.

b. Access to Data. In addition to the records to be stored / maintained by Contractor, all records that are possessed by Contractor in its service to the City of Chicago to perform a governmental function are public records of the City of Chicago pursuant to the Illinois Freedom of Information Act (FOIA), unless the records are exempt under the Act. FOIA requires that the City produce records in a very short period. If the Contractor receives a request from the City to produce records, the Contractor shall do so within 72 hours of notice.

c. Minimum Standard for Data at Rest and Data in Motion. Contractors must, at a minimum, comply with its treatment of Protected Information, with National Institute of Standards and Technology (NIST) Special Publication 800-53 Moderate Level Control. Notwithstanding this requirement, Contractor acknowledges that it must fully comply with each additional obligation contained in this policy. If data is protected health information or electronic protected health information, as defined in the Health Insurance Portability and Accountability Act and Health Information Technology for Economic and Clinical Health Act (HIPAA/HITECH) and regulations implementing these Acts (see 45 CFR Parts 160 and 164), it must be secured in accordance with "Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals," available on the United States Department of Health and Human Services (HHS) website at Breach Notification Rule | HHS.gov, or at Volume 74 of the Federal Register, beginning at page 42742. That guidance from the HHS states that valid encryption processes for protected health information data at rest (e.g., protected health information resting on a server), must be consistent with the NIST Special Publication 800-111, Guide for Storage Encryption Technologies for End User Devices. Valid encryption processes for protected health information data in motion (e.g., transmitted through a network) are those which comply with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security Implementation; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated.

d. Where Data is to be Stored. All data must be stored only on computer systems located in the continental United States.

e. Requirement to Maintain Security Program. Contractor acknowledges that the City has implemented an information security program to protect the City's information assets, which Program is available on the City website at ISTP.pdf (chicago.gov) ("City Program"). Contractor must be responsible for establishing and maintaining an information security program that is designed to: (i) ensure the security and confidentiality of Protected Information; (ii) protect against any anticipated threats or hazards to the security or integrity of Protected Information; (iii) protect against unauthorized access to or use of Protected Information; (iv) ensure the proper disposal of Protected Information; and, (v) ensure that all subcontractors of Contractor, if any, comply with all of the foregoing.

f. Undertaking by Contractor. Without limiting Contractor's obligation of confidentiality as further described herein, in no case shall the safeguards of Contractor's information security program be less stringent than the information security safeguards used by the City Program.

g. Right of Audit by the City of Chicago. The City of Chicago shall have the right to review Contractor's information security program prior to the commencement of Services and from time to time during the term of this Agreement. During the performance of the Services, from time to time and without notice, the City of Chicago, at its own expense, shall be entitled to perform, or to have performed, an on-site audit of the Contractor's information security program. In lieu of an on-site audit, upon request by the City of Chicago, Contractor agrees to complete, within forty-five (45 days) of receipt, an audit questionnaire provided by the City of Chicago or the City of Chicago's designee regarding Contractor's information security program.

h. Audit by Contractor. No less than annually, Contractor shall conduct an independent third-party audit of its information security program and provide such audit findings to the City of Chicago, all at the Contractor's sole expense.

i. Audit Findings. Contractor shall implement at its sole expense any remedial actions as identified by the City because of the audit.

j. Demonstrate Compliance - PCI. No less than annually, as defined by the City of Chicago and where applicable, the Contractor agrees to demonstrate compliance with PCI DSS (Payment Card Industry Data Security Standard). Upon City's request, Contractor must be prepared to demonstrate compliance of any system or component used to process, store, or transmit cardholder data that is operated by the Contractor as part of its service. Similarly, upon City's request, Contractor must demonstrate the compliance of any third party it has sub-contracted as part of the service offering. As evidence of compliance, the Contractor shall provide upon request a current attestation of compliance signed by a PCI QSA (Qualified Security Assessor).

k. Demonstrate Compliance – HIPAA / HITECH. If the Protected Information includes protected health information or electronic protected health information covered under HIPAA/HITECH, Contractor must execute, and be governed by, the provisions in its contract with the City regarding HIPAA/HITECH, the regulations implementing those Acts, and the Business Associate Agreement in its contract with the City. As specified in 1.3, protected health information must be secured in accordance with the "Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals."

l. Data Confidentiality. Contractor shall implement appropriate measures designed to ensure the confidentiality and security of Protected Information, protect against any anticipated hazards or threats to the integrity or security of such information, protect against unauthorized access or disclosure of information, and prevent any other action that could result in substantial harm to the City of Chicago, or an individual identified with the data or information in Contractor's custody.

m. Compliance with All Laws and Regulations. Contractor agrees that it will comply with all laws and regulations.

n. Limitation of Access. Contractor will not knowingly permit any Contractor personnel to have access to any City of Chicago facility or any records or data of the City of Chicago if the person has been convicted of a crime in connection with (i) a dishonest act, breach of trust, or money laundering, or (ii) a felony. Contractor must, to the extent permitted by law, conduct a check of public records in all the employee's states of residence and employment for at least the last five years to verify the above. Contractor shall assure that all contracts with subcontractors impose these obligations on the subcontractors and shall monitor the subcontractors' compliance with such obligations.

o. Data Re-Use. Contractor agrees that all data exchanged shall be used expressly and solely for the purposes enumerated in the Agreement. Data shall not be distributed, repurposed, or shared across other applications, environments, or business units of Contractor. As required by Federal law, Contractor further agrees that no City of Chicago data of any kind shall be revealed, transmitted, exchanged, or otherwise passed to other Contractors or interested parties except on a case-by-case basis as specifically agreed to in writing by an officer of the City of Chicago with designated data, security, or signature authority.

p. Safekeeping and Security. Contractor will be responsible for safekeeping all keys, access codes, passwords, combinations, access cards, personal identification numbers and similar security codes and identifiers issued to Contractor's employees, agents, or subcontractors. Contractor agrees to require its employees to promptly report a lost or stolen access device or information to their primary business contact and to the City of Chicago Information Security Office.

q. Mandatory Disclosure of Protected Information. If Contractor is compelled by law or regulation to disclose any Protected Information, the Contractor will provide to the City of Chicago with prompt written notice so that the City of Chicago may seek an appropriate protective order or other remedy. If a remedy acceptable to the City of Chicago is not obtained by the date that the Contractor must comply with the request, the Contractor will furnish only that portion of the Protected Information that it is legally required to furnish, and the Contractor shall require any recipient of the Protected Information to exercise commercially reasonable efforts to keep the Protected Information confidential.

r. Data Breach. Contractor agrees to comply with all laws and regulations relating to data breach, including without limitation, the Illinois Personal Information Protection Act and other applicable Illinois breach disclosure laws and

regulations. Data breaches of protected health information and electronic protected health information shall be governed by the provisions regarding HIPAA/HITECH, and the regulations implementing those Acts, in the Contractor's contract with the City, specifically the Business Associate Agreement in such contract. Contractor will immediately notify the City if security of any Protected Information has been breached, and will provide information as to that breach in such detail as requested by the City. Contractor will, if requested by the City, notify any affected individuals of such breach at the sole cost of the Contractor.

s. Data Sanitization and Safe Disposal. All physical and electronic records must be retained per federal, state, and local laws and regulations, including the Local Records Act. Where disposal is approved, the Contractor agrees that prior to disposal or reuse of all magnetic media (e.g. hard disk, floppy disk, removable media, etc.) which may have contained City of Chicago data shall be submitted to a data sanitization process which meets or exceeds DoD 5220.28-M 3-pass specifications. Certification of the completion of data sanitization shall be provided to the City of Chicago within 10 days of completion. Acceptance of Certification of Data Sanitization by the Information Security Office of the City of Chicago is required prior to media reuse or disposal. All other materials which contain City of Chicago data shall be physically destroyed and shredded in accordance with NIST Special Publication 800-88, Guidelines for Media Sanitization, specifications.

t. End of Agreement Data Handling. The Contractor agrees that upon termination of this Agreement it shall return all data to the City of Chicago in a useable electronic form, and erase, destroy, and render unreadable all data in its entirety in accordance with the prior stated Data Sanitization and Safe Disposal provisions. Data must be rendered in a manner that prevents its physical reconstruction using commonly available file restoration utilities. Certification in writing that these actions have been completed must be provided within 30 days of the termination of this Agreement or within 7 days of a request of an agent of the City of Chicago, whichever shall come first.

## III. Exceptions

Any exception to the policy must be submitted through a "Policy Exception form" for review and approval by the Information Security Office in advance.

## IV. Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 08/07/2012 | 5.2 | Last update of prior "Information Security Policy document. All future versions are in the "New" format." | DoIT |
| 01/15/2013 | 0.0 | Initial Draft of new format | CISO |
| O7/26/2013 | 0.1 | Approved as Release Candidate v1 | CISO |
| 12/30/2013 | 0.2 | Approved as Release Candidate v2 | CISO |
| 03/20/2013 | 0.3 | Approved as Release Candidate v3 | CISO |
| 06/19/2014 | 0.4 | Approved as Release Candidate v4 | CISO |
| 10/20/2014 | 0.5 | Released for Final Review | CISO |
| 04/07/2022 | 2.0 | Revised to include CJIS and AWWA frameworks; document layout reformatted. Technical requirements removed from policy statements. Takes into consideration the NIST 800-53 Rev5. | GRC Unit |
| 05/07/2024 | 2.1 | Editorial changes for content and clarity. Changed Policy owner to Department of Technology and Innovation. Hyperlinks updated. | GRC Unit |

| Policy 15 | | Policy Owner |
|---|---|---|
| **Social Media and Internet Postings** | | |
| Effective | **10-20-2014** | Department of Technology and Innovation |
| Last Revision | **05-07-2024** | |

# 15. Social Media and Internet Postings

## I. Purpose

City of Chicago ("City") employees, contractors, business partners and all other third-parties are prohibited from making statements or comments intended to be perceived as official statements by the City, a Department, or any elected official without prior authorization from the Chief Operating Officer (COO), the Mayor's Press Office (MPO), a Department Commissioner, Public Information Officer (PIO) or authorized designee.

## II. Policy Statements

### 15.1. Official City of Chicago Social Media Sites

The City utilizes multiple "on-line" channels to communicate with employees, business partners, other government organizations, media outlets and residents. Some examples of these "on-line" channels include but are not limited to Facebook, Instagram, Twitter, Blogs, Wikipedia, YouTube, and any other site where text, documents or multimedia files can be posted. As these sites are also often used by our employees and contractors for personal reasons, it is essential that all personal and official business postings be clearly differentiated. This Policy provides directions for how, who and what can be posted and how official postings on behalf of the City are to be approved and formatted.

#### 15.1.1. Clearly Identifying Official Sites and Accounts

For City-related social media sites, users must be able to recognize that a City-related site is produced and maintained by the City and not another entity or individual.

a. Official accounts should follow a standard naming convention, consistently use design elements (i.e. background, colors, images), and link back to official and relevant section(s) of the City website.
b. All official sites must be registered with the Mayor's Press Office (MPO) and will be linked from the City's website.
c. In a social media site account bio, the site must be described as "official." An example Twitter bio would be "Official Account of the City's Department of Procurement Services." All site names and designs must be approved by the Mayor's Press Office (MPO).
d. Social media communications in connection with the transaction of public business should be posted solely from a city-approved social media account and not from a personal social media account unless permission to do otherwise is obtained from the Mayor's Office and the department head.
e. City employees may include official City social media addresses and accounts on City documentation per internal Department guidelines.
f. All City official social media accounts (including but not limited to Twitter and Facebook) are the property of the City. Twitter accounts should be listed as "@DeptAccount" and Facebook as "Facebook.com/DeptAccount".

#### 15.1.2. Creation and Management of Social Media Sites

All official accounts will be managed by department *Public Information Officers (PIOs)* unless otherwise requested by the department head.

a. To establish a social media account, the PIO must make a request to the department commissioner who must then approve any official site representing their department. After securing commissioner approval, the Mayor's Press Office (MPO) must then approve the account and add it to its list of social media sites utilized by the City. The Mayor's Press Office (MPO) and the Department of Assets, Innovation and Systems (AIS) maintain an inventory of social media

sites used by City departments, including login credentials.

b. The PIO will oversee posting content and monitoring the social media site. Any comments posted by City employees should be considered part of the public record and should focus on highlighting and explaining the department's mission and should not contain any sensitive, personal, or confidential employee information.

#### 15.1.3. Site Management

All official City of Chicago web sites and presences on social media sites are considered an extension of the City's information networks and therefore must be maintained in accordance with City standards.

a. All sites must follow all City and State data retention requirements. Posts made to these sites are considered public records and must be preserved pursuant to the Illinois Local Records Act (LRA).
b. IDs and passwords must be unique. IDs and passwords created and used for social media and/or on sites must not be the same or reused on any other sites, City network, system, or application.
c. Any posts that violate Community and Posting Guidelines must be saved, archived, and then deleted.
d. The following Community and Posting Guidelines must be posted on City managed social media sites. Changes to this language must be approved by the Mayor's Press Office and the Department of Law.

"This is an open, productive forum for discussion. All opinions are welcome and respectful dialogue is encouraged. Please be respectful of the community as you interact and help ensure that replies to posts are on-topic. No graphic, obscene, explicit, or racial comments, hateful or defamatory submissions, or personal attacks will be permitted. Users should not spam the page with duplicative posts. The City has the right to delete posts and block users that violate these guidelines. Also, any links, mentions or interactions with users on this site do not constitute official endorsement by Mayor Emanuel, the Mayor's Office, or staff. Please be aware that you participate at your own risk and assume personal responsibility for your comments, your username and any information provided."

## 15.2. Prohibited Communications & Community and Posting Guidelines

All City of Chicago employees must adhere to all laws, City ordinances, policies, and rules when participating in social media. All City's Ethics rules, Acceptable Use of Assets, Codes of Conduct, Personnel Rules, and any other regulations governing the conduct of city employees apply equally to all social media postings.

No user (City or otherwise) may post, mail, display, or otherwise transmit in any manner any content, communication, or information that can be deemed offensive, a personal attack or violates an established internal code, rule, or law. Examples of prohibited communications include but are not limited to the following:

a. Interferes with official City business.
b. Is hateful, harassing, threatening, libelous or defamatory, pornographic, profane, or sexually explicit.
c. 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.
d. Impersonate a person (living or dead), organization, business, or other entity.
e. Enables or constitutes gaming, wagering, or gambling of any kind.
f. Promotes or participates in unauthorized fundraisers.
g. Promotes or participates in partisan political activities.
h. Promotes or participates in unauthorized advertising of City projects and any advertising of private projects.
i. Compromises or degrades the performance, security, or integrity of the City 's technology resources and information assets.
j. Contains a virus, logic bomb, or malicious code.
k. Constitutes participation in chain letters, unauthorized chat rooms, unauthorized instant messaging, spamming, or any unauthorized auto-response program or service.

## 15.3. Data Protection and Privacy

Due to the evolution of mobile devices, the end-user must apply the same code of conduct to usage of both City-owned and personal mobile devices. As mobile devices may contain features such as cameras and automatic location geotagging, it is imperative that end-users within the City of Chicago adhere to the Information Security Office standards and controls of Data Security and Privacy.

### 15.3.1. Reproduction and Distribution of Images

a. City of Chicago employees not enabled to work with and for the City's official social media accounts are forbidden to post photographs and videos of interior working spaces of the City of Chicago to any social media platforms. This includes both personal and public social media platforms that do not contain official City of Chicago social media accounts.

b. City of Chicago employees are expressly forbidden to photograph, video and live-stream other City of Chicago employees in City of Chicago workspaces/property and post such images and video to private and/or publicly hosted social media sites. Any exception request permission must be given by City of Chicago employees to have themselves photographed and their images reproduced, and only from assignment of Public Information Officers for documented purposes.

### 15.3.2. Social Media Data Hosting Prohibition

Many social media platforms, in addition to hosting photographs and videos, can also store documents. The afore mentioned data is contained indefinitely in almost all social media platforms; usually removed only if the user removes the data they have posted. Thus, social media platforms do not have a time limit for the storage of user-added data; even "time-sensitive "stories" featured on certain social media sites are replicated and allow for retrieval of legacy postings in a search by the user. Due to the indefinite time periods for data hosting of social media platforms, it is mandatory that City of Chicago data, including images and files, cannot be stored on social media platforms. The data storage options of the City of Chicago, including OneDrive and local network folders, must always be used to store City of Chicago data.

## 15.4 Email Communications

Email is a business communication tool, and users of the City's email system are obliged to use it in a responsible, effective, and lawful manner. Every employee has a responsibility to use this communication channel in a manner that prevents irresponsible, ineffective, offensive, or unlawful consequences. All the prohibitions listed in section 15.2 above apply to email communications.

### 15.4.1 Email Signature

An Email Signature is a block of text appended to the end of an email, typically in an automated manner, that conveys the contact details of the sender such as mailing address, telephone number(s) and similar personal and organizational details. An email that ends with a properly formatted signature helps convey the City's civic voice and style (see Chicago Design System at https://design.chicago.gov). Within the departments of the City of Chicago, an email signature is an optional addition to an email message and should follow the City's Email Signature guidelines in 15.4.2.

E-mail signatures should be aligned with the "Chicago Design System" which is the public visual identity of the City of Chicago, from which the guidelines in 15.4.2 have been derived.

### 15.4.2 Email Signature Guidelines

A guideline for formatting and email signature is necessary to ensure consistency across City departments and programs and helps to avoid the presence of content prohibited in section 15.4 above.

Below are acceptable elements of an email signature.

**Identification**: Name of Employee, Personal Pronouns, Title, Department, Business Address, Phone(s), fax (if applicable)

**Fonts and colors:** 12-point size is recommended - The primary colors and fonts of the City should be used in all texts in the signature. This should be aligned with the Chicago Design System which details fonts at https://design.chicago.gov/typography/ and colors at https://design.chicago.gov/basics/ .

**Images and Logos:** Use of the flag blue banner, red star, and Chicago is recommended as a logo/image. This should be aligned with the Chicago Design System which details logos at https://design.chicago.gov/public-mark .

**Avoid complexity:** Keep the number of lines to a minimum.

**Web Addresses:** Inclusion of the City's web address is recommended. An additional address specific to the department and/or program may be included.

**Social Media Links:** Include only when they promote a relevant Department/Program. No inclusion of personal social media links.

**Slogans, Taglines, and Program Information: Programs** and departments may have slogans, taglines, or a brief description of program information that promote their activities. Such should be cleared up with the responsible department or program personnel.

**Personal Quotes/Slogans:** Use of personal quotes, slogans, or similar additions in City email signatures are prohibited.

## III. Exceptions

Any exception to the policy must be submitted through a "Policy Exception form" for review and approval by the Information Security Office in advance.

## IV. Revision History

| Date | Version | Description | Author |
|---|---|---|---|
| 08/07/2012 | 5.2 | Last update of prior "Information Security Policy document. All future versions are in the "New" format." | DoIT |
| 01/15/2013 | 0.0 | Initial Draft of new format | CISO |
| O7/26/2013 | 0.1 | Approved as Release Candidate v1 | CISO |
| 12/30/2013 | 0.2 | Approved as Release Candidate v2 | CISO |
| 03/20/2013 | 0.3 | Approved as Release Candidate v3 | CISO |
| 06/19/2014 | 0.4 | Approved as Release Candidate v4 | CISO |
| 10/20/2014 | 0.5 | Released for Final Review | CISO |
| 04/07/2022 | 2.0 | Revised to include CJIS and AWWA frameworks; document layout reformatted. Technical requirements removed from policy statements. takes into consideration the NIST 800-53 Rev5. | GRC Unit |
| 05/07/2024 | 2.1 | Added Section 15.4 Email Communications and its subsections. Changed Policy Owner to Department of Technology and Innovation following department changes. Editorial changes. | GRC Unit |