RESOLUTION NO. R-66-16

A RESOLUTION ADOPTING AN INFORMATION SECURITY POLICY FOR THE CITY OF WHEATON

WHEREAS, the City of Wheaton, in its ordinary course of business, receives, maintains and uses information from Federal agency information technology systems, such as the Federal Criminal Justice System; and

WHEREAS, the information provided to the City through the Federal systems, contains "Protected Data" as is further defined herein; and

WHEREAS, Federal agencies assembling, maintaining and disseminating Protected Data are required by Federal regulations and standards, recommended by the National Institute of Standards and Technology, to adopt an information security policy (sometimes hereinafter "ISP") establishing a cyber security framework pertaining to the management of Protected Data; and

WHEREAS, the National Institute of Standards and Technologies (hereinafter NIST) has established a recommended cyber security framework for improving critical infrastructure cyber security for information technology systems receiving, maintaining and using Protected Data which recognizes that its framework is a basis for the development of but not a verbatim template to be utilized by entities establishing individualized ISPs; and

WHEREAS, as a downstream user of Protected Data provided by Federal Agencies, the City is also required to have an ISP program; and

WHEREAS, the City has applied the NIST recommendations to its ISP policy; and

WHEREAS, Illinois statute (Personal Information Protection Act, 815 ILCS 530/1 and as amended by HB 1260, effective January 1, 2017) also requires the units of local government to establish cyber security frameworks to manage personal identifiers; and

WHEREAS, information security programs can promote a cyber security framework consistent with the statute, regulations and recommendations described above; and

WHEREAS, in addition cyber security best practices support the concept that local government should undertake efforts to properly manage Protected Data.

NOW, THEREFORE, BE IT RESOLVED by the Mayor and the City Council of the City of Wheaton, DuPage County, Illinois, pursuant to its home rule authority as follows:

1. The "Information Security Policy" attached hereto and incorporated herein as Exhibit 1 is hereby approved and adopted as the ISP of the City of Wheaton.

2. The Information Security Policy may be amended from time to time by the City Manager, upon concurrence of the City's Director of Information Technologies and the City's Corporate Counsel without further action of the Corporate Authorities of the City, subject to the following conditions:

    a. So as to:

        (i) be consistent with evolving technologies and cyber security threats;

(ii) to remain consistent with applicable statutes and laws;

(iii) to correct detected deficiencies which may occur in the administration of the Information Security Policy; or

(iv) to enhance and strengthen the Information Security Policy.

b. All amendments shall be in writing, dated, and attached by the City Clerk to this Resolution when made.

c. In the instance of an amendment, the City Manager shall send a memorandum to each member of the Corporate Authority of the City notifying them of the amendment, which any member of the Corporate Authority may request be placed on a City Council Agenda for discussion and possible further action.

d. The amendment will remain in effect unless otherwise rejected, or further amended by the Corporate Authorities of the City.

3. The City Council further directs the City Manager and Director of Information Technology to implement and revise as deemed necessary the Information Security Program attached hereto and incorporated herein as Exhibit 2 in furtherance of the City's cyber security efforts.

4. Where more than one policy identified in the Information Security Program (Exhibit 2) may be applicable to a situation, the terms of the stricter policy shall apply.

5. This Information Security Policy shall become effective immediately upon its adoption.

ADOPTED this 5th day of December, 2016.

Mayor

ATTEST:

City Clerk

Roll Call Vote:

Ayes: Councilman Rutledge
Mayor Gresk
Councilman Saline
Councilman Scalzo
Councilman Suess
Councilwoman Fitch
Councilman Prendiville

Nays: None
Absent: None

Motion Carried Unanimously

Information Security Policy

Purpose

The City of Wheaton ("the City" or "Wheaton") has adopted this policy to provide protection of confidential and proprietary information that is protected by federal and state statutes, while committing to compliance with the Illinois' Freedom of Information Act requirements.

Towards this end, the City has developed policies, standards, and procedures addressing administrative, technical, and physical safeguards for personal identity, financial, criminal, and health data. Collectively, these policies, standards, and procedures are referred to as the Information Security Program, and the data is referred to as Protected Data. The Information Security Program is designed to:

- Protect the integrity, availability, and confidentiality of Protected Data; and
- Protect against any anticipated threats or hazards to the security, integrity and confidentiality of Protected Data; and,
- Protect against unauthorized access to or use of Protected Data that could result in the commission of a crime, substantial harm of any kind to the City, and inconvenience to any person(s).

Scope

This policy applies to Users with access to Internal Data.

Policy Statement

The City of Wheaton is strongly committed to the protection of all Protected Data. This policy is intended to comply with regulatory and legal requirements applying a multi-disciplinary approach to information security following a framework established by the *IT Audit and Control Association* (ISACA) and *National Institute of Standards and Technology* (NIST).

- Access to Internal Data is granted based upon a Need-To-Know basis or pursuant to law or regulation such as the Freedom of Information Act; and
- Every User is responsible for the security of any Internal Data for which that person has access; and
- Controls, identified and authorized by the City of Wheaton Director of Information Technology, shall be implemented to protect information based on the risk associated with the type of information maintained; and

- The United States Department of Justice – Federal Bureau of Investigation's *CJIS Information Security Policy* is hereby incorporated into the City's Information Security Policy for the purposes of access to criminal justice information (CJI). This policy is available for review at the link described below.

Laws and standards that protect privacy of information collected and which the City must comply with include, but are not limited to:

- **Criminal Justice Information System (CJIS) Security Policy** established by the U.S. Department of Justice, Federal Bureau of Investigation (FBI) requires the protection of certain criminal information; and
- **Payment Card Industry** (PCI) requires the protection of certain credit card information; and
- **Health Information Technology for Economic and Clinical Health** (HITECH) / **Health Insurance Portability and Accountability Act (HIPAA)** requires protection of medical information; and
- **Gramm–Leach–Bliley Act** (GLBA) requires protection of specific banking information (Financial Services Modernization Act of 1999, 15 U.S.C. § 6801 et seq., 16 CFR § 313.1 et seq. (privacy)16 CFR §314.1 et seq.); and
- **Illinois Identity Protection Act** (IPA), requires the protection of social security numbers (5 ILCS 179); and
- **Illinois Personal Information Protection Act** (PIPA), governs the way "personal information" is to be handled and what to do in case of a breach of a data system (815 ILCS 530).

Laws governing public record disclosure which the City must comply with include:

- **Illinois Freedom of Information Act** (5 ILCS 140); and
- **Illinois Personnel Records Review Act** (820 ILCS 40/).

Related Documents and Links

Criminal Justice Information Services (CJIS) Security Policy (https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center)

Roles & Responsibilities

All Users shall protect information that is in their custody as defined by this policy and applicable laws governing data.

Chief Information Security Officer (CISO): The City has contracted for CISO services. The contracted CISO, hereafter referred to as the "Virtual CISO" or "vCISO" reports to the City Manager and coordinates the delivery of services through the City's Director of Information Technology.

CJIS required roles are documented in the "Police Department Training Bulletin: CJIS, LEADS, NCIC and CRIMINAL HISTORY INFORMATION (CHRI)".

Management and Control of Risks

The City acknowledges that the following types of Information Security risk must be managed: legal, regulatory, financial, operational, and reputational. The City is conservative and maintains a low tolerance for risk.

Risk Assessment

Upon significant organizational or technical changes, and no less than once every five years, the City shall review its existing security controls to identify weaknesses and assess the risk of internal or external exploitation. The potential impacts considered will include: unauthorized disclosure, misuse, alteration, and destruction of information or information systems, and shall be weighted by the likelihood of exploitation, the sensitivity of the information, and legal and regulatory requirements.

The City shall employ a risk assessment framework that combines effective and actionable elements from the information security industry's trusted frameworks, e.g., NIST, and compliance standards.

Risk Treatment

Recommendations shall be made to mitigate each identified risk. Recommendations may be derived from industry standards, e.g., NIST and ISO, consultants, or internal experts. Recommendations may include avoiding, modifying, sharing, or retaining the risk.

- Risk Avoidance – preventing a change that would create a new risk or that would increase an existing risk to an unacceptable level

- Risk Modification – reducing the risk to an acceptable level. Risk Modification may be accomplished through the implementation of procedural, logical, or physical controls
- Risk Sharing – spreading the risk to third parties, such as hosting service providers or insurance providers
- Risk Retention – accepting the risk

Actual treatment of each risk shall be determined by City management based upon the severity of the risk and the costs and complexities of implementing the recommendations.

Risk Monitoring

The City shall perform quarterly internal and external vulnerability scans. Intrusion detection and prevention controls shall be implemented on the City's sensitive networks and hosts. Logs from sensitive networks and hosts shall be collected and reviewed every business day. The City shall maintain an information security incident response plan.

Training

The City will provide ongoing training to all Users to ensure knowledge about, and compliance with, the Information Security Program. A copy of the Information Security Policy will be provided to all Users and require written documentation that they have read and understand its requirements. All Users shall understand and comply with supporting policies, standards, and procedures. New Users shall receive and review the Information Security Policy and relevant supporting policies, standards, and procedures upon initial employment.

At a minimum, training will occur on a bi-annual basis and be facilitated by the Director of Information Technology or their designee.

Review of Key Controls

Key controls, systems, and procedures of the Information Security Program will be reviewed periodically. These reviews may be outsourced to an independent third-party. The nature and frequency of the reviews will be determined by the risk assessment.

Service Provider Oversight

The City will exercise due diligence in selecting and managing service providers.

Reporting

The vCISO shall provide verbal and written status reports to the Director of Information Technology as deemed appropriate by the vCISO or at the request of the Director of Information Technology. The vCISO shall provide Executive Summary reports directly to the City Manager following the completion of major information security or regulatory compliance projects. The content and format of the reports shall be evaluated during meetings with City management. Reports shall be developed and provided to the City Council as requested.

Program Review & Revision

The vCISO, or their designee, shall periodically review the effectiveness of the Information Security Program considering changes in: technology, laws or regulations, sensitivity of information, internal or external threats to information or information systems, the City's business arrangements and alliances, the City's organization, the City's programs and services, outsourcing arrangements, and information systems. The vCISO shall report the results of these reviews in a timely manner to enable the City to adopt appropriate responses.

CITY OF WHEATON
INFORMATION SECURITY POLICY AND PROGRAM
INDEX AND GLOSSARY

I. GENERAL

1. Purpose. The policies contained in this chapter are legally mandated and provide a risk, compliance, and security posture for the City of Wheaton in addressing the City's use of information technologies. The Program and its attendant Standards, although not legally mandated by Federal or State law are part of the City's overall IT security strategy and in conjunction with the IT Security Policies shall be adhered to by all Users of the City's Information Technology systems. The only difference between the Policies and Program Standards adopted by City resolution is that the Security Policies are mandated by Federal or State law and City resolution, and the Program Standards are mandated only by City resolution. Both the Policies and Program Standards accommodate the City's efforts to be able to provide for independent review, audit and assessment reports, coordination of security breaches and incident investigations, and establish strategic guidance for additional technology services and projects. Each policy and standard, although generally related, is also independent, and each and all shall be followed by all Users of the City's information technology systems.

2. Compliance. It is essential that all Users of the City's information technology systems fully understand each of the policies and standards, and all parts thereof and implement them in their use of the City's information technology systems. If you do not fully understand any policy or standard, or any aspect thereof, you must consult with the Director of Information Technology or the Director of Human Resources promptly. Every User shall comply with the Security Policies and the Security Program Standards referenced herein.

3. Amendment. These Security Policies and Security Program Standards may be amended or revised from time-to-time as the need arises. Users will be provided with copies of all amendments and revisions. Within 24 hours of receipt, Users shall become responsible for knowing and implementing any and all amendments.

4. Violations. Any User who violates the requirements defined in this Policy and Program, regardless of knowledge or intent, may be subject to disciplinary action, up to and including termination of employment. Users who discover a violation of this policy shall promptly notify the City's Director of Information Technology and/or the City's Director of Human Resources.

II. CITY ADOPTED SECURITY POLICIES INDEX

1. Information Security Policy
2. Identity Protection Policy adopted by Resolution R-33-11.
3. Identity Theft Prevention Program adopted by Resolution R-26-09.

III. CITY ADOPTED SECURITY PROGRAM STANDARDS INDEX

1. Data Classification Standard
2. Acceptable Use Standard
3. Passphrase Standard
4. Anti-Malware Standard
5. Media Handling Standard
6. Physical Security Standard
7. Mobile Device Standard
8. Social Media Standard
9. Reproduction of Public Records as Electronic Records Standard
10. PCI CDE Administrator Standard (Cashier's)
11. PCI User Standard (Cashier's)
12. Business Continuity Planning Standard (Department Heads)
13. Change Management Standard (IT)
14. Incident Response Standard (IT)
15. Log Management Standard (IT)
16. Password Reset Standard (IT)
17. Patch Management Standard (IT)
18. System Recovery Standard (IT)
19. Server Configuration Standard (IT)
20. Router Configuration Standard (IT)
21. Firewall Configuration Standard (IT)

V. GLOSSARY OF TERMS AND DEFINITIONS

When any of the following terms appear in any Security Policy or Security Program Standard, they shall have the meanings set forth in this Glossary of Terms, unless the context or separate definition clearly indicates otherwise.

Authorized Users – Users with a defined business need who have been granted access rights to Secure Areas, systems, or data.

Card Holder Data (CHD) – At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.

Card Holder Data Environment (CDE) -- The people, processes and technology that store, process, or transmit Card Holder Data (CHD).

Criminal Justice Agency (CJA) –Any agency that has access to criminal justice information (CJI) as defined by the FBI CJIS Information Security Policy. The Wheaton Police department is a CJA.

Criminal Justice Information (CJI) – Refers to all the data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions.

Criminal Justice Information Services (CJIS) –The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Device – Any device capable of displaying, storing, sending, or receiving data. These devices include, but are not limited to: desktop computers, notebook/laptop computers, removable drives (e.g. USB "thumb" drives), external portable disk drives, netbooks, tablets, smart-phones, personal digital assistants, printers, scanners, routers, switches, wireless access points, and other computer peripherals.

Federal Bureau of Investigation (FBI)

Gramm Leach Bliley Act (GLBA) – In summary provides that Financial institutions must protect nonpublic information from foreseeable threats and must have a policy in place relating to the diclosure of such information.

Health Data – An individual's health insurance or medical history information, including: health insurance policy number, subscriber identification number, or any unique identifier used by a health insurer to identify the individual; any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional, including such information provided to a website or mobile application. (PIPA 815 ILCS 530/1)

Health Information Technology for Economic and Clinical Health (HITECH) – Requires entities covered by HIPAA to report data breaches. Enforces HIPAA violation fines (Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.)

Health Insurance Portability and Accountability Act (HIPAA) –Defines policies, procedures and guidelines for maintaining the privacy and security of individually identifiable health information (Pub. L. No. 104-191, 110 Stat. 1936 (1996) Codified at 42 U.S.C. § 300gg and 29 U.S.C § 1181 et seq. and 42 USC 1320d et seq.)

Internal Data – All data that is protected by access control technology implemented by the City, e.g., a City authorized username and password, including all Protected Data.

Jailbreaking – see Rooting.

Malware – an unauthorized program that damages, disables, or compromises the security of a computer system. The symptoms of malware include slower response times, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of a computer system.

Mobile Device – Any Device used to access, process, or store City data, either directly or via the Internet. Mobile devices include laptop and tablet computers, smart phones, personal storage devices (such as USB flash drives, CDs, DVDS, cameras) and other simlar devices.

Need-To-Know – A determination made by a possessor of Protected Data that a prospective recipient has a requirement for access to, knowledge of, or possession of that Protected Data in order to perform their official duties.

National Institute of Standards and Technology (NIST): Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, The Cybersecurity Enhancement Act of 2014 and Executive Order (EO) 13636 ordered NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf)

Primary Account Number (PAN) – also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

Password – A sequence of letters, numbers, and special characters. For example: H9Z>ss.Z{c8S.

Passphrase – A longer grouping of words used to authenticate a user to a computer system. For example: bovine diet dodger does outrun enjoy

Payment Card Industry Data Security Standard (PCI DSS) – A set of requirements designed to ensure that ALL organizations in the United States that process, store or transmit credit card information maintain a secure environment. These standards were established in 2006 to manage the ongoing evolution of the Payment Card Industry (PCI) security standards with focus on improving payment account security throughout the transaction process.

Personnally Identifiable Information (PII) – Information which can be used to distinguish or trace an indivdual's identity, such as name, social security number, or biometric records, alone or

when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. (CJIS Security Policy v. 5.4 Section 4.3)

Personal Information – (1) An individual's first name or first initial and last name in combination with any one or more of the following: social security number; state driver's license number; State identification card number; account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; Health Data; or unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data.
(2) User name or email address, in combination with a password or security question and answer that would permit access to an online account. (PIPA 815 ILCS 530/1)

Protected Data – A term used to describe data that is protected from disclosure under any law or regulation, including but not limited to PII [personally identifiable information] and data regulated by GLBA, HITECH/HIPAA, PCI, and /or CJIS, plus other information deemed sensitive by the City.

Protected Health Information (PHI) – see Health Data.

Rooting – the process of allowing users of smartphones, tablets and other devices running the Android mobile operating system to attain privileged control (known as root access) over various Android subsystems

Secure Area – A work area or room where Protected Data is processed or stored.

Service Provider – A service provider is defined as any person or entity that maintains or processes Wheaton Internal Data or is otherwise granted access to information systems through the services it provides to the City.

User – All City full-time and part-time employees, interns, volunteers, contractors, elected officials, and the public who are authorized and granted access to use City devices, software, networks, or data.

Vendor / Contractor – A third-party that provides services to the City.

Virtual Chief Information Security Officer (vCISO) – An expert, independent and unbiased contractor who monitors and provides a risk, compliance, and security posture for the City of Wheaton; independent review of audit and assessment reports; coordination of security breaches and incident investigations; and, strategic guidance for additional information security services and projects.