Policy Statement

SUBJECT: City of Detroit Data Security Policy

Table of Contents

I. Overview

A. Purpose

The purpose of this Data Security Policy ("Policy") is to provide an environment within the municipal government of the City of Detroit ("City") that addresses the data and information security goals of:

- **Confidentiality**: Protecting sensitive information from unauthorized disclosure or intelligible interception.
- **Integrity**: Safeguarding the accuracy, completeness, and timeliness of information, IT systems and computer software (including the ability to audit).
- **Availability**: Ensuring that information and vital services are accessible to City of Detroit employees and affiliates when required.

This Policy is the governing policy in a series of City policies whose purpose is to protect City data and informational assets. All references to data and information herein refer to City data and information. The Policy provides high-level direction to all City officials, appointees, employees, agents, authorities, board, contractors, subcontractors, suppliers, and any other person or entity that has access to City data and information. Questions regarding this Policy may be directed to the City's Director of the Information Technology Services Department.

The Policy will also assist in assuring that the City complies with applicable laws and regulations, as amended from time to time, related to data and information covered by this Policy. Such laws include, but are not limited to:

Subject Matter Covered	Law
Data and Information	Freedom of Information Act*
All	Privacy Act
All	Payment Card Industry
All	Red Flag
Income Tax	445 Trade and Commerce – Social Security Number Privacy Act
Income Tax	445 Trade and Commerce – Identity Theft Protection Act
Income Tax	Privacy Act
Income Tax	Publication 1075 – Tax Information Security Guidelines for Federal, State and Local Agencies
Human Resources	Health Insurance Portability and Accountability Act (HIPAA)
Human Resources	Health information Technology for Economic and Clinical Health Act (HITECH)
Human Resources	Fair Credit and Reporting Act
Human Resources	The Civil rights Act of 1964
Human Resources	The Pregnancy Discrimination Law
Human Resources	The American with Disability Act
Human Resources	The Age Discrimination Act
Human Resources	The Equal Pay Act pf 1963
Human Resources	The Employment Retirement Income Security Act
Human Resources	The Family Medical Leave Act

Subject Matter Covered	Law
Human Resources	The Fair Credit Reporting Act
Human Resources	The Fair Labor Standards Act
Human Resources	The Occupational Safety and Health Act
Human Resources	The Whistleblowers Protection Act
Human Resources	The National Labor Relations Act
Human Resources	The Immigration and Reform Control Act
Law Enforcement	Criminal Justice Information System (CJIS)
Law Enforcement	Law Enforcement Information Network (LEIN)
Finance	State of Michigan directives or statutes
Meetings	Michigan Open Meetings Act

* The Michigan Freedom of Information Act may be found on the State of Michigan's official website. One of the many electronic links to the Michigan Freedom of Information Act is: http://www.legislature.mi.gov/documents/publications/openmtgsfreedom.pdf

Questions regarding any laws related to this Policy, especially the Michigan Freedom of Information Act and the Open Meetings Act, must be directed to the Corporation Counsel of the City's Law Department.

B. Scope

For the purposes of this Policy, security is defined as the ability to protect the confidentiality, integrity, and availability of all data and information, in any form, including but not limited to, electronic, digital, internet, soft copy or hard copy, which is either at rest, in motion or in use. It is important to emphasize in this information age that hardcopy, as well as other forms of data and information, must continue to be protected.

Data and information must also be protected from unauthorized use or modification and from accidental or intentional damage or destruction. Protection includes the security of facilities and off-site storage, computing devices, storage devices, telecommunications, and applications. Protection also includes the security of related services purchased from commercial, private or government entities, and Internet-related applications and connectivity.

Outsourced processing and storage facilities, such as service bureaus, vendors, partnerships, and alliances, must be monitored and reviewed to ensure compliance with this Policy or that a level of control is provided which is equivalent to this Policy. This should be accomplished through contractual, licensing, or other binding commitments with provisions to permit auditing and monitoring to ensure compliance.

This Policy applies City-wide.

II. Policy

A. General Policy Statement

The City is entrusted with data and information which it creates, collects or stores, and is responsible for their protection. Data and information must be protected from unauthorized modification, destruction, or disclosure, whether accidental or intentional, as well as to ensure their authenticity, integrity, and availability. No matter what tool is used (i.e. application, email,

pen & pencil) by the City to create, collect, or store data and information, care must be taken to appropriately protect this data and information at all times.

Data and information concerning the City's processes, procedures, and practices must also be protected. These processes, procedures, and practices may contain data or information, which may be confidential or private about the City's business processes, communications, tax payers, organizations operating within the City boundaries or assisting the City with conducting City business, computing operations and employees, among others. The processes, procedures and practices concerning distribution of any data and information must consider both the sensitivity of the data or information and any related legal exemptions for disclosing such information, before allowing their public disclosure.

B. Responsibility of Data Security Coordinator

The City's Data Security Coordinator is responsible for developing and maintaining City-wide security processes, procedures and practices in conformance with this Policy to help ensure the confidentiality, integrity and availability of the data and information and to help prevent the unauthorized disclosure of confidential or privileged data and information. These processes, procedures and practices must first be in writing and made public on the City's intranet and internet websites for at least seven calendar days before they become effective. In addition, they may be changed, supplemented, or cancelled by the Data Security Coordinator at any time after they become effective, but for such actions to become effective, any changes, supplements or cancellations must also be in writing and made public on the City's intranet and internet websites for at least seven days. All of these processes, procedures and practices may supplement, but may not override or be inconsistent with, professional or legally mandated obligations related to security, confidentiality or privilege required of persons in such professions including, but not limited to, law, accounting, health, and law enforcement.

C. Compliance and Enforcement

City officials, appointees, employees, agents, contractors, subcontractors, suppliers, and any other person or entity that has access to data and information are responsible for understanding and complying with this Policy and any processes, procedures, or practices made in accordance with this Policy . Non-compliant situations will be brought to the attention of the Data Security Coordinator. Depending on the severity of non-compliance, employees or other persons or entities that violate this Policy, or any processes, procedures, and practices made in accordance with this Policy, may be subject to discipline or adverse action in accordance with the Detroit City Code, City Human Resource Rules, applicable contracts, and collective bargaining agreements. Additionally, individuals who violate this policy are subject to loss of City technology and other access privileges, as well as civil and criminal prosecution.

III. Data and Information Categories to be protected

The City has established three categories into which all City data and information will be classified. The three categories are 1.) Public, 2.) Internal, and 3.) Confidential. The level of protection for data and information is specified in each category. Details concerning the purpose and scope of the classifications into categories, as well as additional details concerning the information categories, responsibilities, access, storage, labeling, disposal and distribution for each category, can be found in the City's Information Classification Policy.

Note that Privacy is an important issue with respect to data and information classified into any of the above three categories. For example, private, personally identifiable information ("PII") refers to information that can be used to distinguish or trace an individual's identity, or a particular aspect of a person's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not limited to any single category of data or information. Rather, it requires a case-by-case assessment of the specific risk that an individual or aspect of an individual can be identified as a result of disclosure or release of information. In performing this assessment, it is important to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual, or a particular aspect of an individual. In this event, data or information that is determined to be Private must be considered to be in the Confidential category, no matter what category in which it had originated.

A similar Privacy issue and analysis arises with respect to Protected Health Information (PHI) – which is individually identifiable health information that relates to a person's past/present/future physical/mental health, health care received, or payment for health care, among others.

The City will also issue a Privacy Policy that provides details about Privacy issues related to data and information. Any questions technical about Privacy should be directed to the Data Security Coordinator and any legal questions to the City's Corporation Counsel.

IV. Roles and Responsibilities

Security of data and information requires the active support and ongoing participation of all City officials, appointees, employees, agents, contractors, subcontractors, suppliers, and any other person or entity that has access to data and information. Security requires direction and support from the executive levels and also requires universal compliance. Responsibility for satisfying policy requirements is shared and extends to all personnel involved with data and information at rest, in motion or in use. Each person involved with data and information shall satisfy the requirements as they relate to the portion of data and information under their control.

The following are specific individual roles and responsibilities for all persons involved with data and information.

A. Data and Information Owners/Stewards

Departmental leadership (or equivalent) is the data and information owners and stewards. They are responsible and accountable for the ultimate security of data and information, at all stages, under the control of their department. Departmental leadership is also responsible for the implementation of the enterprise security policy in their departments. Departmental leadership will appoint data and information custodians in their own departments who will have access to data and information on a "need to know" basis and the responsibility of data and information protection. Departmental leadership will sponsor awareness and training programs along with furnishing necessary staffing and material resources to ensure compliance with both City-wide and departmental-wide security.

B. Data and Information Custodians

Data and Information Custodians are designated by the Owner/Stewarts of certain data or information, to maintain the designated security safeguards for the data and information owned by that department. These Custodians approve or authorize access to data and information under

their control and responsibility, determine the value or importance of the data and information, and ensure compliance with applicable controls through regular review of data and information classification and authorized access. These Custodians also assist data and information owners in assessing the risks to the confidentiality, integrity, and availability of applicable data and information.

C. Data and Information Users

Each data and information User shall, within their capabilities, protect data and information under their control against occurrences of compromise, including, but not limited to, sabotage, tampering, denial of service, fraud, misuse, and, in addition, to disclosure or release of information to unauthorized persons. Security provided by Users includes, but is not limited to, protecting passwords and other account information, following appropriate policies, processes, and procedures; and, notifying appropriate authorities when incidents occur.

V. Exceptions:

The City Information Technology Services Director and City Corporation Counsel must approve any exceptions to this policy.

VI. Approval Block

Data Security Policy	
Approval Date: 7/1/2013	**Review: Bi-Annual**
Effective Date: 7/1/2013	**Last Review = 10/2/2015**