Data Governance Plan

Contents

Purpose

Data Governance is the overall management of the confidentiality, availability, and integrity of data including a defined set of procedures and a plan to execute those procedures.

The primary purposes of this policy are:

- To establish the governance structure, including responsibility and authority
- To establish and define City data
- To define and communicate City data architecture
    - Data Standards
    - Data Classifications
    - Data Quality
    - Data Security
    - Data Privacy
- To monitor and enforce compliance with standards
- To define the primary operational roles for execution of data governance, including identification of responsible parties

Scope

The City of Milwaukee is committed to sharing data in a structured format to improve access to information and enhance coordination and efficiency among departments, partner organizations and citizens.

This policy establishes a framework for the management of data as an asset across the City and applies to all information resources created and owned by the city and its departments. Elected officials, employees, consultants, and vendors working on behalf of the City of Milwaukee are responsible for adhering to this policy.

Data Governance Roles and Responsibilities

Chief Information Officer

The Chief Information Officer or designee under the guidance of the City Information Management Committee (CIMC) shall ensure the effective implementation of Information Technology Policies, Standards, and Procedures within the City of Milwaukee.

- Manage, protect, and ensure the integrity and usefulness of City data.
- Identify the sensitivity and criticality of the data. Ensure that appropriate processes are in place to keep the data secure, maximize data accuracy, and ensure that responsible staff are trained to maintain data quality.
- Support planning and governance to meet the data needs of the City.
- Work closely with the Department Heads for Computing and Information Services and other members of administration to ensure that the appropriate resources (staff, technical infrastructure, etc.) are dedicated to prioritizing data needs and setting/enforcing policies related to data management and use.
- Implement City policies and ensure compliance with federal laws related to data governance.

- Serve as escalation point for issues related to data governance.
- Work with departments to designate data stewards.

Data Steward

A data steward is a staff member with oversight responsibility for a subset of the City's data. The steward is typically a functional end user within a department who is deemed an expert regarding data managed by that operational area.

Major responsibilities:

- Implement data standards.
- Ensure that staff who maintain data are trained to follow standards.
- Monitor data quality.
- Work with technical and operational staff to create a process for identifying data entry errors and correcting the data to match City standards.
- Report to the CIO any issues that may require larger action on behalf of the City's data governance structure.
- Handle inquiries about data.
- Receive and respond to any inquiries related to data that originates from the area they oversee, e.g., questions regarding access, standardization, organization, definition, and usage, etc.

Data Custodian

A data custodian is a system administrator or other technical professional who is responsible for some aspect of the management and operation of any of the systems that serve as sources of City Data.

Major responsibilities:

- Provide a secure infrastructure in support of the data. This includes, but is not limited to, physical security, backup and recovery processes, and secure transmission of the data.
- Implement data access policies.
- Grant access privileges to authorized system users, documenting those with access and controlling level of access to ensure that individuals have access only to that information for which they have been authorized and that access is removed in a timely fashion when no longer needed.
- Ensure system availability and adequate response time.
- Install, configure, patch, and upgrade hardware and software used for data management, ensuring that system availability and response time are maintained in accordance with City policies and/or service level agreements.
- Participate in setting data governance priorities.
- Provide details on technical, systems, and staffing requirements related to data governance initiatives.

Data Users

A Data User is different from an End User. A Data User is an individual who has been granted access to City data as part of assigned duties or in fulfillment of assigned roles.

Major responsibilities:

- Ensure that data is used only for the approved purposes to avoid the misinterpretation of data.
- Responsible for preventing the disclosure of confidential and or sensitive information such as PII.

Data Governance Committee

This committee meets quarterly to set strategic priorities for data management and provides stewardship of the guiding principles of data governance in their areas. The committee reviews proposed data governance roles across The City of Milwaukee. This group promotes the importance of the principles of data governance in their areas of responsibility, including access, consistency, and security. When needed, the group resolves conflict and confusion around data ownership and accountability.

Data (definition)

"Data" means statistical, factual, quantitative, or qualitative information that is maintained or created by or on behalf of a City department. "Data" does not include information provided to a department or division by other governmental entities, nor does it include image files, such as designs, drawings, maps, photos, or scanned copies of original documents. Nothing in this policy shall be deemed to prohibit the voluntary disclosure of information not otherwise defined as "data".

Minimum Metadata Standards

The City of Milwaukee shall create and implement data standards to maximize data quality and facilitate use, access, sharing, and interoperability. Standards make it easier to create, share, and integrate data by making sure that there is a clear understanding of how data is represented and that the data you receive is in an expected format.

The table below summarizes the minimum standards:

Group	**Purpose**	**Fields**
Basic Descriptive Information	Provide the core information to describe the dataset, including the source department. Each of these fields help our users discover and distinguish between datasets.	- Dataset title - Description - Category - Department
Detailed Descriptive Information	Support informed use of the data. They allow users to assess the appropriateness of the dataset for their needs (including data coverage, size, and other details), address common questions or misconceptions, and provide a means of conveying additional detail.	- Data dictionary - Tags - Related documents
Publishing Details	Allow users to understand what to expect in terms of how often	- Last updated - Frequency of data

	the data is updated and its relative "freshness". This informs how the data can be used and helps users assess if it is appropriate for their desired use.	change - Frequency of data publishing - License and rights
Web & Technical Information	Provide web and technical details that support web or application access to the dataset. These fields are heavily used by programmers and administrative users of the data platform.	- Unique identifier - Permanent link - URL - Endpoint (for APIs) - Download URL - Format -File Type -Data Source
Internal Management	Support internal management of datasets for publishing datasets and answering data questions. These metadata fields are private.	- Access level - Public access comment - Data steward/contact name - Data steward/contact email

Data Classification

The Data Classification Standard is intended to provide standardization for identification, classification, and labeling of information assets, to facilitate the use of appropriate security, privacy, and compliance measures to protect the confidentiality, integrity, and availability of data/information and associated Information Technology (IT) Security Policy objectives.

Classification Objectives

Security Objectives	FISMA Definition [44 U.S.C., Sec. 3542]	FIPS 199 Definition
Confidentiality	"Preserve authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information..."	A loss of confidentiality is the unauthorized disclosure of information.
Integrity	Avoid "improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity..."	A loss of integrity is the unauthorized modification or destruction of information.
Availability	"Ensure timely and reliable access to and use of information..."	A loss of availability is the disruption of access to or use of information or an information system.

Risk Levels

All Data must be classified into one of three classes: Low, Medium, or High. Each is described below.

Data class	Description	Potential adverse impact
Level 1 Public	In accordance with Wisconsin public record's law, data that may be released to the public and requires no additional levels of protection from unauthorized disclosure.	Low
Level 2 Restricted	Disclosure could cause limited harm to individuals and/or the City of Milwaukee with some risk of civil liability. Either subject to contractual agreements or regulatory compliance, or is individually identifiable, confidential, and/or proprietary. Types of Data include: • Building plans and associated information • Employee records (multiple types) • Emergency planning information • IT configuration information • IT security plans • Public safety and security information • Telecommunications systems information	Medium
Level 3 Confidential	Information made Confidential by State or Federal Law that has the potential to cause great harm or damage to individuals or institutions if breached or disclosed by unauthorized users. Confidential Data is subject to regulatory or compliance requirements, contains PII, PHI/ePHI or state/federal tax information and/or contractual language requiring a confidential or high classification level for information/data. • Protected Health Information [Health Insurance Portability and Accountability Act (HIPAA) • Payment Card Industry Data Security Standard (PCI DSS) v3.2.1] • Personally Identifiable Information (PII) (Wis. Stat. § 134.98) • Taxpayer Information - Internal Revenue Service Publication 1075 (IRS Pub 1075) • Other records protected by Wisconsin open records (Wis. Stat. § 19.36)	High

Data Security

The classes determine the level of security that must be placed around the data. The data steward is responsible for classifying information correctly.

If data includes multiple classifications, the classification must default to the highest level. For example, a system that stores, processes, transfers, or communicates both Low Risk and Medium Risk data would be classified as Medium Risk.

Information security controls shall be implemented commensurate with information value, sensitivity, and risk. Information in each classification level will require varying security controls appropriate to the degree to which the loss or corruption of the data would be harmful to individuals, impair business functions, result in financial loss, or violate law, policy, or City contracts.

Public Security Requirements

Publicly available information may be subject to appropriate review to mitigate potential risks of inappropriate disclosure. Public information assets have low impact levels. Information assets at this level do not require encryption of data at rest, in use, or in transit.

Restricted Security Requirements

Restricted information assets have a medium impact level. Authorization is required for access to this information.

- Restricted Information shall be limited in distribution to those employees, contractors, and vendors with an established business need-to-know.
- When at all possible, this information should be accessed from its original source and copies, or printed versions of the information should be kept to a minimum.
- An access review shall be performed annually. Evidence of an annual access review shall be made available to the Information Security Officer on request.
- Restricted information shall be secured (e.g., encrypted) when traversing an unsecured network or when traveling outside the City network.
- Printed copies of restricted information should be closely guarded to prevent unauthorized disclosure or theft.

Confidential Security Requirements

Confidential information assets have a high impact level. Information assets at this level must limit access to authorized individuals only and must employ encryption of data at rest, in use and in transit.

- Confidential information shall be limited in distribution to those with an established business need-to-know.
- When at all possible, confidential information should be accessed from its original source and copies or printed versions of the information should be kept to a minimum.
- An access review shall be performed annually. Evidence of an annual access review shall be made available to the Information Security Officer on request.

- Confidential information shall always be secured (e.g., encrypted) when traversing an unsecured network or when traveling outside the City network.
- Printed copies of confidential information should be closely guarded to prevent unauthorized disclosure or theft.
- Due care is required when in verbal contact with another party regarding this information.
- Employees should receive annual training on their responsibilities regarding appropriate use and steps they can take to protect confidential information.

Data Sharing

All users must observe requirements for transferring or communicating information based on its sensitivity. Data stewards, or their assigned representative, may designate additional controls to further restrict access to, or to further protect information.

Access to Medium and High-Risk data may be granted only after a business need has been demonstrated and approved by the Data Steward.

The following table shows authorized methods for the transfer and communication of data.

Method of Transfer or Communication	**Classification**		
	Low Risk	**Medium Risk (Restricted)**	**High Risk (Highly Restricted)**
Copying	No Restrictions	Permissions of Data Custodian Advised	Permissions of Data Custodian Advised
Storage	Encryption Optional	Encryption or physical access control.	Encryption required.
Fax	No Restrictions	Encryption Required	Encryption Required.
Electronic Mail	Encryption Optional	Encryption Required	Encryption Required
Audit Log	No Restrictions	Data Custodian is required to include audit trails for all access and destruction of information.	Data Custodian is required to include audit trails for all access and destruction of information.
Sharing Data	No Restriction	Data Custodian or Designee Only	Data Custodian or Designee Only
Access Rights	No Restrictions	Must be an authorized user and have a job-related need.	Must be an authorized user and have a job-related need.

Data Archive/Data Retention

To the extent that data and datasets are determined to be public records, as defined in Wis Stat. §19.32(2), authorities must comply with all retention and disposition requirements. For purposes of identification and retention calculation, a record in this context is defined as **a collection of related data elements treated as a conceptual unit, independent of how or where the information is stored.** This

may take the form of a data record (i.e., a row in a database table) or of a large data set, if the full context of individual data records requires multiple data records together.

Data stewards, as defined elsewhere in this document, are responsible for the disclosure, maintenance, retention, and disposition of records maintained within information systems under their purview. Data stewards are to maintain the authoritative copy of both data records and any derivative records. Version control should be maintained for major additions or deletions. Non-authoritative copies of records should be destroyed once copies are no longer administratively useful.

Wisconsin Administrative Code Ch. ADM 12 prescribes six essential qualities for maintaining information systems that house electronic public records, including data and datasets. Different information systems will require different ways of fulfilling these criteria; data stewards should consult with City Records and Data Custodians to determine which apply to their system. A summary is below (the three technical qualities have been combined for clarity):

Quality	Description	How to fulfill
Accessible	information arranged, identified, indexed, or maintained in a manner that permits the custodian of the public record to locate and retrieve the information in a readable format within a reasonable time.	Follow guidelines in the "Metadata Models" and "Data Quality" sections of this document
Accurate	all information produced exhibits a high degree of legibility and readability and correctly reflects the original record	Follow guidelines in the "Data Quality" section of this document
Authentic	the retained electronic record correctly reflects the creator's input and can be substantiated	Maintain audit trails/version control; be aware of specific authenticity controls in your application
Legible, Readable, Reliable	Data retrieved reflects the data that was originally entered, and can be used as uncorrupted information for documenting a transaction or carrying out City business	Use universal data encoding and file formatting standards; present data in a high-quality access platform; maintain database integrity through migrations as needed

Data and datasets that maintain administrative or historical value, but which are no longer actively updated, should be removed from the Line of Business system, and stored on an archival-quality digital preservation and access platform. Long-term data should be stored on-premises if possible. Data intended for long-term preservation should be preserved with any associated data dictionaries or other documentation and migrated to an open data format if possible.

Data Disposal

The following table summarizes disposal methods for each data risk classification.

Disposal	Classification		
	Low Risk	**Medium Risk (Restricted)**	**High Risk (Highly Restricted)**
	No Restrictions	Shredding or Secure Disposal	Shredding or Secure Disposal

Before disposal or re-use, media must be sanitized in accordance with the National Institute for Standards and Technology (NIST) Special Publication 800-88 revision 1, *Guidelines for Media Sanitization.* These methods ensure that data is not unintentionally disclosed to unauthorized users. The baseline for sanitizing media is shown in the table below.

Sanitization	Classification		
	Low Risk	**Medium Risk (Restricted)**	**High Risk (Highly Restricted)**
	Not Required	Mandatory	Mandatory

Data Quality

The ability to create, collect, store, maintain, transfer, process, and present data to support business processes in a timely and cost-effective manner requires both an understanding of the characteristics of the data that determine its quality, and an ability to measure, manage and report on data quality.

Data quality dimensions include accuracy, completeness, consistency, timeliness, validity, and uniqueness.

Accuracy

Data quality is measured by the degree of accuracy upheld, accurate data needs both trueness and precision. Accuracy is when a measured value matches the actual (true) value and it contains no mistakes, such as outdated information, redundancies, and typos.

Completeness

The degree to which all the necessary components and parts of a dataset are reported. Completeness is designed to measure if all the necessary data is found in a precise dataset. This dimension also reflects the ability to determine what data is missing, and whether omissions are acceptable (for example, optional data). Departments must determine and understand whether a data asset contains unacceptable gaps, as these may place limitations on the data leading to an increased reliance on assumptions and estimations or preclude the asset for use altogether. It is also useful to note the level of completeness, particularly if 100% is not required to meet the original purpose of the dataset. Also, if the dataset is considered complete as at a particular point in time, e.g., beginning or end of month.

Consistency

Data is collected, grouped, structured, and stored in a consistent and standardized way. This requires standard concepts, definitions, and classifications to be implemented across departments, and agreed upon as to their meanings and interpretation.

Data must also be consistent in the context of its use. For example, data may appear similar but have different meanings or uses in different departments. Duplication, or different meanings for similar data, may result in confusion or misinterpretation of data and render such data unsuitable for comparison with related assets. Also, it may be unclear if trends are due to a true effect or due to problems with inconsistent data collection.

Timeliness

Timeliness refers to how quickly data can be made available when required, and the delay between the reference period (period to which data refers, such as a financial year) and the release of information. Factors that may impact this include collection method and processing. Data must be discoverable, available, and accessible throughout all stages of the data asset lifecycle from creation to retirement, to be available for greater internal use, external use (external partners or other government departments) and the public. If delays occur during the provision of data, currency and reliability may be impacted.

Uniqueness

The extent to which a data element is one of its kind or unlike any other data element. This metric assesses how unique a data entry is, and whether it is duplicated anywhere else. Uniqueness is ensured when the piece of data has only been recorded once.

Data Privacy

The City of Milwaukee has an ongoing responsibility to safeguard the identifying information of its employees and officials, and in some instances, members of the public, maintained by City agencies. With advances in technology, the increasing volume of electronic transactions involving such information calls for robust privacy protection and data security practices to guard against the unauthorized access, fraud, theft, and other misuse of such information.

In meeting such obligations and new challenges, City agencies should adhere to the following privacy protection principles ("Privacy Principles") as they strive to balance privacy protections with the importance of responsible data sharing, where permitted by law, to provide benefits, services, and care to individuals and families who need them, advance and improve coordination of multiagency initiatives that deliver health and human services, and strengthen City infrastructure, help ensure public safety, and improve economic outcomes.

City agencies should incorporate these Privacy Principles into all aspects of agency decision-making and operations where individuals' privacy interests are implicated, whether directly or indirectly.

Privacy Principle	Description
Accountability	City agencies should establish and implement agency privacy protection policies and protocols, develop strategies, and plans to periodically assess and modify such practices as privacy and security threats emerge and evolve, and guide their covered contractors and subcontractors in such efforts.
Public Trust	City agencies and their covered contractors and subcontractors should collect, use, retain, and disclose identifying information in a manner that protects individuals' privacy interests to the greatest extent reasonable under the circumstances so that all members of the public can seek and safely access needed City services and resources, trusting that the City is appropriately safeguarding their personal information.
Responsible Governance and Stewardship	In delivering necessary City services and striving to improve outcomes for its residents, City agencies and their covered contractors and subcontractors should appropriately protect the privacy and security of identifying information so that such information is used, collected, accessed, stored, and disclosed or otherwise shared only with authorized persons for lawful purposes.
Data Quality, Integrity, and Accuracy	City agencies should endeavor to maintain identifying information in a manner that protects its quality, integrity, and accuracy. Agencies should take reasonable steps to ensure that inaccurate or outdated identifying information is corrected, updated, or, where appropriate, securely disposed.
Security Safeguards	City agencies and their covered contractors and subcontractors should use appropriate safeguards in both physical and virtual places to protect

	identifying information from unauthorized access and disclosure, in accordance with applicable laws, regulations, and City