COP 1400 Data Classification Policy

Effective 2/26/2026

Scope

This policy applies to all permanent and temporary City of Tulsa employees, contractors, subcontractors, consultants, boards, committees, commissions, and vendors who are permitted to use or access City data, networks, or technology infrastructure for any reason.

City data is information generated by or for, owned by, or otherwise in the possession of the City of Tulsa related to the City's activities. City data may exist in any format (e.g., electronic, paper) and includes, but is not limited to, all administrative, academic, and research data, as well as the computing infrastructure and program code that supports the business of the City of Tulsa.

Employees are required to comply with this Policy. Failure to do so may result in disciplinary action, up to and including termination.

This Policy does not supersede or exempt the City's requirements under other applicable laws, including contractual, legal, or regulatory obligations such as the Oklahoma Open Records Act. https://oklahoma.gov/libraries/law-legislative-reference/library-laws-and-regulations/statutes-and-rules--open-record-act.html.

Purpose

The purpose of this policy is to establish a framework for classifying City of Tulsa ("City") Data based on its Disclosure Risk and Impact Risk. Data classification facilitates the protection of City Data internally and to the public when the risk of disclosure is outweighed by the City's commitment to transparency. This policy is intended to provide guidance to City personnel when deciding how to generate, collect, process, disseminate, or destroy City Data.

- The Data Classification Policy applies to all City of Tulsa data and records, as defined in this policy. The Data Classification Policy governs all permanent and temporary City of Tulsa employees, contractors, subcontractors, consultants, and vendors who are permitted to use or access City Data for any reason.

- Data Stewardship is the careful and responsible management of City Data belonging to the City as a whole, regardless of the entity or source that may have originated, created, or compiled the Data. Data Stewards provide maximum access to City Data internally and to the public, balanced by the obligation to protect the information in accordance with the policies established by the City of Tulsa and any other law or regulation. Any Data generated, collected, processed, disseminated, or disposed of by the City of Tulsa is an asset of the City, not of the particular department or subordinate organization which acts on the City's behalf. Departments developing policies, procedures, practices, and training should avoid the mindset of Data ownership and implement the practice of Data Stewardship.

1 Classification Standards

.1 New data collection programs. At the beginning of a new Data collection effort, Data shall be originally classified under this policy if any of the following conditions are met:

.11 A Record is maintained containing Data,

.12 A Record may be created from Data, or

.13 An individual with the authority to classify Data determines that unauthorized access, disclosure, or alteration of Data could reasonably result in damage to the City, and the individual can identify or describe the damage.

.2 Existing data collection programs. For Data that the City has collected prior to implementation of this Policy, Data may be classified under this policy if any of the following conditions are met:

.21 A request for disclosure of Data is received.

.22 It is determined that unauthorized access, disclosure, or alteration of Data could reasonably result in damage to the City, and the individual can identify or describe the damage.

.3 Implementation guidance for classification standards. The Data Governance Steering Committee reviews classification standards, promotes consistency, and resolves disputes. The committee works with Information Technology Security and Legal to ensure compliance with applicable regulations and policies.

.4 The default classification will be set to "Public" unless and until specifically classified otherwise.

2 Data Classification Categories

To effectively secure City data, the organization must adopt a common language to categorize the data and quantify the degree of protection required. This policy defines four (4) categories into which all City data can be divided:

.21 **Public**: The classification applied to data that does not require any level of protection from disclosure. The data contains no Internal, Sensitive, or Protected information. While it may be necessary to protect original (source) documents from unauthorized modification, Public data may be shared with a broad audience both within and outside the city or greater community, and no steps need be taken to prevent its distribution.

.22 **Internal:** The Internal classification applies to internal business, financial, or personnel data that, while not subject to specific legal or regulatory protections, requires controlled access due to its potential to compromise city operations, competitive advantage, or individual privacy if improperly disclosed. Examples of Internal data include draft budgets and policies, internal human resources communications, vendor evaluations, and grant applications in progress. Unintended exposure of this information could negatively affect negotiations, erode trust, or disrupt internal processes. Internal data is generally not shared outside the originating department or project team and should only be accessed by authorized individuals with a defined business need.

.23 **Sensitive:** This classification applies to data related to emergency management, public safety, infrastructure continuity, and PII,. This data includes, but is not limited to, network and firewall configurations, operational systems, and their backups, etc. This data, if lost or accessed improperly, could cause significant disruption to business operations, legal exposure, financial loss, or reputational damage. Sensitive data is generally not shared outside the originating department or project team and should only be accessed by authorized individuals as approved by the department Director or Director's Designee. Sensitive data shared outside the organization must be approved by the Data Governance Steering Committee and/or the Data Governance Steering Committee Chair.

.24 **Protected:** The classification applies to data that is protected against unauthorized disclosure or modification. Generally, data under this classification is specifically required by law (contractual, legal, or regulatory obligation) to be safeguarded in the most stringent manner, such as PHI and CJI data. Unintended disclosure could raise privacy, confidentiality, or security concerns or have the potential to jeopardize public health, safety, or welfare to an extent that is greater than the potential public benefit of making the information public. Additionally, Protected data will be used only when necessary for business purposes as approved by department Director or Director's Designee. Protected data shared outside the organization must be approved by the Legal Department and the Data Governance Steering Committee and/or the Data Governance Steering Committee Chair. Protected data should be safeguarded both when it is in use and when it is being stored or transported. Protected data will be used only when no alternative exists.

3 Classifying Authority

.31 The authority to classify Data may be exercised only by:

.311 The Mayor, by executive authority, or an employee to whom the Mayor has delegated authority.

.312 Directors of Departments, concerning all Data generated within their department, or an employee to whom the Director has delegated authority.

.32 Delegated Authority

a. Delegations of classification authority shall be limited to the minimum required to administer this policy. No delegated authority shall exist without training in classification as required by Implementation Guidance.

b. Delegation of the executive authority. The Mayor may delegate his or her Classifying Authority to a subordinate individual within the Office of the Mayor to act as the Mayor's representative if that individual meets the requirements of Section 3.32a of this policy.

c. Delegation of total departmental-level authority to Data Stewards within the department. Directors of departments may delegate their Classifying Authority to a Data Steward within their department to act as their representative if that individual meets the requirements of Section 3.32a of this policy.

4 Classification Review, Oversight, and Dispute Resolution

.41 Reclassification review. Classifying Authorities shall review all Data Classifications made within their authority from time to time.

.42 Uniform guidance. The Data Governance Steering Committee shall from time to time as established in Policy review all Implementing Guidance, policies, procedures, practices, instructions, or training created by any Classifying Authority under the provisions of this policy for the purpose of recommending Uniform Guidance for all Classifying Authorities to the Mayor, for the promulgation of standardized policy, procedure, practice, instruction, or training across the organization with regard to Data Classification.

.43 Oversight. The Data Governance Steering Committee shall have oversight responsibility for the implementation of this Policy.

.44 Challenges and Dispute Resolution

.441 Classifying Authorities who, in good faith, believe that the classification of Data or Records, whether original, derivative, or correlative, or Originating Authority to make such Classification is improper, may challenge the Classification to the Data Governance Steering Committee.

.442 The Data Governance Steering Committee Authorities shall establish Implementation Guidance under which authorized holders or users of Data may challenge the classification of Data they believe is improperly classified before the Information Technology Security Sub-Committee.

.443 The Data Governance Steering Committee shall ensure by policy and procedure that challengers or disputants are not subject to retribution for bringing such actions and challenges and disputes are given an opportunity for impartial review.

5 Definitions

.51 Data: Data refers to elements of information that are collected, stored, processed, or transmitted by an organization. These elements can exist in various formats (e.g., text, numbers, images, audio) and may be structured (e.g., databases), semi-structured (e.g., XML, JSON), or unstructured (e.g., emails, documents). Data may or may not have context or meaning on its own.
Example: A customer's name, a temperature reading, or a single transaction amount.

.52 Record: A record is a collection of related Data that are grouped together and treated as a single unit because they represent a complete instance of information regardless of medium or format. Records have context, structure, and are created, maintained, and retained for legal, regulatory, operational, or historical purposes for the City of Tulsa. In some cases, a record may include materials which are duplicates or require action and are needed for documentary purposes.
Example: A customer record that includes name, address, contact details, and purchase

history, or contracts, policies, reports, or meeting minutes, or any other collection of related Data.

.53 PII: Personally Identifiable Information. Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (**NIST Special Publication 800-122**)

.54 PHI: Protected Health Information. Any individually identifiable health information that is transmitted or maintained in any form or medium by a covered entity or its business associate, whether electronic, paper, or oral. **(NIST Special Publication 800-66 Revision 1)**

.55 CJI: Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. **(Criminal Justice Information Services Security Policy)**

Approvals

Shawn Flaherty, Director of Information Services Date

Michael Dellinger, Chief Information Officer Date

James Wagner, Deputy City Administrator Date