CITY OF DUBLIN
ADMINISTRATIVE ORDERS
OF THE CITY MANAGER

ADMINISTRATIVE ORDER 9.3
TO: All City of Dublin Employees
FROM: Megan O'Callaghan, City Manager Megan O'Callaghan
SUBJECT: Data Classification and Protection Policy
DATE: January 23, 2023
New Administrative Order
PROPONENT: Information Technology

1. PURPOSE

This policy provides the data classification methodology and standards for the purpose of identifying and treating ***data*** and ***information*** assets according to their levels of ***confidentiality***. The increased connectivity of computers and databases makes more data available to individuals and organizations. As a result, the potential for unauthorized disclosure, modification, or destruction of personal, financial, and other data also has increased. The classification of data and information assets provides a basis for deploying appropriate levels of security relevant to the use, handling, management, and control of data and information assets.

2. SCOPE

A. Data is an asset of vital importance to the City of Dublin. The City's policy is to take reasonable and appropriate steps to identify and protect sensitive data originated or owned by the City or entrusted to the City by others. The scope of this policy includes electronic data stored, operated, owned, or administered by City departments and supported by the Division of Information Technology.

B. City of Dublin divisions are responsible for identification and classification of data central to their mission, and for determining the method by which they will classify this data and information.

C. This document does not address data retention or disposal. Refer to A.O. 1.19 for data retention and disposal topics.

3. POLICY

A. Data classification is a process that identifies what information needs to be protected against unauthorized access, misuse, and the extent to which it needs to be secured and controlled. Each City division shall serve as a ***classification authority*** for the data and information that it collects or maintains in fulfilling its mission.

B. **Data Classification Definitions and Actions**

Class	Definition
Public	Public data poses no risk if made generally available and requires no review before release
Sensitive	Sensitive data requires a greater level of protection. This data may include information that may be a public record but requires a review for context or disclosure limitations before it is released.
Protected	Protected is the highest level of sensitivity and may be considered exempted from the Ohio Public Records Act (https://www.ohioattorneygeneral.gov/yellowbook). This data requires a review for context or disclosure limitations before it is released. In the case of Public Records Requests, see A.O. 1.18. Protected data also requires an IT review to ensure secure electronic storage and transfer processes.

4. RECOMMENDATIONS FOR CLASSIFICATION AND DATA HANDLING/MANAGEMENT

A. Assignment of a Data Steward by the Division Director

B. The Data Steward identifies the type of data managed or handled by the division and assigns the appropriate classification

C. The Data Steward notes all data that is classified as "Sensitive" or "Protected" and identifies its stored location.

(1) Sensitive data requires a review for context or disclosure limitations before it is released or shared

(2) Protected data requires a review for context or disclosure limitations and an Information Technology review to ensure electronic storage and transfer processes are followed.

(3) Protected data should ONLY be stored on Information Technology supplied secured drives. See A.O. 9.2 - Section C Item 6 or contact Information Technology Division for guidance.

(4) Protected data requires a review for context or disclosure limitations and an Information Technology review to ensure electronic storage and transfer processes are followed.

(5) PII (Personal Identifiable Information) shall always be classified as "Protected" data.

D. The Division Director communicates this policy to staff, including the classification requirements as identified in chart 3.1 and the types of data managed and handled by their teams

E. Contact the Information Technology Division if questions arise regarding electronic storage and transfer of data to third parties.

F. When looking for new hosted solutions or software, determine if "Sensitive" or "Protected" data will be stored or shared. Contact the Information Technology Division to discuss best practices for data management.

G. Report any accidental or malicious disclosure of "Protected" data to Data Owner, Division Director, and Information Technology.