General Order

Houston Police Department

ISSUE DATE:	NO.
July 7, 2021	800-01

REFERENCE: This newly created General Order supersedes all prior conflicting Circulars, Directives, and General Orders

SUBJECT: DATA GOVERNANCE

POLICY

Data is a departmental asset that must be maintained and supported through data governance principles. To support effective and innovative management relative to the operation, planning, and administration of the department, data must correctly represent the information intended through accuracy and quality, as well as integration capacities via technological systems.

This General Order establishes appropriate responsibility for the management of HPD data as a department wide asset. The goal is to improve ease of access to data and ensure the users have enough information about the attributes of the data to be able to interpret and use the elements correctly. Improving the integrity of the data results in greater accuracy, timeliness, and quality of information for decision-making. The security of data is improved by defining security and confidentiality standards that align with protection security protocols.

This General Order applies to all employees.

DEFINITIONS

Data Dictionary. A reference tool that provides a description of all the core departmental *data elements* and *data values.*

Data Element. A single data item. For example, gender is a *data element.*

Data Integrity. The qualities of reliability and accuracy of *data values* that permit the departmental utilization of the data for plans, projections, and decisions.

Data Model. A diagrammatic representation, sometimes represented in a data flow diagram, of the systems and their data relationships that are needed to accomplish the department mission.

Data Security Classification. The classification of data based on the level of sensitivity within the department, most commonly defined by legal statutes.

Data Value. The set of values each *data element* may have. For example, gender may have male, female, or other listed as a value within the *data element.*

Data Warehouse. A large centralized storage source that houses accumulated data from various sources within the department that is used to gather meaningful and actionable business insights.

Information Management System. A system that holds data used for decision-making, coordination, and analysis of information across the department. This could be a self-developed

database structure, a software system that is purchased or leased, as well as a system that interfaces with outside systems.

Technological Strategic Plan. Document that establishes a technological direction for the department, to include a technical strategic component that includes the five year goals and objectives.

1 DUTIES AND RESPONSIBILITIES

Executive Chief, Executive Assistant Chiefs, Assistant Chiefs, Chief Technology Officer, and Chief Data Officer

The Executive Chief, executive assistant chiefs, assistant chiefs, Chief Technology Officer (CTO), and Chief Data Officer (CDO) shall participate in the Executive Staff Oversight Council (ESOC), as directed by the Chief of Police, to help promote data governance development and to ensure evolving information technology advancements meet or exceed Criminal Justice Information Services (CJIS), Health Insurance Portability and Accountability Act (HIPPA), and departmental policy standards. The Executive Chief shall act as the chairman of the ESOC.

Executive Staff Oversight Council (ESOC)

The ESOC is the governing body that provides oversight for the CDO as it relates to overall strategic direction and mission critical needs as it relates to data governance. The ESOC is responsible for program leadership and oversight and setting program goals according to department strategic objectives. The ESOC shall assist the CDO in decisions related to suitable strategies to meet program objectives.

Chief Data Officer (CDO)

The CDO is responsible for the implementation of policy related to data governance and prioritization of projects to accomplish the purpose of open data, data governance (quality, quantity, and value of data), shared platforms of data analytics, and long term strategic planning for efficiency and effectiveness.

The CDO shall work with the Office of Technology Services (OTS) and the CTO to stay abreast of new software and information system purchases. The CDO is responsible for the oversight of the Data Governance Unit and its goals and objectives as defined within this policy. The CDO shall work with the ESOC to provide research, background, and understanding of data governance issues and concerns, so that goals and objectives of the department can be defined, measured, and achieved.

Chief Technology Officer (CTO)

The Office of Technology Services, headed by the department's CTO, serves as the main resource for HPD network systems operations and deliverance of data related services. The CTO shall work closely with the CDO to ensure that the Data Governance Unit (DGU) is a part of the project management team for the purchase of new, restructuring of existing, or decommissioning of older information technology systems.

Data Governance Unit (DGU)

The DGU is a work group within the Office of Planning & Data Governance that has the operational responsibility for data governance as it relates to processes and policies defined in this General Order. The DGU is responsible for maintaining the latest version of all data dictionaries related to the various information systems across the department. DGU shall maintain a standard set of principles approved by the CDO related to *data elements* and *data values* for the department to increase interoperability and integration. DGU shall maintain a *data model* for the department, so interoperability and integration can be easily navigated.

DGU shall coordinate with the Office of Technology Services and data stewards to ensure that policies outlined in the City of Houston, Administrative Procedure, 8-1, *Use of City Information and City Information Technology Resources*, are considered when dealing with data.

The DGU shall be responsible for creating a master data management plan that includes the following objectives.

a. Data Access – data discovery, indexing, and matching variables across systems.

b. Data Standardization – a standard *Data Model* that serves to join disparate information to a unified storage source such as a *data warehouse*.

c. Consolidated Data Quality – oversight of data stewards to ensure data governance principles are a focus.

Division Commanders

Division commanders and civilian equivalents are responsible for ensuring that they designate a data steward within the division who works in liaison with the DGU to eliminate data silos, define a *data dictionary* from each system within their control, and address data gaps, accuracy, and clarity.

Data Stewards

Data stewards are divisional or command representatives who primarily serve to define the business roles and needs of stakeholders as they relate to data collection, integration, control, or dissemination. Data stewards shall ensure business definitions and appropriate meta-data values for the data they control are recorded by utilizing the tools and processes that have been identified and that are supported by the DGU within the *data dictionary* process. Data stewards responsibilities are listed below.

a. Assist the division commander in identifying the specific *data elements* and *data values* needed to operate the flow of informational data within their business area and within the informational systems that fall in their control.

b. Participate in the enforcement of data quality standards by identifying and resolving data quality issues, data gaps, and *data integrity* issues pertaining to the data that they control.

c. Provide for effective and appropriate information security through data classification and partnering with OTS to ensure security protections are in place.

d. Convey new or changed business requirements within an information system to individuals who might be affected, as well as the DGU.

2 CATEGORIES OF DATA

Criminal Justice Information (CJI). For the purposes of this General Order, *criminal justice information* refers to any and all of the FBI-provided criminal justice data necessary for law enforcement agencies to perform their mission. Such data includes, but is not limited to, biometric, identity history, person, organization, property, and case/incident history data as well as *criminal history record information*.

Confidential Data. Data categorized as restricted due to a legal mandate, such as data that falls under CJIS, HIPPA, or other legal guidelines. Confidential status may also represent CJI within a crime report that is access-restricted within the Records Management System (e.g., murder incident report).

Sensitive Data. Data that is sensitive in nature and should be protected against unwarranted disclosure due to harm to the organization or individuals. May not be protected under a confidential status but should have limited access to the data.

Unrestricted Data. Data which is not confidential or sensitive and can be released to the public through approved processes.

3 PURCHASE OF NEW INFORMATION MANAGEMENT SYSTEMS

To initiate the procurement of a software system, the concerned division or command shall contact the Office of Technology Services as outlined in General Order 400-19, **Microcomputer Regulations**.

Project Managers assigned to OTS shall ensure that the DGU is included in the project management team for the procurement of any information software system that stores data. DGU shall ensure purchases include the creation or submission of a *data dictionary* for the *information management system*, analysis of the *data elements* and *data values* for designation of a particular *data security classification*, and the integrity and interoperability of the data.

The DGU is responsible for evaluating current siloes of information created at the divisional level that are not a component of an enterprise system and work to move those data variables, elements, and structures into an enterprise system that creates efficiency and effectiveness.

DGU shall ensure that the proper data user agreement forms are completed when necessary and forwarded to the OTS Project Manager to be included within the procurement process.

4 MODIFICATION, MIGRATION OR DECOMMISSION OF AN EXISTING INFORMATION MANAGEMENT SYSTEM

Data stewards and OTS shall include the DGU in projects that change *data elements* or *data values* within existing information systems. The objective is to ensure that *data elements* or

data values within an information system that is modified do not have a negative impact on the flow of information. The DGU shall research and bring issues to the project team for consideration and decisions, escalating issues to the CDO or ESOC where necessary to ensure that departmental strategies are met, and all master *data dictionary* files are updated to reflect the approved changes.

The DGU shall ensure that not only is the overall departmental *data dictionary* updated, but the *data model* is modified if the data changes affect the model.

5 CREATE AND MAINTAIN THE TECHNOLOGICAL STRATEGIC PLAN

Technical infrastructure is the responsibility of the OTS and data governance is the responsibility of the OPDG. OPDG and OTS shall provide annually the Executive Staff Oversight Council with the current status of departmental technology. Outcomes of this annual meeting will create, modify, or eliminate strategic goals related to technical systems that support the department.

OPDG and OTS will formalize the outcomes of decision points to create and maintain the HPD *Technological Strategic Plan*.

6 VENDOR PRODUCT REVIEW TEAM (VPRT)

The Vendor Product Review Team, maintained by the OPDG, is responsible for the initial review and functional analysis of any new software or technological system that outside vendors offer to the department. The unit shall establish and define a basic overview of the product being offered, evaluate the functions as they align to the Technical Strategic Plan, and provide insight into the products ability to increase effectiveness or efficiency of current processes or new processes being developed. The unit will review and complete a functional analysis of all informational software systems or technology products being presented to the department for consideration outside of the Request for Proposal process or the Request for Information process.

When the OTS is creating a Request for Proposal or Request for Information, OTS shall include the DGU in the project.

7 PUBLIC TRANSPARENCY AND OPEN DATA

The CDO shall maintain an open data portal in order to fulfill the intent of City of Houston, Administrative Procedure 8-7, *Open Data*. The CDO will work with the Data Governance Unit to determine what data can be released under the Texas Public Information Act (TPIA).

Troy Finner
Chief of Police