Policy Title:	Data Usage and Classification Policy		
	**OFFICE OF THE CHIEF INFORMATION OFFICER**	**Category**	Information Technology Services
		Administrative Policy #	
		Revision #	N/A
		Review Frequency	As Needed – no less frequently than annually
Administrative Division	Information Technology Services (ITS)	**Reviewed By**	Chief Information Officer; Human Resources Director
BOWC Approval		**Last Reviewed/Update Date**	
Implementation Date		**Resolution #**	

1. **OBJECTIVES**

1.1. To ensure that data usage and classification align with and enhance the Detroit Water and Sewerage Department's (DWSD) business goals.

1.2. To maintain transparency and accountability in DWSD's data usage.
1.3. To protect DWSD's Sensitive Data and information from misuse.
1.4. To promote responsible data acquisition, development, and deployment.
1.5. To ensure DWSD complies with United States National Security Memorandum on Critical Infrastructure Security and Resilience, NSM-22

2. **PURPOSE**

2.1. The purpose of this Policy is to establish guidelines for the classification and usage of data within DWSD to ensure its confidentiality, integrity and availability.

3. **DEFINITIONS**

Data Classification includes the following definitions:

"DWSD-Critical" means data that, if disclosed, altered, and/or destroyed without authorization, could cause significant harm to individuals and/or DWSD. This type of data is likely subject to strict legal or regulatory requirements. Data in this category includes, but is not limited to, Social Security Numbers, financial account numbers, government-issued identification (e.g., driver's license), critical infrastructure information, and DWSD information system passwords.

"DWSD-Restricted Data" means data, if disclosed, altered, and/or destroyed without authorization, could cause harm to individuals and/or DWSD. This type of data is potentially subject to legal and/or regulatory requirements. Data in this category includes, but is not limited to, the last 4 digits of Social Security Numbers, personally identifiable information, detailed infrastructure plans, maps, etc., detailed or sensitive information technology or security records, records pertaining to employee health (e.g., medical records), or other sensitive employee information.

"DWSD-Internal Data" means data that is generally available within DWSD but is not readily available to the public. Data in this category includes, but is not

limited to, employee numbers or other related information (e.g., offer letters), basic infrastructure plans, general information technology reports, third-party contracts, and non-restricted or critical DWSD records created during the ordinary course of business.

"DWSD-Public Data" means data that, if disclosed, altered, and/or destroyed, is unlikely to cause harm to individuals and/or DWSD. This type of data is designed for public consumption and is freely available and accessible by the public. Data in this category includes, but is not limited to, general department information not regarded as critical, restricted, or internal, and public websites. While data in this category does not typically require sensitive handling or specific control requirements, some level of control may be required to ensure the integrity and availability of public data.

"Data Owner" means the person or persons responsible for the usage, classification, management, and quality of data assets in DWSD. Data owners are typically senior management or business division managers.

"Data Custodian" means those responsible for the technical implementation and maintenance of security controls as defined by the data classification policy. The data custodian ensures that protections are properly implemented according to policy. (Data custodians can be system administrators, Database administrators, and 3rd party IT vendors or cloud service providers.)

"Data User" means any individual, employee, contractor, or third party authorized to access and use data within the organization.

"Personally Identifiable Information" means data that can directly identify an individual without the use of any other additional information. Personally identifiable information can include, but is not limited to, full name, Social Security Number, driver's license number, or financial information.

"Sensitive Data" means data which are classified as DWSD-Critical or DWSD-Restricted.

4. SCOPE

4.1. This policy applies to all DWSD employees, contractors, interns, volunteers, people authorized to use DWSD's computer and technology resources, and persons authorized to handle DWSD data.

5. RESPONSIBILITIES

5.1. **Information Technology Services** ("DWSD-IT")

5.1.1. DWSD-IT is responsible for developing and updating this policy as needed, no less frequently than annually.

5.1.2. DWSD-IT is responsible for regularly reviewing access approvals to determine if access is still appropriate based on the Data User's job description or other approved reasons and for monitoring data systems to detect and immediately address issues.

5.1.3. DWSD-IT is responsible for providing regular mandatory training to all DWSD employees on data classification, usage, and handling whenever there has been a Policy amendment or update.

5.2. **Management**

5.2.1. Management is responsible for monitoring work areas for compliance and addressing any incident(s) of noncompliance by employees, contractors or volunteers, and is responsible for alerting DWSD-IT and Human Resources when a suspected or actual violation occurs.

5.3. **Human Resources**

5.3.1. Human Resources is responsible for issuing, reviewing and/or authorizing appropriate disciplinary action for employees who do not comply with this Policy.

5.4. **Data Owners**

5.4.1. Data Owners are responsible for identifying and classifying data and determining appropriate access controls for Data Users requesting access.

5.5. **Data Custodians**

5.5.1. Data Custodians implement and enforce access controls as assigned by the Data Owner and ensure data integrity.

5.6. **Data Users**

5.6.1. All DWSD computer and technology users are expected to exercise good judgment when using DWSD data. Effective security is a team effort involving the participation and support of every DWSD employee and affiliate who deals with data and/or information systems.

5.6.2. It is the responsibility of every computer and technology user to know these data standards and to properly handle and use data accordingly.

6. POLICY

6.1. **Data Use.** Data must only be used for business purposes or work-related tasks that are aligned with DWSD business objectives.

6.2. **Sensitive Data Privacy and Security**. Sensitive Data shall only be accessed if the Data User has written approval from DWSD-IT.

6.2.1. A Data User's supervisor must request approval from the Data Owner and provide a sufficient explanation why the Data User requires access to Sensitive Data.

6.2.2. The Data Owner requests approval from DWSD-IT.

6.2.3. DWSD-IT makes the final determination regarding data access.

6.2.4. Sensitive Data may only be shared with other approved Data Users using approved, secure methods, such as encrypted email, or IT-approved file-sharing and collaboration tools.

6.3. **Data Storage**

6.3.1. All Data must be stored in appropriate locations based on the classification and sensitivity of data (e.g., pertinent Box files, enQuesta, Cityworks)

6.4. **Unauthorized Disclosure**

6.4.1. Persons who know or believe that data has been disclosed, altered, and/or destroyed without authorization must immediately report the incident to the IT Service Desk by emailing ServiceDesk@detroitmi.gov, calling 313-628-4357 or using the IT Ticketing System.

6.4.2. DWSD-IT shall conduct a thorough investigation into all reports of unauthorized disclosures, alteration, or destruction of data and shall notify affected parties and regulatory authorities as required by law.

6.5. **Training and Awareness**

6.5.1. DWSD-IT commits to promoting a culture of data security through awareness campaigns.

6.6. **Compliance and Violations**

6.6.1. Employees should contact their supervisor if they have questions about whether proposed actions may violate this Policy.

6.6.2. Failure of a DWSD employee to comply with this Policy is a violation of DWSD's Employee Standards of Conduct Policy and may also constitute violations of other DWSD Policies, and may result in revocation of system privileges and/or disciplinary action up to and including termination according to DWSD's Corrective Action Policy.

6.6.3. Failure of a contractor using DWSD technology resources to comply with this Policy may be considered grounds for breach of its contract and revocation of system privileges.

6.6.4. Employees or contractors who use data for illegal purposes are subject to legal action by DWSD or other government authorities.

6.7. **Reasonable and Necessary Accommodations**

6.7.1. Management may take reasonable and necessary actions to accomplish the intent of this Policy.