PRO-302.2
CONFIDENTIAL AND PROPRIETARY INFORMATION ADMINISTRATIVE PROCEDURE

1.0 Purpose.

The purpose of this Administrative Procedure is to implement Section 302.3.1 of TRWD Board Policy 302 Employee Standards of Conduct and Code of Ethics to establish the principles and guidelines on the access, maintenance, and handling of TRWD's confidential and proprietary information.

2.0 Scope.

This Administrative Procedure applies to all departments, divisions, and offices within TRWD, and to all TRWD employees.

3.0 Confidential and Proprietary Information.

For purposes of this Administrative Procedure, confidential and proprietary information is generally information that falls within an exception to disclosure under the Texas Public Information Act.

Confidential and proprietary information includes, but is not limited to: certain financial records, such as types of investment information, and credit card, debit card, or other account number information; commercial information that would cause substantial competitive harm to the person from whom the information was obtained; certain information submitted by potential vendors or contractors; certain economic development information; certain geological or geophysical information; information regarding computer network security; health and/or medical records; personnel records other than an individual's own personnel records; payroll records; personally identifiable information on District records such as social security and credit card numbers; contracts; research data; computer system passwords and security codes; other TRWD proprietary information/data; other information and records which the employee is directed under proper authority to not disclose; and any other information for which access, use, or disclosure is not authorized by: a) federal, state, or local law; or b) TRWD policy or operations.

Confidential and proprietary information can be in any form including physical records/printed documents (e.g., forms, reports, memoranda, correspondence, microfilm, microfiche, books); computers, networks, electronically stored information; magnetic or optical storage media (e.g., hard drive, zip drive, flash drive, memory card, diskette, tape, CD, DVD); or physical storage environments (e.g., offices, filing cabinets, drawers).

Confidential information does not include information publicly disclosed by TWRD or which is required to be disclosed in accordance with the law, including the Texas Public Information Act, or contract.

4.0 Employee Duties and Responsibilities.

All TRWD employees shall use, maintain, protect, and handle all confidential and proprietary information, and other TRWD records, in a manner which protects the integrity

of the data and information and the privacy of those associated with it. Confidential, sensitive and proprietary information shall be protected from unauthorized access and disclosure consistent with the principles and requirements of this Administrative Procedure and as required by applicable law. Unless authorized to do so, employees may not access, remove, publish, destroy, or alter confidential or proprietary information.

An employee's responsibilities and obligations under this Administrative Procedure shall survive the termination of employment with TRWD.

5.0 Storage and Maintenance of Confidential and Proprietary Information.

All confidential and proprietary information in electronically stored information must reside and be stored on the network servers of TRWD, and not on local work stations, personal computers, laptops, or flash drives. All confidential information and proprietary information in the form of physical records must be stored in file cabinets that are secured and locked.

Based on and in accordance with record retention requirements, physical records, electronically stored information, and other records containing confidential or proprietary information must be disposed of in a way that ensures that the information is no longer recognizable or retrievable.

Upon conclusion of an employee's employment or upon request of a supervisor, employees, contractors/consultants, and volunteers will return originals and copies of all documents and files (whether electronic or hardcopy) containing confidential and proprietary information to the District and relinquish all further access to and use of such information.

6.0 Specific Requirements Regarding Personally Identifiable Information.

All confidential information containing personally identifiable information must be accessed and used only by authorized employees of TRWD. Such confidential information shall be used by TRWD only for legitimate purposes. Employees who are authorized to access and use such confidential information shall take all necessary precautions to assure that proper administrative, technical, and physical safeguards are established and followed to protect the confidentiality of the personally identifiable information.

7.0 Responsibilities of Authorized Users of Confidential and Proprietary Information.

Each authorized user of confidential information is responsible for understanding and complying with this Administrative Procedure. Each authorized user of confidential and proprietary information shall:

- Access only the information authorized and reasonably necessary to perform his or her duties as an employee of TRWD;
- Take appropriate measures to protect TRWD's confidential and proprietary information for which he or she is an authorized user;
- Safeguard the confidentiality of any security controls and passwords that allow access to confidential or proprietary information; and

- Report any suspected activities that may compromise confidential information to his or her immediate supervisor, the Human Resources Department, and the Information Technology Department.

8.0 Responsibilities of Supervisors of Authorized Users of Confidential Information.

Supervisors are responsible for establishing and maintaining security for confidential and proprietary information within their areas of responsibility consistent with this Administrative Procedure and shall:

- Identify confidential and proprietary information and materials within their areas of responsibility and implement adequate controls to secure confidential and proprietary data and information;
- Require and ensure that only authorized users have access to confidential and propriety information;
- Ensure that the employees he or she supervisors understand this Administrative Procedure and their duties and responsibilities in the handling of confidential and proprietary information and materials; and
- Engage in efforts to protect against the unauthorized disclosure of confidential or proprietary information.

9.0 Violations.

Noncompliance with or violation of this Administrative Procedure may result in disciplinary action, including termination of employment.