# SAN BERNARDINO MUNICIPAL WATER DEPARTMENT

*POLICIES & PROCEDURES MANUAL*

POLICY 21.020 – EMPLOYEE CONFIDENTIALITY

| | |
|---|---|
| Date: | September 24,2024 |
| Revision No: | New |
| Supersedes: | New |
| First Adopted: | September 24,2024 |

**POLICY**

An Employee Confidentiality Policy is critical to maintain trust and protect sensitive information obtained through the course of daily business. The purpose of this policy is to establish clear expectations and guidelines for maintaining the confidentiality of sensitive and personal information to prevent data breaches, maintain a positive work environment and ensure ethical business practices. Because data security is a top concern, having a robust confidentiality policy in place is essential.

Department Employees may unavoidably receive and handle personal and private information about employees, clients, partners, and the Department. Confidentiality at work refers to the ethical and legal obligation of employees to protect and keep private any sensitive and confidential information they come across in the performance of their regular job duties and during the course of their employment. Sensitive and personal information should remain private unless the owner of that information wishes to disclose it.

This policy applies to all employees, contractors and third-party vendors who have access to confidential and/or sensitive information. Employees are required to adhere to this policy in all aspects of their work which means they must be cautious when discussing sensitive information, handling documents, and accessing electronic data. Employees should also be mindful of who they share entrusted information with responsibly, both within and outside of the Department.

Confidential/sensitive information may include, but is not limited to, customer data, financial information, trade secrets, employee information and any other information that is not publicly available to include:

- Uncirculated financial information
- Certain records pertaining to customers, partners, clients, and/or employees.

- Patents, formulas, or proprietary methods/methodologies.
- Written/electronic documents or similar material entrusted to the Department by outside parties.
- Pricing/marketing/contracts and other unrevealed strategies as applicable
- Any material explicitly marked as confidential.
- Uncirculated material pertaining to goals, predictions and proposals marked as confidential.

Depending on their job title/responsibilities, seniority and other factors, employees may have differing levels of authorized access to this type of sensitive information and/or material. Employees must:

- Maintain the confidentiality of all sensitive information they have access to in the course of their job duties, including but not limited to, personal information about employees, customers, stakeholders, and any other confidential business information.
- Only access and use confidential information to perform their job responsibilities as authorized by the Department.
- Protect the confidentiality of sensitive information by using appropriate safeguards, such as password protection and secure storage of documents and data.
- Ensure confidential material is never left in plain view or otherwise unsecured.
- Shred confidential material when it is no longer needed.
- Ensure that any confidential information in a digital format is only viewed on secure devices.
- Refrain from making authorized disclosures to coworkers or unauthorized individuals within or outside the Department unless required by law or authorized by management.
- Refrain from taking confidential documents off company property unless necessary.

- Surrender all confidential documents and material to the company upon resignation, termination or at any time upon the request of their supervisor.

- Take reasonable steps to ensure that they do not mistakenly disclose any confidential information to any unauthorized persons in or outside the company.

- Report any inadvertent disclosures of confidential information to their direct supervisor as soon as possible.

Employees are prohibited from doing the following:

- Sharing or disclosing sensitive information to unauthorized individuals or for unauthorized purposes and using confidential information for financial or personal gain or to benefit others outside the course of their work duties.

- Removing, forwarding by email, downloading, or making copies of confidential material; or facilitating the reproduction of confidential material relating to the Department in any manner.

- Employees should not access the personal office space of others including locked desk drawers and/or file cabinets without permission.

Any employee who becomes aware of a confidentiality breach must report it to their supervisor or Human Resources immediately.

From time to time, some circumstances may warrant disclosure of confidential or sensitive information such as:

- A regulatory/law enforcement/or other government agency requests it as part of an investigation or audit.

- If we consider a venture or partnership requiring the disclosure some information (within legal parameters)

When this happens, employees who receive such requests or are privy to such considerations should carefully document their disclosure procedure and gather required authorizations.

The Department will investigate any breach of this policy. Violation of this policy may result in disciplinary action up to and including termination.

Confidentiality obligations continue even after the termination of employment. Former employees must refrain from disclosing or using any confidential information obtained during their employment.

This policy will be reviewed annually and updated as needed to ensure it remains current and effective.

**Policy Review**

Established/Board approved: 9/24/2024