SAN BERNARDINO MUNICIPAL WATER DEPARTMENT

POLICIES & PROCEDURES MANUAL

POLICY 61.050 - SECURITY AWARENESS TRAINING

Date:	February 22, 2022
Revision No:	New
Supersedes:	New
First Adopted:	February 22, 2022

POLICY:

Cybersecurity is a critical component of the Department's overall information Technology (IT) strategic plan. The IT Section maintains an active Security Awareness Training program available to all staff. This policy establishes the authority of the IT Section to mandate Security Awareness Training as needed and outlines the expectations for individuals and sections in assisting with ensuring the confidentiality, integrity, and availability of Department systems, services, and data.

SCOPE:

This policy applies to all Department staff who regularly interact with or have access to any Department computing system, including email.

PROCEDURE:

Staff knowledge of the threats and risks to the Department's systems and data is a critical component in helping to defend the Department from cyberattack.

The IT Section maintains an Information Security Awareness Program that supports Department staff needs for regular training. Training on important information security topics is available or communicated in multiple formats including:

- Online training systems with a variety of topics relevant to information security.
- Communications to targeted groups by email of ongoing or imminent threats

- Postings on various web-based systems across the Department
- Quarterly security awareness evaluations

As part of ongoing operations and staff development, annual Security Awareness Training is mandated by the Department through the IT Section. Training opportunities may include offerings from the IT Section or a tailored program for specific threats against divisions or systems, which may also be included in procedural manuals or scheduled as group training.

In some areas, Security Awareness Training may be mandatory based on federal or industry regulations. Training for these programs must be coordinated with the IT Section to ensure regulatory requirements are met.

Failure to comply with mandatory Security Awareness Training, or to coordinate training with the IT Section, may result in discipline up to and including termination.

Policy Review

Established/Board approved:	2/22/2022
No changes:	7/2022
No changes:	7/2023
No changes:	7/2024