TWAIN HARTE COMMUNITY SERVICES DISTRICT
Finance/Policy Committee Meeting

Chair: *Mary Dearborn*
Co-Chair: *Charlotte Bohlman*

THCSD CONFERENCE ROOM
22912 VANTAGE POINTE DR., TWAIN HARTE
November 4, 2026 1:30 p.m.

NOTICE: Public May Attend this Meeting In-Person.

The meeting will be accessible via ZOOM for anyone that chooses to participate virtually:

- Videoconference Link: https://us02web.zoom.us/j/89166816374
- Meeting ID: 891 6681 6374
- Telephone: (669) 900-6833

AGENDA

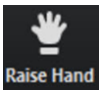
1. **Annual review of Policy #1015 – Identity Theft Prevention Program.**
2. **Annual review of Policy #2082 – Internet Email and Social Media Use.**
3. **Review and discuss proposed revisions to Policy #4000 – Board of Directors.**
4. **Adjourn.**

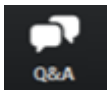
HOW TO VIRTUALLY PARTICIPATE IN THIS MEETING

The public will have an opportunity to comment before and during the meeting as follows:

- **Before the Meeting**:
  - Email comments to ksilva@twainhartecsd.com, write "Public Comment" in the subject line. In the body of the email, include the agenda item number and title, as well as your comments.
  - Mail comments to Board Secretary: 22912 Vantage Pointe Dr., Twain Harte, CA 95383
- **During the Meeting:**
  - Computer/Tablet/Smartphone: Click the "Raise Hand" icon and the host will unmute your audio when it is time to receive public comment. If you would rather make a

comment in writing, you may click on the "Q&A" icon and type your comment. You may need to tap your screen or click on "View Participants" to make icons visible.

Raise Hand Icon: 

Q&A Icon: 

- Telephone: Press *9 if to notify the host that you have a comment. The host will unmute you during the public comment period and invite you to share comments.
- In-Person: Raise your hand and the Board Chairperson will call on you.

PUBLIC COMMENT RULES

- If you wish to speak on an item on the agenda, you are welcome to do so during consideration of the agenda item itself.
- If you wish to speak on a matter that does not appear on the agenda, you may do so during the Public Comment period.
- Persons providing public comment will be limited to five minutes or depending on the number of persons wishing to speak, it may be reduced to allow all members of the public the opportunity to address the Board.
- Except as otherwise provided by law, no action or discussion shall be taken/conducted on any item not appearing on the agenda.
- Public comments must be addressed to the board as a whole through the President. Comments to individuals or staff are not permitted.

MEETING ETIQUETTE

Attendees shall make every effort not to disrupt the meeting. Cell phones must be silenced or set in a mode that will not disturb District business during the meeting.

ACCESSIBILITY

Board meetings are accessible to people with disabilities. In compliance with the Americans with Disabilities Act, those requiring accommodations for this meeting should notify the District office 48 hours prior to the meeting at (209) 586-3172.

WRITTEN MEETING MATERIALS

If written materials relating to items on this Agenda are distributed to Board members prior to the meeting, such materials will be made available for public inspection on the District's website: www.twainhartecsd.com

TWAIN HARTE COMMUNITY SERVICES DISTRICT

Policy and Procedure Manual

POLICY TITLE: Identity Theft Prevention Program
POLICY NUMBER: 1015
ADOPTED: June 11, 2009
LAST REVIEWED: 11/12/2025
LAST AMENDED: November 12, 2025

1015.10 PURPOSE

This program is intended to identify red flags that will alert District employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, and provide measures to respond to such events.

1015.20 RISK ASSESSMENT

This policy is based on an internal risk assessment conducted by the District to evaluate how at risk the current procedures are at allowing customers to create a fraudulent account and evaluate if current (existing) accounts are being manipulated. This risk assessment evaluated how new accounts were opened and the methods used to access the account information. Using this information, the District identified red flags that were appropriate to prevent identity theft for the following types of activities:

- New accounts opened in person for new construction
- New accounts opened via mail (copy of Grant Deed required)
- Account information accessed in person
- Account information accessed via telephone (person)

1015.30 DETECTION (RED FLAGS)

At a minimum, the following red flags will be used to detect potential fraud. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary.

- Identification documents appear to be altered.
- Photo and physical description do not match appearance of applicant.
- Other information is inconsistent with information provided by applicant.
- Other information provided by applicant is inconsistent with information on file.
- Application appears altered or destroyed and reassembled.

- Personal information provided by applicant does not match other sources of information (e.g. credit reports, SS# not issued or listed as deceased).
- Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application).
- Information commonly associated with fraudulent activity is provided by applicant (e.g. address that is a mail drop or prison, non-working phone number or associated with answering service/pager).
- SS#, address, or telephone # is the same as that of another customer.
- Customer fails to provide all information requested.
- Personal information provided is inconsistent with information on file for a customer.
- Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet.
- Identity theft is reported or discovered.

1015.40 RESPONSE TO POTENTIAL FRAUD

Any employee that may suspect fraud or detect a red flag will implement the following response as applicable. All detections or suspicious red flags shall be reported to senior management.

1. Ask applicant for additional documentation
2. Notify internal manager: Any District employee who becomes aware of suspected or actual fraudulent use of a customer or potential customers' identity must notify the Customer Services Manager and General Manager.
3. Notify law enforcement: The District will notify Sheriff's Department at Sonora, CA of any attempted or actual identity theft.
4. Do not open the account.
5. Close the account.
6. Do not attempt to collect against the account but notify authorities.

1015.50 PERSONAL INFORMATION SECURITY PROCEDURES

The District shall implement the following security procedures:

1. Paper documents, files and electronic media containing secure information will be stored in locked file cabinets.
2. Only specially identified employees with a legitimate need will have keys to the office and cabinets.
3. Files containing personally identifiable information are kept in locked file cabinets except when an employee is working on the file.
4. Employees will not leave sensitive papers out on their desks when they are away from their workstations.

5. Employees will store files when leaving their work areas.
6. Employees will lock file cabinets when leaving their work areas.
7. Visitors who must enter areas where sensitive files are kept must be escorted by a District employee.
8. No visitor will be given any entry codes or allowed unescorted access to the office.
9. Access to sensitive information will be controlled using “strong” passwords. Employees will choose passwords with a mix of letters, numbers, and characters.
10. Passwords will not be shared or posted near workstations.
11. When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
12. Sensitive information that is sent to third parties over public networks will be encrypted.
13. Anti-virus and anti-spyware programs will be run on individual computers and on servers daily.
14. When sensitive data is received or transmitted, secure connections will be used.
15. Computer passwords will be required.
16. Usernames and passwords will be different.
17. The computer network will have a firewall where your network connects to the Internet.
18. Check references or do background checks before hiring employees who will have access to sensitive data.
19. New employees sign an agreement to follow the District’s confidentiality and security standards for handling sensitive data.
20. Access to customer’s personal identity information is limited to employees with a “need to know.”
21. Procedures exist for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information.
22. Implement a regular schedule of employee training.
23. Employees will be trained to recognize attempts at phone/email/text phishing and other forms of cyber security breach tactics.
24. Employees are required to notify the General Manager immediately if there is a potential security breach.

25. Employees who violate security policy are subjected to discipline up to, and including, dismissal.
26. Service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of our data.
27. Paper records will be shredded before being placed into the trash.
28. Paper shredders will be available in the office.
29. Any data storage media will be disposed of by shredding, punching holes in, or incineration.

1015.60 IDENTITY THEFT PREVENTION PROGRAM REVIEW AND APPROVAL

Annually, at each November board meeting, the General Manager will prepare and submit a report to the governing body that includes matters related to the program, the effectiveness of the policies and procedures, the oversight and effectiveness of any third party billing and account establishment entities, a summary of any identify theft incidents and the response to the incident and recommendations for substantial changes to the program, if any.

Appropriate employees will be trained on the contents and procedures of this policy.

Twain Harte Community Services District
MEMORANDUM

DATE: November 4, 2026

TO: Board of Directors

FROM: Tom Trott, General Manager

SUBJECT: Annual Report – Identity Theft Prevention Program (Policy #1015)

Twain Harte Community Services District staff successfully implemented the Identity Theft Prevention Program (Policy #1015) over the last year of business. The following report summarizes Policy activities over the past year.

Actions:

- Detection. Employees looked for red flags identified in the Policy when opening new accounts, receiving requests to access account information, and in daily business activities with other staff, vendors and customers.
- Response. When red flags were detected, employees responded according to the Policy by asking for additional information. This prevented fraud in all cases related to customer or vendor interactions. It also helped identify fraudulent emails from cyber thieves who attempted to coerce District staff to provide unauthorized information or access.
- Personal Information Security Procedures. All procedures were followed.
- Training. Appropriate staff reviewed Policy 1015 and were trained on its contents and procedures to prevent fraud. All staff have received cyber security training and specific training on password management utilizing the District's password management platform.

Incidents:

ZERO incidents occurred in the last year related to District staff, customers and vendors.

Recommendations:

Policy guidelines proved effective in preventing fraud; therefore, no substantive Policy changes are recommended.

TWAIN HARTE COMMUNITY SERVICES DISTRICT
Policy and Procedure Manual

POLICY TITLE: Internet, Email and Social Media Use
POLICY NUMBER: 2082
ADOPTED: May 14, 2009
AMENDED: 3/8/2012, 1/10/2013, 9/8/2016, 11/12/2020, 11/12/2025
LAST REVIEWED: ~~11/12/2025~~11/12/26
LAST AMENDED: ~~November 12, 2025~~ November 12, 2026

2082.10 PURPOSE

The District believes that employee access to and use of internet, email, social media and other electronic communications resources benefits the District. This policy is established to ensure that all District employees use internet, email and social media resources in an ethical, legal and appropriate manner. This policy defines acceptable and unacceptable use of internet, email and social media resources. It also establishes actions the District may take for inappropriate use of such resources, since misuse has the potential to harm the District's reputation and success.

2082.20 ACKNOWLEDGEMENT AND REVIEW

2082.21 Acknowledgment. All employees must read and adhere to the guidelines and requirements established herein. Employees shall verify that they have read the policy by signing a form that will be placed in their personnel file.

2082.22 Review. The District Board shall review this policy annually. At the same time as the Board's review or any time after the Board revises this policy, all District employees shall re-read the policy and acknowledge their review in writing.

2082.30 DEFINITIONS

2082.31 Email. All forms of electronic information sent over the internet, including but not limited to electronic mail and instant chat messages.

2082.32 Post. Content an individual shares on a social media site or the act of publishing content on a site.

2082.33 Profile. Information that a user provides about himself or herself on a social networking site.

2082.34 Social Media. A category of internet-based resources that enable the user to generate content and encourage other user participation. This includes, but is not

limited to, social networking sites: Facebook, Instagram, X, NextDoor, TikTok, Snapchat, YouTube and other sites. (There are thousands of these types of sites and this is only a short list.)

2082.35 Social Networks. Platforms where users can create profiles and share information with others using a range of technologies.

2082.36 Speech. Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication.

2082.40 NO RIGHT TO PRIVACY

2082.41 Employees do not have any right to privacy in District internet, email and social media use. This includes, but is not limited to internet sites visited, downloads and email messages produced, sent or received through the District's email system or the District's servers and network.

2082.42 The District maintains administrative controls to email and internet and may reset passwords to access accounts at any time. Employees must disclose passwords to systems, software and sites not directly controlled by the District.

2082.43 Employees access to and use of the internet, email and other electronic communications (including all associated content) will be monitored frequently to promote the administration of the District, its business and policies.

2082.44 The District retains backup copies of all documents, including email messages produced, sent, received, and deleted through the District's email system, in accordance with the District's Records Retention Policy. All such copies may be considered a public record available to the public via the Public Records Act.

2082.45 It is advisable for all employees of the District to remind customers/clients/ contractors that email and/or documents sent to the District are not confidential.

2082.50 APPROPRIATE USE GUIDELINES

District employees and Board members shall adhere to the following guidelines of appropriate use of District internet, email and social media resources:

1. Correspondence with customers (and others) through the District's email system may be considered part of the District's public records and should be treated as such.

2. When employees communicate using email or other features of the internet, the employee must be extremely mindful of the image being portrayed of the District.

3. Email and any attachments are subject to the same ethical and legal concerns and standards of good conduct as memos, letters and other paper-based documents.

Employees shall not transmit information in an email that should not be written in a letter, memorandum or document available to the public.

4. Be aware of the content placed within an email. Email, once transmitted, can be printed, forwarded and disclosed by the receiving party without the consent of the sender.

5. Employees shall take all necessary steps to prevent unauthorized disclosure of confidential or privileged information.

6. Employees are to be continually aware of phishing scams and other methods hackers use to compromise security and shall consider such scams before downloading or opening files and other items on their computers to prevent the introduction of computer viruses.

7. Emails that employees need to retrieve from their personal internet accounts must be retrieved via that user's personal internet account.

8. ~~Employees will only access the internet using the approved internet browser. Any other browser being used on a workstation will be promptly removed.~~Employees shall use District-approved internet browsers and software. Additional browsers or software may be installed or used only as authorized under District procedures.

9. Employees will only download information and/or publications for official business purposes.

10. Employees will respect all copyright and license agreements regarding software or publication that they access or download from the internet. The District will not condone violations of copyright laws and licenses and the employee will be personally liable for any fines or sanctions caused by the license or copyright infringement. Any software or publication, which is downloaded onto District computer resources, becomes the sole property of the District.

2082.60 INAPPROPRIATE USE RESTRICTIONS

District employees and Board members shall not engage in any of the following restrictions related to use of District internet, email and social media resources:

1. Accessing internet sites that contain pornography, exploit children or that would generally be regarded in the community as offensive, or for which there is no official business purpose to access.

2. Participating in any profane, defamatory, harassing, illegal, discriminatory or offensive activity or any activity that is inconsistent in any way with the District's policies (i.e. Policy #2002 Discrimination, Policy #2215 Unlawful Harassment).

3. Using speech containing obscene or sexually explicit language, images, or acts and statements or other forms of speech that ridicule, malign, disparage, or otherwise express bias against any protected class of individuals.

4. Using speech involving themselves or other District personnel reflecting behavior that would reasonably be considered reckless or irresponsible.

5. Transmitting offensive messages of any kind.

6. Posting, downloading or viewing inappropriate pictures or images.

7. Using email or the internet to distribute copyrighted materials.

8. Using email, internet or social media for inappropriate or unauthorized advertising and promotion of the District or others.

9. Using email, internet or social media for personal commercial activity.

10. Using another employee's username/account without express permission of the user or systems administrator.

11. Receiving and/or downloading executable files and programs without express permission of the systems administrator. This includes, but is not limited to, software programs and software upgrades. This does not include email and/or documents received via email and the internet. All downloaded files must be scanned for viruses.

12. Exploiting security weaknesses of the District's computer systems and network and/or other networks or computers outside the District.

13. Using internet, email and/or social media in a manner that interferes with the timely and efficient performance of job duties. Access to these resources is not a benefit of employment with the District.

2082.70 PERSONAL USE OF SOCIAL MEDIA

2082.71 Purpose and Philosophy. Social media provides a valuable means of assisting the District and its personnel in gathering community information and other related organizational and community objectives. This section identifies possible uses of social media that may be deemed necessary by Board members and District personnel.

2082.72 Employee and Board Responsibility. The proper functioning of any public agency relies upon the public's confidence and trust in the individuals and the agency to provide effective service and protection. Any matter, which brings the integrity of District personnel or Board members into question has the corresponding effect of reducing public confidence and trust, impeding the ability to work and serve the public. While employees and Board members have the right to use personal/social networking web pages or sites, as members of the District, they are encouraged to remember their position of public responsibility, trust, and transparency when using personal social media. Employees and Board members shall maintain a level of professionalism in both on and off-duty conduct. Employees and Board members shall not engage in conduct that contradicts or impedes the mission of the District.

2082.73 Personal Use Cautions. Employees and Board members are cautioned to take into account the following when using social media for personal use:

1. Employees are free to express themselves as private citizens on social media sites to the degree that their speech does not impair working relationships of the District, impede the performance of duties, impair discipline and harmony among co-workers, or negatively affect the public perception of the District.

2. Employees are cautioned that their speech either on or off duty has a nexus to the employee's professional duties and responsibilities and may not necessarily be protected speech under the First Amendment.

3. Employees should assume that their speech and related activity on social media sites will reflect upon their position within the District and should be mindful that their speech becomes part of the worldwide web.

4. Employees should expect that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the District at any time without prior notice.

5. Employees should not display department logos, uniforms, or similar identifying items on personal web pages without prior written permission.

6. Employees should not post any material that brings discredit to or may adversely affect the efficiency or integrity of the District.

7. Employees should not complain about their jobs, supervisors, or co-workers in a public forum. These comments reflect poorly on employee, the organization and the persons criticized. Negative and derogatory comments may also lead to claims of defamation and slander.

2082.74 Personal Use Prohibitions. Employees and Board members are prohibited from the following types of personal use of social media:

1. Using social media or other electronic communication to discuss or deliberate District business, directly or indirectly, in a manner that violates the Brown Act.

2. Using the Twain Harte Community Services District name, logos, or employee status on personal social media to imply, directly or indirectly, that personal opinions or posts are an official position or opinion of the District.

3. Divulging information gained by reason of their authority as a District employee or making any statements, speeches, appearances, and endorsements, or publishing materials that could reasonably be considered to represent the views or positions of the District without express authorization.

4. Linking work activities to personal social media postings.

5. Posting inappropriate status updates that discuss department, other staff members, or that may implicate unprofessional conduct.

6. Posting photographs/images, video, audio files and/or any other information related to any emergency response activity conducted by the District.

7. Posting, transmitting, or otherwise disseminating any information accessed as a result of employment without written permission from the General Manager or designee.

8. Using social media while engaged in District work activities, except when such use is directly related to performance of District work activities. Access to social media sites on a personal device should only occur during breaks or absolute down time (firefighters only). It is inappropriate to post statuses or to view social networking profiles while engaged in District work activity.

2082.80 OFFICIAL DISTRICT SOCIAL MEDIA USE

At the discretion of the General Manager, the District may establish and utilize social media accounts to gather and disseminate information. All such use shall serve to further the mission and vision of the District. The General Manager, or his/her official designee, shall manage and oversee all official District social media use. All content posted via District social media must be approved prior to posting by the General Manager or official designee.

2082.90 VIOLATIONS

Failure to adhere to the guidelines and requirements of this policy may lead to disciplinary action, up to and including, immediate termination. Any employee becoming aware of or having knowledge of a posting or of any social media site or web page in violation of the provision of this policy shall notify his or her supervisor immediately for follow-up action. Violation of this social media policy may result in suspension or termination.

TWAIN HARTE COMMUNITY SERVICES DISTRICT
Policy and Procedure Manual

POLICY TITLE: **Board of Directors**
POLICY NUMBER: **4000**

ADOPTED: **September 17, 1996**

AMENDED: **2/10/11, 9/15/21**

LAST AMENDED: ~~**September 15, 2021**~~**November 12, 2026**

4000.10 BOARD OF DIRECTORS

4000.11 Governing Body. The District shall be governed by a five-member Board of Directors, in accordance to California Government Code Sections 61000-61250 (Community Services Districts). Members of the Board of Directors must meet the following criteria:

1. No person shall be a candidate for the Board of Directors unless he or she is a voter of the District.

2. A member of the Board of Directors shall not be the General Manager, the District Treasurer or any other compensated employee of the District.

4000.12 Purpose. The Board of Directors is responsible for the overall governance of the District, establishing policies for District operation and appointing a General Manager to implement those policies. All Directors shall exercise their independent judgment on behalf of the interests of the entire District, including the residents, property owners, and the public as a whole.

4000.20 SELECTION OF DIRECTORS

4000.21 Election and Terms. Directors shall be elected at large, serving as follows:

1. Directors shall serve staggered terms of four years.

2. Terms shall begin on the first Friday in December following their election.

4000.22 Vacancies. Board of Director vacancies in the middle of a term shall be filled pursuant to Section 1780 of the California Government Code.

4000.30 OFFICERS

4000.31 Board Officers. Each December, ~~T~~the Board of Directors shall vote to elect Directors to serve as Board President and Vice President ~~elect the following Officers each December to serve in that office~~ for the following calendar year. Directors elected to serve in these roles are expected to be present at Board meetings to fulfill their respective duties. If a Director elected as President or Vice President is absent for three meetings within the calendar year, the Director will forfeit their Board Officer position and the Board will vote to elect a replacement at the next regular Board meeting. General duties of Board Officers are as follows:

1. President. The President of the Board of Directors shall serve as chairperson at all Board meetings. He/she shall have the same rights as the other members of the Board in voting, introducing motions, resolutions and ordinances, and any discussion of questions that follow said actions.

2. Vice President. In the absence of the President, the Vice President of the Board of Directors shall serve as chairperson over all meetings of the Board. If the President and Vice President of the Board are both absent, the remaining members present shall select one of themselves to act as chairperson of the meeting.

4000.32 District Officers. The Board of Directors shall appoint the following District Officers to serve at their pleasure:

1. General Manager. The General Manager shall be responsible for all of the following:

    A. Implementation of the policies established by the Board of Directors for the operation of the District.

    B. Appointment, supervision, discipline, and dismissal of the District's employees, consistent with employee relations policies and agreements established by the Board of Directors.

    C. Supervision of the District's facilities and services.

    D. Supervision of the District's finances.

2. District Treasurer. The Board may appoint the General Manager as the District Treasurer. The District Treasurer shall be responsible for all of the following:

    A. Implementation of a system of accounting that adheres to generally accepted accounting principles and, at all times, shows the District's financial condition.

    B. Implementation of the Board's financial policies and laws to control withdrawals and deposits of District funds, make

payments, manage loans, pay employee salaries and make other financial transactions required for District operations.

C. Providing written reports to the Board of Directors regarding the receipts, disbursements and balances in the accounts controlled by the District Treasurer.

TWAIN HARTE COMMUNITY SERVICES DISTRICT
Policy and Procedure Manual

POLICY TITLE: **Board of Directors**
POLICY NUMBER: **4000**

ADOPTED: **September 17, 1996**

AMENDED: **2/10/11, 9/15/21**

LAST AMENDED: **November 12, 2026**

4000.10 BOARD OF DIRECTORS

4000.11 Governing Body. The District shall be governed by a five-member Board of Directors, in accordance to California Government Code Sections 61000-61250 (Community Services Districts). Members of the Board of Directors must meet the following criteria:

1. No person shall be a candidate for the Board of Directors unless he or she is a voter of the District.

2. A member of the Board of Directors shall not be the General Manager, the District Treasurer or any other compensated employee of the District.

4000.12 Purpose. The Board of Directors is responsible for the overall governance of the District, establishing policies for District operation and appointing a General Manager to implement those policies. All Directors shall exercise their independent judgment on behalf of the interests of the entire District, including the residents, property owners, and the public as a whole.

4000.20 SELECTION OF DIRECTORS

4000.21 Election and Terms. Directors shall be elected at large, serving as follows:

1. Directors shall serve staggered terms of four years.

2. Terms shall begin on the first Friday in December following their election.

4000.22 Vacancies. Board of Director vacancies in the middle of a term shall be filled pursuant to Section 1780 of the California Government Code.

4000.30 OFFICERS

4000.31 Board Officers. Each December, the Board of Directors shall vote to elect Directors to serve as Board President and Vice President for the following calendar year. Directors elected to serve in these roles are expected to be present at Board meetings to fulfill their respective duties. If a Director elected as President or Vice President is absent for three meetings within the calendar year, the Director will forfeit their Board Officer position and the Board will vote to elect a replacement at the next regular Board meeting. General duties of Board Officers are as follows:

1. President. The President of the Board of Directors shall serve as chairperson at all Board meetings. He/she shall have the same rights as the other members of the Board in voting, introducing motions, resolutions and ordinances, and any discussion of questions that follow said actions.

2. Vice President. In the absence of the President, the Vice President of the Board of Directors shall serve as chairperson over all meetings of the Board. If the President and Vice President of the Board are both absent, the remaining members present shall select one of themselves to act as chairperson of the meeting.

4000.32 District Officers. The Board of Directors shall appoint the following District Officers to serve at their pleasure:

1. General Manager. The General Manager shall be responsible for all of the following:

    A. Implementation of the policies established by the Board of Directors for the operation of the District.

    B. Appointment, supervision, discipline, and dismissal of the District's employees, consistent with employee relations policies and agreements established by the Board of Directors.

    C. Supervision of the District's facilities and services.

    D. Supervision of the District's finances.

2. District Treasurer. The Board may appoint the General Manager as the District Treasurer. The District Treasurer shall be responsible for all of the following:

    A. Implementation of a system of accounting that adheres to generally accepted accounting principles and, at all times, shows the District's financial condition.

    B. Implementation of the Board's financial policies and laws to control withdrawals and deposits of District funds, make

payments, manage loans, pay employee salaries and make other financial transactions required for District operations.

C. Providing written reports to the Board of Directors regarding the receipts, disbursements and balances in the accounts controlled by the District Treasurer.