TWAIN HARTE COMMUNITY SERVICES DISTRICT
Finance/Policy Committee Meeting

Chair: *Gary Sipperley*
Co-Chair: *Eileen Mannix*

THCSD CONFERENCE ROOM
22912 VANTAGE POINTE DR., TWAIN HARTE
November 2, 2022 1:30 p.m.

NOTICE: Public May Attend this Meeting In-Person. Facial coverings are recommended for any person attending, regardless of vaccination status.

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

- Videoconference Link: https://us02web.zoom.us/j/83250369421
- Meeting ID: 832 5036 9421
- 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 of Policy #2011 – On-Call Duty.**
4. **Review of Policy #2030 – Holidays.**
5. **Review of Policy #2032 – Management Leave.**
6. **Adjourn.**

HOW TO VIRTUALLY PARTICIPATE IN THIS THIS MEETING

The public can virtually observe and participate in a meeting as follows:

- **Computer**: Join the videoconference by clicking the videoconference link located at the top of this agenda or on our website. You may be prompted to enter your name and email. Your email will remain private and you may enter "anonymous" for your name.
- **Smart Phone/Tablet**: Join the videoconference by clicking the videoconference link located at the top of this agenda OR log in through the Zoom mobile app and enter the Meeting ID# and Password found at the top of this agenda. You may be prompted to enter

your name and email. Your email will remain private and you may enter "anonymous" for your name.

- **Telephone**: Listen to the meeting by calling Zoom at (4669) 900-6833. Enter the Meeting ID# listed at the top of this agenda, followed by the pound (#) key.

***** NOTE: your personal video will be disabled and your microphone will be automatically muted.

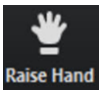
FOR MORE DETAILED INSTRUCTIONS, CLICK HERE

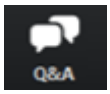
SUBMITTING PUBLIC COMMENT

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 THCSD Board Secretary: P.O. Box 649, 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.

* NOTE: 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 speaking during the 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

ORIGINAL VERSION

TWAIN HARTE COMMUNITY SERVICES DISTRICT

Policy and Procedure Manual

POLICY TITLE:	**Identity Theft Prevention Program**
POLICY NUMBER:	**1015**
ADOPTED:	**June 11, 2009**
REVIEWED:	**10/9/2014, 10/10/2015, 10/6/2016, 10/12/2017, 10/10/2018, 11/12/2019, 11/12/2020**
LAST AMENDED:	**March 11, 2020**

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, methods to ensure existing accounts were not opened using false information and 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 Utility employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers' identity must notify Finance Officer or General Manager.
3. Notify law enforcement: The Utility 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 store files when leaving their work areas.
6. Employees 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 alert to attempts at phone phishing.
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

Policy and Procedure Manual

POLICY TITLE: **Identity Theft Prevention Program**
POLICY NUMBER: **1015**
ADOPTED: **June 11, 2009**
LAST REVIEWED: **November 10, 2021**
LAST AMENDED: **March 11, 2020**

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 a suspected or actual fraudulent use of a customer or potential customers' identity must notify Finance Officer or 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 store files when leaving their work areas.
6. Employees 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 alert to attempts at phone phishing.
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

Policy and Procedure Manual

POLICY TITLE: Identity Theft Prevention Program
POLICY NUMBER: 1015
ADOPTED: June 11, 2009
LAST REVIEWED: November 10, 2021
LAST AMENDED: March 11, 2020

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, ~~methods to ensure existing accounts were not opened using false information~~ 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 ~~Utility~~District employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers' identity must notify Finance Officer or General Manager.
3. Notify law enforcement: The ~~Utility~~ 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 store files when leaving their work areas.
6. Employees 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 alert to attempts at phone phishing.
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 2, 2022

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 bank charges, which occurred this past year. The charges were quickly identified, reported and reversed.
- 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.

Incidents:

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

Recommendations:

The guidelines of this policy 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**
REVIEWED: **12/10/2015, 12/14/2017**
LAST AMENDED: **November 10, 2021**

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, Twitter, 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.

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.

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 #2170 Sexual Harassment, Policy #2215 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 administrative and supervisory personnel.

2082.72 Employee 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 into question has the corresponding effect of reducing public confidence and trust, impeding the ability to work and serve the public. While employees 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 shall maintain a level of professionalism in both on and off-duty conduct. Employees shall not engage in conduct that contradicts or impedes the mission of the District.

2082.73 Personal Use Cautions. Employees 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 that has a nexus to the employee's professional duties and responsibilities 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 you, the organization and the persons that you criticize. Negative and derogatory comments may also lead to claims of defamation and slander.

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

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

2. 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.

3. Linking work activities to personal social media postings.

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

5. Post photographs/images, video, audio files and/or any other information related to any emergency response activity conducted by this District.

6. Post, transmit, or otherwise disseminate any information to which they have access as a result of their employment without written permission from the General Manager or designee.

7. 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) as you would use a personal cell phone when on duty. It is inappropriate to post statuses or to view social networking profiles while engaged in District work activity.

2082.80 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.

ORIGINAL VERSION

TWAIN HARTE COMMUNITY SERVICES DISTRICT
Policy and Procedure Manual

POLICY TITLE: **On-Call Duty**
POLICY NUMBER: **2011**
ADOPTED: **October 11, 2007**
AMENDED:

2011.10 In order to insure that no emergency within District facilities goes unattended, an On-Call Duty Operator system has been established. This system requires that at least two District Operations or Maintenance employees be available twenty-four (24) hours a day to respond to any emergency which may arise.

2011.20 The Operations Manager will post an On-Call Duty Operator schedule for operations and maintenance employees to cover off-shift, night, weekend and holiday emergency work. The schedule will rotate assignments to be fair to all employees. Any employee so scheduled will be on-call as scheduled, including holidays.

2011.30 It is the scheduled Duty Operator's responsibility to insure that coverage is available during all assigned off-shift hours. If an employee has a conflict with the schedule or is otherwise unable to maintain coverage, it is that person's responsibility to get another qualified employee to cover time away from the District and to inform the Operations Manager of the substitution.

2011.31 Under non-emergency circumstances, all requests for schedule changes or substitutions should be in writing and receive prior approval by the Operations Manager or his/her designee.

2011.32 In the event an emergency substitution is needed during off-shift hours, the Duty Operator requesting the substitution must arrange with someone else to take his/her place and note the substitution in the Duty Operator Shift Log. The substituting employee will immediately notify the Operations Manager or his/her designee.

2011.40 The On-Call Duty Operator will have the following responsibilities:

2011.41 The assigned Duty Operator will be available by the District's emergency pager. When on call, the Duty Operator shall be free to utilize his/her time as desired, but must remain fit for duty and be within the general Twain Harte area, going no farther than 20 minutes travel time away from the District office.

2011.42 The Duty Operator will promptly respond to all calls received by any means. All District pager call outs will be considered an emergency requiring an immediate response and shall not be ignored.

2011.43 The Duty Operator will perform a daily pager test to insure its proper operation and routinely check the cell phone voice mail system.

2011.44 The Duty Operator will receive compensation in addition to his/her regular compensation at the current rate established by the Board of Directors, as detailed in THCSD Policy 2010.

TWAIN HARTE COMMUNITY SERVICES DISTRICT
Policy and Procedure Manual

POLICY TITLE: On-Call Duty
POLICY NUMBER: 2011
ADOPTED: October 11, 2007
AMENDED:
LAST AMENDED:

2011.10 PURPOSE

Due to the potential health and safety risks that can be caused by emergencies in water and wastewater operations, the District must have Operators available and on-call after normal working hours, including nights, weekends and holidays. This Policy establishes requirements for an On-Call Duty system that requires Operators to be available twenty-four (24) hours a day to respond to any emergency which may arise.

2011.20 SCHEDULING

The Operations Manager will be responsible to create and post an On-Call Duty schedule for operations and maintenance employees that provides continuous on-call coverage of off-shift, night, weekend and holiday emergency work. The schedule will rotate assignments to be fair to all employees. Any employee so scheduled will be on-call as scheduled, including holidays. The Operations Manager shall be responsible to create clear guidelines to address schedule conflicts, trade requests, leaves of absence, etc.

2011.30 ON-CALL DUTY REQUIREMENTS

The general On-Call Duty requirements are listed below. The Operations Manager shall have authority to add to or clarify these requirements to best serve the District's operational needs; however, any additions that constitute a potential change in wages, hours or work conditions.

1. The District shall have at least two Operators on-call during normal non-working hours. Only certain emergencies will require response from both on-call Operators. The Operations Manager will be responsible to determine who is the primary response Operator and who is the back-up Operator and may also identify the types of calls that require response by any or all of the Operators assigned to On-Call Duty.

2. Operators assigned to On-Call Duty may use time spent while on-call primarily for their own benefit; however, they must be accessible by telephone or pager at all times.

3. Operators assigned to On-Call Duty shall promptly respond to emergency calls and must report to the District within 30 minutes whenever needed. No after hours calls or pages shall be ignored.

4. Operators assigned to On-Call Duty must remain fit for duty at all times. This includes refraining from use of alcohol and other substances that inhibit the performance of work.

2011.40 ON-CALL DUTY COMPENSATION

2011.41 On-Call Pay. Operators assigned to On-Call Duty shall receive a daily stipend, whether or not they are called out for service. Stipend rates shall be negotiated and established in a Board-approved Union Labor Contract.

2011.42 Call-Out Pay. Operators called back to work after the regular work shift (call-out) shall be entitled to call-out pay, which is a minimum of two (2) hours of overtime. Call-out pay shall be the subject to the following requirements:

1. Once an employee is dispatched to respond to a call-out, time is counted as overtime and is paid at on and on-half (1 ½) times the employee's normal hourly rate. Time begins when the employee gets the call and starts travel to the work site and ends when the employee returns home. The employee shall record the date, time, reason for call-out, and the amount of call-out duty worked.

2. Special tours of duty scheduled in advance (24-hour notice) are not considered call-out hours for purposes of this section.

3. An employee need not be assigned to On-Call Duty to receive call-out compensation.

TWAIN HARTE COMMUNITY SERVICES DISTRICT
Policy and Procedure Manual

POLICY TITLE: On-Call Duty
POLICY NUMBER: 2011
ADOPTED: October 11, 2007
AMENDED:
LAST AMENDED:

2011.10 PURPOSE

Due to the potential health and safety risks that can be caused by emergencies in water and wastewater operations, the District must have Operators available and on-call after normal working hours, including nights, weekends and holidays. ~~In order to insure that no emergency within District facilities goes unattended, an~~This Policy establishes requirements for an On-Call Duty system ~~On-Call Duty Operator system has been established. This system requires that at least two District Operations or Maintenance employees~~ that requires Operators to be available twenty-four (24) hours a day to respond to any emergency which may arise.

2011.20 SCHEDULING

The Operations Manager will be responsible to create and post an On-Call Duty ~~Operator~~ schedule for operations and maintenance employees ~~to~~ that provides continuous on-call coverage of off-shift, night, weekend and holiday emergency work. The schedule will rotate assignments to be fair to all employees. Any employee so scheduled will be on-call as scheduled, including holidays. The Operations Manager shall be responsible to create clear guidelines to address schedule conflicts, trade requests, leaves of absence, etc.~~**2011.30** It is the scheduled Duty Operator's responsibility to insure that coverage is available during all assigned off-shift hours. If an employee has a conflict with the schedule or is otherwise unable to maintain coverage, it is that person's responsibility to get another qualified employee to cover time away from the District and to inform the Operations Manager of the substitution.~~

~~**2011.31** Under non-emergency circumstances, all requests for schedule changes or substitutions should be in writing and receive prior approval by the Operations Manager or his/her designee.~~

~~**2011.32** In the event an emergency substitution is needed during off-shift~~

~~hours, the Duty Operator requesting the substitution must arrange with someone else to take his/her place and note the substitution in the Duty Operator Shift Log. The substituting employee will immediately notify the Operations Manager or his/her designee.~~

~~**2011.40**~~
2011.30 ON-CALL DUTY REQUIREMENTS

The ~~On-Call Duty Operator~~general On-Call Duty requirements are listed below. The Operations Manager shall have authority to add to or clarify these requirements to best serve the District's operational needs; however, any additions that constitute a potential change in wages, hours or work conditions. ~~will have the following responsibilities:~~

1. The District shall have at least two Operators on-call during normal non-working hours. Only certain emergencies will require response from both on-call Operators. The Operations Manager will be responsible to determine who is the primary response Operator and who is the back-up Operator and may also identify the types of calls that require response by any or all of the Operators assigned to On-Call Duty.

2. Operators assigned to On-Call Duty may use time spent while on-call primarily for their own benefit; however, they must be accessible by telephone or pager at all times.

3. Operators assigned to On-Call Duty shall promptly respond to emergency calls and must report to the District within 30 minutes whenever needed. No after hours calls or pages shall be ignored.

4. Operators assigned to On-Call Duty must remain fit for duty at all times. This includes refraining from use of alcohol and other substances that inhibit the performance of work.

~~1.~~

~~**2011.41** The assigned Duty Operator will be available by the District's emergency pager. When on call, the Duty Operator shall be free to utilize his/her time as desired, but must remain fit for duty and be within the general Twain Harte area, going no farther than 20 minutes travel time away from the District office.~~

~~**2011.42** The Duty Operator will promptly respond to all calls received by any means. All District pager call outs will be considered an emergency requiring an immediate response and shall not be ignored.~~ ~~**2011.43** The Duty Operator will perform a daily pager test to insure its proper operation and routinely check the cell phone voice mail system.~~

2011.40 ON-CALL DUTY COMPENSATION

2011.414 On-Call Pay. Operators assigned to On-Call Duty shall receive a daily stipend, whether or not they are called out for service. Stipend rates shall be negotiated and established in a Board-approved Union Labor Contract. ~~The Duty Operator will receive compensation in addition to his/her regular compensation at the current rate established by the Board of Directors, as detailed in THCSD Policy 2010.~~

2011.42 Call-Out Pay. Operators called back to work after the regular work shift (call-out) shall be entitled to call-out pay, which is a minimum of two (2) hours of overtime. Call-out pay shall be the subject to the following requirements:

1. Once an employee is dispatched to respond to a call-out, time is counted as overtime and is paid at on and on-half (1 ½) times the employee's normal hourly rate. Time begins when the employee gets the call and starts travel to the work site and ends when the employee returns home. The employee shall record the date, time, reason for call-out, and the amount of call-out duty worked.

2. Special tours of duty scheduled in advance (24-hour notice) are not considered call-out hours for purposes of this section.

~~1.~~3. An employee need not be assigned to On-Call Duty to receive call-out compensation.

TWAIN HARTE COMMUNITY SERVICES DISTRICT
Policy and Procedure Manual

POLICY TITLE: **Holidays**
POLICY NUMBER: **2030**
ADOPTED: **October 11, 2007**
AMENDED: **July 10, 2008**
AMENDED: **September 9, 2010**

2030.10 This policy shall apply to all employees.

2030.20 The following days shall be recognized and observed as paid holidays:

New Year's Eve
New Year's Day
Martin Luther King Day
President's Day
Memorial Day
Independence Day
Labor Day
Veteran's Day
Thanksgiving Day
Friday after Thanksgiving Day
Christmas Eve
Christmas Day

2030.30 In addition to those days listed above as recognized and observed as paid holidays, all District employees shall be provided paid holiday time off according to the following schedule:

2030.31 One (1) personal leave day (birthday/floating holiday) per calendar year, taken one full day at a time.

2030.32 Any day declared as a holiday by the President of the United States or Governor of the state of California.

2030.33 Any day declared a holiday at the discretion of the General Manager for the District. With the exchange of Columbus Day for Martin Luther King Day, the District shall retain Columbus Day as a District holiday for 2008.

2030.40 All regular full time employees shall receive one (1) day's pay for each of the holidays

listed above.

2030.41 Regular part time employees shall receive (1) day's pay for holidays that fall on their scheduled work days.

2030.50 Whenever a holiday falls on Saturday, the preceding Friday shall be observed as the holiday. Whenever a holiday falls on Sunday, the following Monday shall be observed as the holiday.

2030.60 When an employee is taking an authorized leave with pay when a holiday occurs, said holiday shall not be charged against said leave with pay.

2030.70 If any employee works on any of the holidays listed above, he/she shall, in addition to his/her holiday pay, be paid for all hours worked at the rate of time and one-half (1 ½) his/her regular rate of pay, or as otherwise specified under Policy 2010, Employee Compensation, Hours of Work and Overtime.

2030.80 Fire Personnel: Due to the nature of a fire department and staffing requirements, holidays must be covered. Fulltime shift employees will cover the department, but will receive 6 hours of additional pay per pay period as compensation. Where the employee actually works the calendar (actual) day of a holiday listed above, they will receive one-half time for the day worked which is equivalent to: (24 hours times half time rate of normal salary).

TWAIN HARTE COMMUNITY SERVICES DISTRICT
Policy and Procedure Manual

POLICY TITLE: **Holidays**
POLICY NUMBER: **2030**
ADOPTED: **October 11, 2007**
AMENDED: **7/10/2008, 7/9/2010**
LAST AMENDED: **September 9, 2010**

2030.10 PURPOSE

This ~~policy shall apply to all employees.~~ Policy identifies and establishes requirements for paid holidays for all Regular Full-time and Part-time Benefited District employees.

2030.20 PAID HOLIDAYS

The following days shall be recognized and observed as paid holidays:

- New Year's Eve
- New Year's Day
- Martin Luther King Day
- President's Day
- Memorial Day
- Juneteenth
- Independence Day
- Labor Day
- Columbus Day
- Veteran's Day
- Thanksgiving Day
- Friday after Thanksgiving Day
- Christmas Eve
- Christmas Day

Formatted: Tab stops: Not at 0.5"

2030.30 ADDITIONAL PAID HOLIDAYS

In addition to those days listed above as recognized and observed as paid holidays, all Regular Full-time and Part-time Benefited District employees shall be provided paid holiday time off ~~according to the following schedule~~as follows:

1. ~~**2030.31**~~ One (1) personal leave day (birthday/floating holiday) per calendar year, taken one full day at a time.

Formatted: Indent: Left: 0.38", Space After: 12 pt

2. Any day declared as a holiday by the President of the United States or Governor of the state of California.

~~1.~~3. Any day declared a holiday at the discretion of the General Manager for the District. ~~With the exchange of Columbus Day for Martin Luther King Day, the District shall retain Columbus Day as a District holiday for 2008.~~

Formatted: Indent: Left: 0.38", Space After: 0 pt

2030.40 HOLIDAY PAY REQUIREMENTS

Holiday pay shall be subject to the following requirements:

1. ~~All regular~~ Regular ~~full~~ Full-time Benefited employees (non-fire employees only) shall receive one (1) day's pay for each of the holidays listed above.
2. Regular ~~part~~ Part-time Benefited employees (non-fire employees only) shall receive one (1) day's pay for holidays that fall on their scheduled work days. One day will be based upon their normal schedule that day and shall not exceed eight (8) hours.
3. Due to constant staffing requirements for emergency response, Fire Division employees must work on holidays. Regular Full-time Benefited Fire Division employees will receive eight (8) hours pay for holidays when off duty and one and one-half (1 ½) times their normal rate of pay when on duty. Payment of such holiday pay will be made in the same pay period in which the holiday falls. This does not apply to exempt employees.
4. When an employee is taking authorized paid leave (i.e. vacation) when a holiday occurs, the employee will receive holiday pay and will not be required to use the authorized paid leave account.

Formatted: Space After: 12 pt

~~1.~~5. If any non-fire employee works on a holiday, he/she shall, in addition to his/her holiday pay, be paid for all hours worked at the rate of time and one-half (1 ½) his/her regular rate of pay, or as otherwise specified under Policy #2010, Employee Compensation, Hours of Work and Overtime. This does not apply to exempt employees.

Formatted: Space After: 0 pt

2030.50 HOLIDAY SCHEDULING

Whenever a holiday falls on Saturday, the preceding Friday shall be observed as the holiday. Whenever a holiday falls on Sunday, the following Monday shall be observed as the holiday. As an exception, the General Manager may propose to the Board that holidays be observed on different days to benefit employees. All such proposals shall be subject to approval by the Board when it adopts the annual Board Calendar.

~~**2030.60** When an employee is taking an authorized leave with pay when a holiday occurs, said holiday shall not be charged against said leave with pay.~~

~~**2030.70** If any employee works on any of the holidays listed above, he/she shall, in addition to his/her holiday pay, be paid for all hours worked at the rate of time and one-~~

half (1 ½) his/her regular rate of pay, or as otherwise specified under Policy 2010, Employee Compensation, Hours of Work and Overtime.

2030.80 Fire Personnel: Due to the nature of a fire department and staffing requirements, holidays must be covered. Fulltime shift employees will cover the department, but will receive 6 hours of additional pay per pay period as compensation. Where the employee actually works the calendar (actual) day of a holiday listed above, they will receive one-half time for the day worked which is equivalent to: (24 hours times half time rate of normal salary).

TWAIN HARTE COMMUNITY SERVICES DISTRICT
Policy and Procedure Manual

POLICY TITLE: Holidays
POLICY NUMBER: 2030
ADOPTED: October 11, 2007
AMENDED: 7/10/2008, 7/9/2010
LAST AMENDED: September 9, 2010

2030.10 PURPOSE

This Policy identifies and establishes requirements for paid holidays for all Regular Full-time and Part-time Benefited District employees.

2030.20 PAID HOLIDAYS

The following days shall be recognized and observed as paid holidays:

- New Year's Eve
- New Year's Day
- Martin Luther King Day
- President's Day
- Memorial Day
- Juneteenth
- Independence Day
- Labor Day
- Columbus Day
- Veteran's Day
- Thanksgiving Day
- Friday after Thanksgiving Day
- Christmas Eve
- Christmas Day

2030.30 ADDITIONAL PAID HOLIDAYS

In addition to those days listed above as recognized and observed as paid holidays, all Regular Full-time and Part-time Benefited District employees shall be provided paid holiday time off as follows:

1. One (1) personal leave day (birthday/floating holiday) per calendar year, taken one full day at a time.

2. Any day declared as a holiday by the President of the United States or Governor of the state of California.

3. Any day declared a holiday at the discretion of the General Manager for the District.

2030.40 HOLIDAY PAY REQUIREMENTS

Holiday pay shall be subject to the following requirements:

1. Regular Full-time Benefited employees (non-fire employees only) shall receive one (1) day's pay for each of the holidays listed above.
2. Regular Part-time Benefited employees (non-fire employees only) shall receive one (1) day's pay for holidays that fall on their scheduled work days. One day will be based upon their normal schedule that day and shall not exceed eight (8) hours.
3. Due to constant staffing requirements for emergency response, Fire Division employees must work on holidays. Regular Full-time Benefited Fire Division employees will receive eight (8) hours pay for holidays when off duty and one and one-half (1 ½) times their normal rate of pay when on duty. Payment of such holiday pay will be made in the same pay period in which the holiday falls. This does not apply to exempt employees.
4. When an employee is taking authorized paid leave (i.e. vacation) when a holiday occurs, the employee will receive holiday pay and will not be required to use the authorized paid leave account.

5. If any non-fire employee works on a holiday, he/she shall, in addition to his/her holiday pay, be paid for all hours worked at the rate of time and one-half (1 ½) his/her regular rate of pay, or as otherwise specified under Policy #2010, Employee Compensation, Hours of Work and Overtime. This does not apply to exempt employees.

2030.50 HOLIDAY SCHEDULING

Whenever a holiday falls on Saturday, the preceding Friday shall be observed as the holiday. Whenever a holiday falls on Sunday, the following Monday shall be observed as the holiday. As an exception, the General Manager may propose to the Board that holidays be observed on different days to benefit employees. All such proposals shall be subject to approval by the Board when it adopts the annual Board Calendar.

TWAIN HARTE COMMUNITY SERVICES DISTRICT
Policy and Procedure Manual

POLICY TITLE: **Management Leave**
POLICY NUMBER: **2032**
ADOPTED: **November 13, 2014**
REVISIONS:

2032.10 This policy shall apply only to exempt employees.

2032.20 According to District Policy #2080, exempt employees are not eligible for overtime pay under any circumstances. In recognition that exempt employees often must be available outside of normal working hours and are often required to work more than the expected minimum forty hours per week, each exempt employee will be provided sixteen (16) hours of paid time off per fiscal year. Such leave will be made available to each exempt employee at the beginning of each fiscal year.

2032.30 The General Manager may grant up to sixteen (16) hours of additional paid leave per fiscal year per exempt employee to reward exemplary performance. The granting of such leave and the amount of leave awarded, if any, is at the discretion of the General Manager. Leave amounts may be granted at any time and are not required to be granted equally amongst employees.

2032.40 Management leave does not constitute guaranteed time off and requires the pre-approval of the General Manager.

2032.50 Introductory Employees are not eligible for management leave until they have successfully completed the introductory period.

2032.60 All management leave balances will expire at the end of the fiscal year if not used. Management leave may not be cashed out.

2032.70 Management leave must be taken in increments of four hours.

TWAIN HARTE COMMUNITY SERVICES DISTRICT
Policy and Procedure Manual

POLICY TITLE: **Management Leave**
POLICY NUMBER: **2032**
ADOPTED: **November 13, 2014**
AMENDED:
LAST AMENDED:

2032.10 PURPOSE

According to District Policy #2080, exempt employees are not eligible for overtime pay under any circumstances. In recognition that exempt employees often must be available outside of normal working hours and are frequently required to work more than the expected minimum forty hours per week, this Policy provides a system of providing Management Leave to exempt employees.

2032.20 MANAGEMENT LEAVE REQUIREMENTS

Management Leave shall be provided to exempt employees based on the following:
e

1. Only Regular Full-time and Part-time Benefited, exempt employees shall be eligible to receive Management Leave.

2. Introductory Employees are not eligible for Management Leave until they have successfully completed the introductory period.

3. Each Regular Full-time and Part-time benefited, exempt employee will be provided two (2) days of paid time off per fiscal year as Management Leave. For Part-time Benefited employees a “day” will be based on their normal work schedule. Such leave will be made available to each exempt employee at the beginning of each fiscal year.

4. Management Leave balances will expire at the end of the fiscal year if not used.

5. Management Leave may not be cashed out.

6. Use of Management Leave does not constitute guaranteed time off and requires the pre-approval of the General Manager.

2032.30 PERFORMANCE INCENTIVE MANAGEMENT LEAVE

The General Manager may grant up to two (2) days of additional paid leave per fiscal

year per exempt employee to reward exemplary performance. The granting of such leave and the amount of leave awarded, if any, is at the discretion of the General Manager. Leave amounts may be granted at any time and are not required to be granted equally amongst employees.

TWAIN HARTE COMMUNITY SERVICES DISTRICT
Policy and Procedure Manual

POLICY TITLE: Management Leave
POLICY NUMBER: 2032
ADOPTED: November 13, 2014
AMENDED:
LAST AMENDED:

2032.10 PURPOSE

According to District Policy #2080, exempt employees are not eligible for overtime pay under any circumstances. In recognition that exempt employees often must be available outside of normal working hours and are frequently required to work more than the expected minimum forty hours per week, this Policy provides a system of providing Management Leave to exempt employees.
~~This policy shall apply only to exempt employees.~~

2032.20 MANAGEMENT LEAVE REQUIREMENTS

Management Leave shall be provided to exempt employees based on the following:
~~According to District Policy #2080, exempt employees are not eligible for overtime pay under any circumstances. In recognition that exempt employees often must be available outside of normal working hours and are often required to work more than the expected minimum forty hours per week,~~
e

1. Only Regular Full-time and Part-time Benefited, exempt employees shall be eligible to receive Management Leave.

2. Introductory Employees are not eligible for Management Leave until they have successfully completed the introductory period.

3. E~~e~~ach Regular Full-time and Part-time benefited, exempt employee will be provided ~~sixteen (16) hours~~two (2) days of paid time off per fiscal year as Management Leave. For Part-time Benefited employees a "day" will be based on their normal work schedule. Such leave will be made available to each exempt employee at the beginning of each fiscal year.

4. Management Leave balances will expire at the end of the fiscal year if not used.

5. Management Leave may not be cashed out.

~~1.~~6. Use of Management Leave does not constitute guaranteed time off and requires the pre-approval of the General Manager.

2032.30 PERFORMANCE INCENTIVE MANAGEMENT LEAVE

The General Manager may grant up to ~~sixteen (16) hours~~two (2) days of additional paid leave per fiscal year per exempt employee to reward exemplary performance. The granting of such leave and the amount of leave awarded, if any, is at the discretion of the General Manager. Leave amounts may be granted at any time and are not required to be granted equally amongst employees.

~~**2032.40** Management leave does not constitute guaranteed time off and requires the pre-approval of the General Manager.~~

~~**2032.50** Introductory Employees are not eligible for management leave until they have successfully completed the introductory period.~~

~~**2032.60** All management leave balances will expire at the end of the fiscal year if not used. Management leave may not be cashed out.~~

~~**2032.70** Management leave must be taken in increments of four hours.~~