Ref: 20-6893

AGENDA

HUMAN RESOURCES COMMITTEE MEETING
LEUCADIA WASTEWATER DISTRICT

November 7, 2019 – 9:30 AM
1960 La Costa Avenue, Carlsbad, CA 92009

---

1. **Call to Order**

2. **Roll Call**

3. **Public Comment**

4. **New Business**
   A. Adopt Resolution No. 2319 Updating LWD's Electronic Media Usage Policy. (Pages 2-11)

5. **Information Items**
   None.

6. **Directors' Comments**

7. **General Manager's Comments**

8. **Adjournment**

Ref: 20-6892

MEMORANDUM

DATE: November 4, 2019

TO: Human Resources Committee

FROM: Paul J. Bushee, General Manager

SUBJECT: **Resolution No. 2319 Updating LWD's Electronic Media Usage Policy**

RECOMMENDATION:

1. Adopt Resolution No. 2319 Updating LWD's Electronic Media Usage Policy.

2. Discuss and take other action as appropriate.

DISCUSSION:

Tactical Goal: People/ Administrative Policy Updates/Review

LWD's current Electronic Media Usage Policy was developed as a supplemental policy to LWD's Human Resources Policy Manual during January 2011 and later revised in October 2013. Due to the rapid changing nature of technology, this policy is outdated and requires revisions to meet current administrative procedures.

Below please find a summary of the policy's revisions:

Section 1: Background

- This section includes various minor changes to reflect updated technology language, grammatical updates, and language that is consistent with the District's Human Resources Policy Manual and Anti-Harassment/Discrimination Policy.

Sections 2-4: Scope

- These sections include language that clarifies who the policy applies to, updated IT definitions, and revisions to reflect current administrative procedures.

The policy also includes Attachment A, E-Mail Guidelines. The revised guidelines now include language that explains how to recognize and avoid phishing scams and it also provides examples of types of phishing emails. The purpose of adding this language will help employees identify phishing emails to prevent computer viruses.

The proposed Resolution No. 2319 which amends the Electronic Media Usage Policy is provided as Attachment 1 and contains the full strikeout text of the proposed policy.

Therefore, staff requests that the HRC recommend that the Board of Directors adopt Resolution No. 2319 amending the Electronic Media Usage Policy, or provide direction as appropriate.

Staff will provide a detailed overview of the changes at the upcoming meeting.

Attachment
th:PJB

RESOLUTION NO. 2319

A RESOLUTION OF THE BOARD OF DIRECTORS OF THE LEUCADIA WASTEWATER DISTRICT ADOPTING THE AMENDED ELECTRONIC MEDIA USAGE POLICY

Whereas, the Electronic Media Usage Policy was established during January 2011 and it was last updated during October 2013; and

Whereas, the Board of Directors desire to amend the Electronic Media Usage Policy to reflect the changing nature of technology and be consistent with current procedures and with District's Human Resources Policy Manual.

NOW, THEREFORE, it is hereby resolved as follows:

1. The LWD Board of Directors adopts the amended Electronic Media Usage Policy attached hereto as Exhibit "A" and directs that it be implemented consistent with related District policies.

Passed and Adopted by the Board of Directors of the Leucadia Wastewater District this 13th day of November 2019 by the following vote:

AYES:

NOES:

ABSENT:

ABSTAIN:

_____
David Kulchin, President

Attest:

_____
Paul J. Bushee, Secretary /Manager

Exhibit A

Electronic Media Usage Policy Manual

LEUCADIA WASTEWATER DISTRICT

ELECTRONIC MEDIA USAGE POLICY

Ref: 20-~~DRAFT~~6891

1. Background

The Leucadia Wastewater District (LWD) makes every effort to provide its employees with technology-based resources in order to conduct official business more effectively. In this regard, LWD has installed personal computers, local area networks (LANs), electronic mail (~~email~~e-mail) and access to the ~~Internet~~internet. In addition, ~~District~~ authorized staff may utilize ~~pagers and digital cellular telephones~~cell phones and tablets~~iPads~~ ~~with~~ which include~~s~~ similar features as a computer, such as; internet access, sending and receiving ~~email~~e-mail~~s~~, text messages, photographs and multimedia messages. ~~voicemail features.~~

All District provided electronic media resources, including ~~email~~e-mail systems, ~~Internet~~internet access, tablets, ~~and~~ ~~telephones~~ cell phones and ~~(including~~ voicemail~~)~~, etc. are intended to be used primarily for business purposes. Any personal use must be of an incidental nature, and not interfere with business activities~~, must not involve solicitation, and must not potentially embarrass the District, its residents, its ratepayers, or its employees.~~ Electronic devices and services are provided primarily for District use. Limited, occasional or incidental use of electronic devices (sending or receiving) for personal, non-business purposes is understandable and acceptable. However, employees need to demonstrate a sense of responsibility and may not abuse this.

Electronic devices may not be used for knowingly transmitting, retrieving or storage of any communications of a discriminatory or harassing nature, or which are derogatory to any individual or group, or which are obscene or X-rated communications, or are of a defamatory or threatening nature, or for "chain letters," or for any other purpose which is illegal or against District policy or contrary to the District's interest.

2. Scope

This policy is supplemental to section 3.12 of the Human Resources Policy Manual and ~~statement~~ applies to all District Board Members~~,~~ and employees~~, contractors an~~d consultants.

All vendors, contractors, consultants and temporary employees are required to abide by the aforementioned policy items when conducting business on District property, or using District equipment. When you are remotely connected to District systems, you are considered to be both on District property and using District equipment.

3. Definitions

Attachment: An application specific file, such as a Word or Excel document, that is transported with an e-mail message. The recipient must have suitable software for viewing the attachment.

E-mail: A message, possibly with attachments~~, composed on a computer and received by a computer. A network, potentially including the Internet, is the transmission medium~~ distributed by electronic means from one computer user to one or more recipients via network.

Text Message: An electronic communication/message sent and received by a mobile phone.

Internet: A worldwide network of computers, adhering to universal standards, that is capable of exchanging data with each other.

LAN: Local Area Network. The District's internal network is an example.

Phishing: A cybercrime in which a target or targets are contacted by e-mail, telephone, or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data.

4. General

~~1.~~4.1. The General Manager~~, Administrative Services Manager or Technical Services Manager~~ or his/her designee must authorize ~~Internet~~internet use. Each employee will be responsible for the security of his/her account password and held responsible for the use or misuse of the account.

~~2.~~4.2. All data created on all District resources/electronic devices, including printed material and e-mail, are owned by the District. Management reserves the right to monitor and access all ~~email~~ files created, stored or received on all District systems, at any time, with no prior notice. There is **NO** expectation of personal privacy in the use of the ~~Internet~~internet, text messages and ~~email~~e-mail. These mediums are subject to archival policies and any scrutiny normally afforded to paper files and documents covering the same subject matter.

~~3.~~4.3. The District is not responsible for items originating in the ~~Internet~~internet.

~~4.~~4.4. The District reserves the right to restrict access to portions of the ~~Internet~~internet.

~~5.~~4.5. Relevant, existing District policies apply to ~~Internet~~internet usage. This includes but is not limited to:

- Internet and District provided resources shall not be used to obtain or disseminate any sexually oriented material.
- The use of these ~~Internet~~resources to send threatening, slanderous, racially and/or sexually harassing messages is prohibited.
- The use of any District resource for personal gain is prohibited.

~~• Copyrighted software shall not be downloaded unless it is a "demo" package provided by the vendor and approved by the Technical Services Manager.~~

- No programs or software may be installed on District computer systems (office pc or the network) without the written authorization of the Technical Services Manager. The Technical Services Manager or Field Services Superintendent shall authorize all modifications or software installations on the District SCADA network.

- All downloaded data and software, or disks containing data originating outside LWD's network ~~must~~will be scanned for viruses prior to opening and use.

- ~~Unencrypted, confidential documents must never be sent via e-mail.~~

When using ~~e-mail~~electronic media, remember that each employee represents the District. Do not speak for the District unless authorized to do so. In addition, employees should take reasonable care to prevent introduction or spread computer viruses/malware into or through LWD communication and information systems and equipment. If an employee(s) receives suspicious phishing ~~email~~e-mail(s)/text messages, he/she shall not open the ~~email~~e-mail/ text messages or any attachments. Employees shall delete the ~~email~~e-mail/text message and block future

- ~~mail~~e-mails from the sender or forward the ~~email~~e-mail to the District's contracted IT support desk to verify if the ~~email~~e-mail is safe to open. To assist~~s~~ employees with the use of ~~email~~e-mails and how to identify phishing ~~email~~e-mails, guidelines are attached for additional information.

~~6.~~

5. Enforcement

A violation of standards, procedures or guidelines established pursuant to this policy shall be presented to District management for appropriate action and may result in disciplinary action including termination. If, based on the District's audit and review of any employee's ~~I~~internet usage, the District has reason to believe that an employee's use of the ~~I~~internet violates the law in any manner, the District may refer the matter to the proper authorities for prosecution.

6. Frequency of Review

This policy shall~~will~~ be provided to new employees and reviewed by each employee with~~and~~ his/her immediate supervisor prior to the first use of any District furnished electronic media, including ~~I~~internet and ~~email~~e-mail related resources. New updates to the policy shall be sent to all employees.

7. Policy Coordinator

Administrative Services ~~Manager~~Supervisor

Date of Last Revision/Review
January 2011
October 2013
~~September~~November 2019

ELECTRONIC MEDIA USAGE AUTHROIZATION REQUEST

End-User Information

Director/Employee: _____

~~Dept.:~~ Dept.: _____

Required/Requested ~~-~~Services or Equipment: ___ ~~Internet~~ E-mail ___ Internet Access

~~____ Pager~~ ____ Cell~~ular~~ Phone ____ iPad ___ SCADA Network

Electronic Usage Policy Review

I have received a copy of the LWD Electronic Usage Policy and agree to abide by its provisions.

Director/Employee Signature: _____

Date: _____

I have reviewed the LWD Electronic Usage Policy with this employee.

Manager/Supervisor: _____

Date: _____

LWD Electronic Media
Usage Authorization

Authorizing Signature: _____

Date: _____

Instructions:

1. Fill out the above as required.
2. Review the ~~Internet Electronic Usage~~Electronic Media Usage Policy with the employee requiring authorization.
3. Return signed form to the Administrative Services Supervisor~~ASM~~.

ATTACHMENT A

E-MAIL GUIDELINES

The following section is NOT part of the ~~I~~internet Usage Policy. It contains information and hints that will assist you in the use of ~~I~~internet based ~~email~~e-mail.

General Guidelines

1. ~~Email~~E-mail is not secure. Never include in an ~~email~~e-mail anything you want to keep secure and confidential.

2. Be careful when sending attachments. The recipient may not have the software to read it. An example of this is sending a Microsoft Word document to a site that only uses WordPerfect.

3. Don't send large files over ~~10~~9MB via ~~email~~e-mail unless necessary. The recipient may have a "slow" ~~I~~internet connection and/or may be paying for each received byte. It may be necessary to send a large file via file-sharing software (e.g.: Dropbox, Google Drive, ~~Sharepoint~~SharePoint etc.) or~~through~~ surface mail rather than ~~email~~e-mail.

4. Include a signature block at the bottom of ~~email~~e-mail messages. This usually contains the sender's name, ~~email~~e-mail address and voice/fax phone numbers as well as District approved Confidentiality Notice. Outlook ~~may~~ can be configured to add this automatically.

5. Delivery of ~~email~~e-mail is not 100% reliable. For important items, notify senders that their ~~email~~e-mail was received and when a response can be expected.

6. Be careful of punctuation and spelling. Always use the built-in checkers.

7. All ~~email~~e-mail~~s~~ that reside~~s~~ on the ~~email~~e-mail server are~~is~~ backed up to ~~magnetic tape~~a server archive. Note that all messages may be available for audit, via the backup, even if the online version is erased.

How to Recognize and Avoid Phishing Scams

Phishing ~~email~~e-mails and text messages may look like they're from a company you know or trust. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store. Phishing ~~email~~e-mails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you must confirm some personal information
- include a ~~fake invoice~~fake invoice
- want you to click on a link to make a payment

- say you're eligible to register for a ~~government~~government refund
- offer a coupon for free items ~~coupon for free stuff~~
- say you are eligible to receive a lump sum of money

~~7.~~

What to Do if You Suspect a Phishing ~~Email~~E-mail

Answer the following questions before opening the ~~email~~e-mail(s):

1. Does the District have an account with the company/vendor or know the person that has contacted me? If your answer is no, it could be a phishing scam
2. Do you notice several spelling or grammar errors in the ~~email~~e-mail? If your answer is yes, it could be a phishing scam.
3. Is the sender asking you to update bank or account information? If your answer is yes, it could be a phishing scam.
4. Is it asking you to click on something?

If you suspect any phishing email(s), DO NOT open the email or attachment, and DO NOT respond. Delete it as quickly as possible.

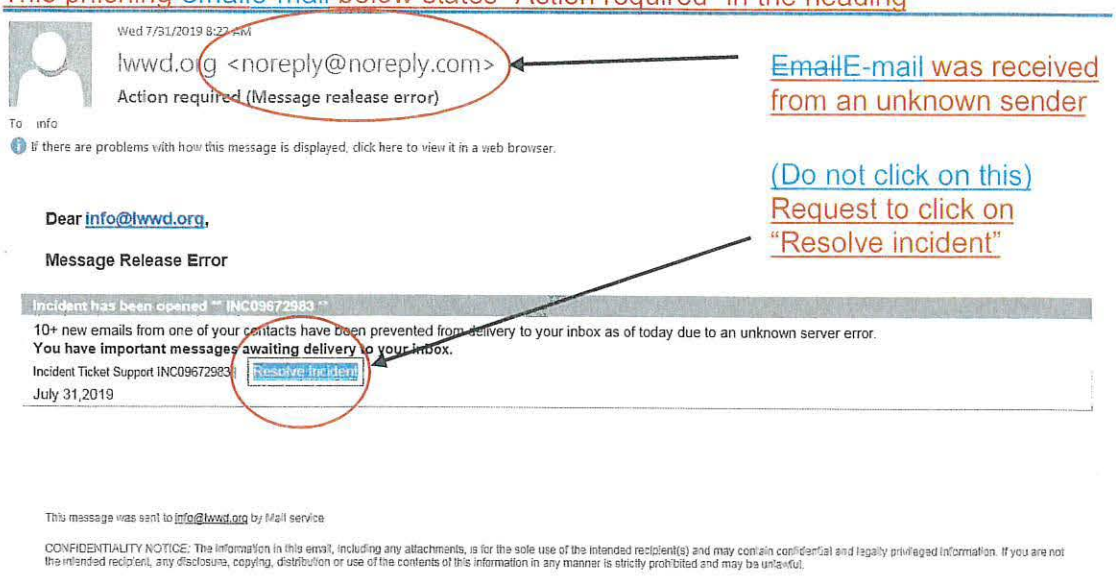
Phishing/Spam ~~Email~~E-mails Examples:

The ~~email~~e-mail below states in the heading under the sender's name "Suspected Spam" and the District security software quarantined this ~~email~~e-mail. Delete these ~~email~~e-mails immediately and do not open.

Symantec Mail Security replaced Payment_copy.zip with this text message. The original text contained an executable file and was quarantined.

ID:EXCH1::SYQ5490475f2
The email message was also quarantined.

This phishing ~~email~~e-mail below states "Action required" in the heading



Message Release Error