Santa Clara Valley Water District

MEMORANDUM

To:	Board of Directors	**From:**	Beau Goldie
Subject:	Misdirecting Response to District Received E-mails	**Date:**	November 13, 2015

This is to inform you of a practice that can misdirect District email responses and what preventative measure you can take. A recent incident was discovered by the District's IT Deputy Administrative Officer in responding to an e-mail from a Board Member (Attachment 1). The e-mail reply would have resulted in the reply being redirected to a third party. Fortunately, the redirection of the reply was detected.

E-mail can be redirected so that the e-mail messages appear to have originated from someone or somewhere other than the actual source, a practice known as "*spoofing*". *Spoofing* is often used by spammers and can be accomplished by changing your "FROM" e-mail address. District's Information Technology has invested in several safeguards to prevent e-mail spoofing of District e-mail addresses. However, we also agree that we cannot fully eliminate it from happening.

While the District's practice is to make appropriate public records open and transparent "spoofing" may result in the inadvertent release of security or confidential information if an e-mail user does not review and confirm the intended e-mail reply address.

We have sent a message to all employees to remind them of the risks in e-mail and the preventative actions that an individual can take (Attachment 2).

If you have any questions please contact me or if you would like or need assistance in understanding email protection measures, please contact Ashu Tikekar at (408) 630-2736.

Chief Executive Officer

/svd
cc: S. Yamamoto, M. King, J. Nava, A. Tikekar

Santa Clara Valley Water District

MEMORANDUM

FC 14 (01-02-07)

TO: Beau Goldie **FROM:** Ashu Tikekar

SUBJECT: Chair Kremen emails **DATE:** November 2nd, 2015

I received an email from Chair Kremen on August 31st, 2015, while on vacation in India. In his email, he requested information about our data and email backups. When I went to reply to his email to let him know that I will convert the email into an IBMR and respond accordingly, I noticed something was strange in the Reply-To-Address. The Reply-To-Address was for Josh Koehn jKoehn@metronews.com. At that point, I did not reply to the email and forwarded that email to Frank Fung and requested him to check if it was a spoofing attempt.

Frank sent an email to Chair Kremen on September 2nd, 2015 to confirm his request, and that he was in receipt of it, and would be addressing the questions shortly. Frank never got a response from Chair Kremen. In the meantime the Clerk of the Board issued an IBMR-I-15-400, and Frank started working to answers all the questions in the IBMR.

I came back to work from my vacation on September 7th, 2015. On September 8th, 2015 I wrote an email to Chair Kremen, once again wanting to confirm if the email of August 31st, 2015 was truly sent by him. This time I also provided him the header information of his original email and highlighted the Reply-To-Address: Josh Koehn jKoehn@metronews.com in red. I did not receive a reply back from Chair Kremen. I also followed up with him about this matter in the parking lot after the Board meeting of September 8th, 2015.

In the meantime, Frank completed the IBMR-I-15-400 and I approved it on September 9th 2015.

Ashu Tikekar
DAO Information Technology Division

Cc: Jesus Nava
Jim Fiedler
Stan Yamamoto

Sudhanshu Tikekar

From: Gary Kremen
Sent: Monday, August 31, 2015 2:23 PM
To: Sudhanshu Tikekar
Subject: Questions on backups

We must do lots of critical business using email / outlook calendar. Correct? Questions:

- Do we have backup software?
- Can people download their own copies of their .pst and other outlook files?
- Which brand of backup software do we use?
- Do we test out the backup restore process?
  - How often?
- Do we copies backup off site?
  - Where do we keep them?
  - Do we use services such as Iron Mountain?
- Do we recycling copies or keep them in read only mode?
- How are deletes of emails handled?
- What happens if someone deletes an email but does not "empty the trash?"
- Who has admin or related access to emails?
- What is our policies in this area?

Gary Kremen | linkedin.com/in/gkremen | +1 415.305.3052 | @GKremen

Santa Clara Valley Water District

FRANK FUNG
Santa Clara Valley Water District
5750 Almaden Expy, San Jose, CA 95118
Phone: (408) 630-2347
Fax: (408) 979-5605
FFUNG@valleywater.org

From: Sudhanshu Tikekar
Sent: Tuesday, September 01, 2015 3:17 AM
To: Frank Fung; Lonnie Spin
Subject: Fwd: Questions on backups

Guys,

Please investigate this. When I went to reply to the below message wanting to tell Gary that Frank will be responding, the reply to address resolved to Josh of Metro News.

Please keep me posted.

Ashu Tikekar
iN Outlook on iPhone

From: Gary Kremen <gkremen@valleywater.org>
Sent: Tuesday, September 1, 2015 6:22 AM
Subject: Questions on backups
To: Sudhanshu Tikekar <stikekar@valleywater.org>

We must do lots of critical business using email / outlook calendar. Correct? Questions:

- Φ0B7 Do we have backup software?
- Φ0B7 Can people download their own copies of their .pst and other outlook files?
- Φ0B7 Which brand of backup software do we use?
- Φ0B7 Do we test out the backup restore process?
  - How often?
- Φ0B7 Do we copies backup off site?
  - Where do we keep them?
  - Do we use services such as Iron Mountain?
- Φ0B7 Do we recycling copies or keep them in read only mode?
- Φ0B7 How are deletes of emails handled?
- Φ0B7 What happens if someone deletes an email but does not "empty the trash?"
- Φ0B7 Who has admin or related access to emails?
- Φ0B7 What is our policies in this area?

Gary Kremen | linkedin.com/in/gkremen | +1 415.305.3052 | @GKremen

Sudhanshu Tikekar

From: Sudhanshu Tikekar
Sent: Tuesday, September 01, 2015 7:07 PM
To: Frank Fung
Subject: RE: Questions on backups

Frank,

Before we respond we need to find out if Gary's email address was spoofed.

Ashu Tikekar
iN Outlook on iPhone

From: Frank Fung <ffung@valleywater.org>
Sent: Wednesday, September 2, 2015 2:47 AM
Subject: RE: Questions on backups
To: Sudhanshu Tikekar <stikekar@valleywater.org>

I am still waiting for the IBMR. In the meanwhile I have drafted the below response.

To prevent against email data loss, the District's email system uses a combination of disk-to-disk and disk-to-tape technology to backup email. Monthly copies of the backup are sent off site to Iron Mountain in Fremont, CA for six (6) months per the District Records Retention Schedule. Based on age of tape, returned copies of the backup tape are either reused or destroyed. The District uses Commvault Simpana software technology for data backup and recovery. Several times a year, IT staff have conducted successful recovery of staff email from backup.

In the past due to technology limitation in supporting large size email storage, the District practiced using Microsoft personal storage table (PST) to provide staff with expandable means in storing older emails. Recent upgrades to the email system and the implementation of email archiving made the need for PST files no longer applicable. IT discourages the use of PST but does not prevent staff from creating their own PST.

Items moved to the Deleted Items folder are not permanently deleted until the folder is emptied. Over time the contents of the Deleted Items folders can consume a large amount of file storage, employees at their own discretion can permanently empty their Deleted Items Folder. Contents in the Deleted Items Folder is recoverable from email archive and/or backup.

Only essential IT staff have administrative access to emails as needed to perform essential duties of managing, maintaining, and operating the District email system. Staff who have administrative access are the engineering systems analyst, two senior information technicians, and the unit manager.

The District e-mail policy, AD 7.5 Information Management Electronic Mail, addresses retention of email, employee compliance obligations, and appropriate use of the email systems, privacy and confidentially of information, email system security, and actions for violation of the policy

Regards

Sudhanshu Tikekar

From: Sudhanshu Tikekar
Sent: Wednesday, September 02, 2015 3:22 PM
To: Frank Fung
Subject: Re: FW: Questions on District Email System

Thanks.

Ashu Tikekar
iN Outlook on iPhone

On Wed, Sep 2, 2015 at 3:18 PM -0700, "Frank Fung" <FFung@valleywater.org> wrote:

If he acknowledges the email that I just sent him then we can assume it was a valid request.

Frank Fung
Santa Clara Valley Water District
408-630-2347

On Wed, Sep 2, 2015 at 3:16 PM -0700, "Sudhanshu Tikekar" <STikekar@valleywater.org> wrote:

Frank,

Are we sure that the email for information was from Gary.? I have sent you earlier emails to check. I think his email address has been spoofed.

Ashu Tikekar
iN Outlook on iPhone

On Wed, Sep 2, 2015 at 1:28 PM -0700, "Frank Fung" <FFung@valleywater.org> wrote:

Ashu

The IBMR response (see attached) requires unclassified staff approval. Please let me know if the response is acceptable.

Regards

FRANK FUNG
Santa Clara Valley Water District
5750 Almaden Expy, San Jose, CA 95118
Phone: (408) 630-2347
Fax: (408) 979-5605
FFUNG@valleywater.org

From: Frank Fung
Sent: Wednesday, September 02, 2015 1:21 PM
To: Gary Kremen
Subject: Questions on District Email System

Good afternoon Gary:

This is Frank Fung, Infrastructure UM, reporting to Ashu Tikekar who has been on vacation the past three weeks. I wanted you to know the COB just issued an IMBR for your questions on the District's email system. I wanted to confirm your request and wanted you to know that I am in receipt of your request and will be addressing your questions shortly.

Regards

FRANK FUNG
Santa Clara Valley Water District
5750 Almaden Expy, San Jose, CA 95118
Phone: (408) 630-2347
Fax: (408) 979-5605
FFUNG@valleywater.org

Sudhanshu Tikekar

From: Sudhanshu Tikekar
Sent: Tuesday, September 08, 2015 3:47 PM
To: Gary Kremen
Cc: Frank Fung; Sudhanshu Tikekar
Subject: FW: Questions on backups

Gary,

I just got back from my vacation. Before we respond to the below questions, I would like to confirm with you that the below email was sent by you as I see in the header information the reply-to: address is different.

Thanks
Ashu

Received: from SRVEXCHMBX2.scvwd.gov ([fe80::c9c6:f5bf:3482:6d80]) by SRVHT2.scvwd.gov ([::1]) with mapi id 14.03.0235.001; Mon, 31 Aug 2015 14:22:31 -0700
Content-Type: application/ms-tnef; name="winmail.dat"
Content-Transfer-Encoding: binary
From: Gary Kremen <GKremen@valleywater.org>
To: Sudhanshu Tikekar <STikekar@valleywater.org>
Subject: Questions on backups
Thread-Topic: Questions on backups
Thread-Index: AQHQ5DMlA7hfPNLEvECzH2zdQBP+Ew==
Date: Mon, 31 Aug 2015 14:22:49 -0700
Message-ID: <31E207D0-47B5-4FBC-8416-E04B53D027CF@valleywater.org>
Reply-To: Josh Koehn <jKoehn@metronews.com>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-Exchange-Organization-SCL: -1
X-MS-TNEF-Correlator: <31E207D0-47B5-4FBC-8416-E04B53D027CF@valleywater.org>
MIME-Version: 1.0
X-MS-Exchange-Organization-AuthSource: SRVHT2.scvwd.gov
X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 04
X-Originating-IP: [10.25.5.165]
X-TM-AS-Product-Ver: SMEX-10.2.0.1135-8.000.1202-21782.005
X-TM-AS-Result: No--32.096700-8.000000-31
X-TM-AS-User-Approved-Sender: No
X-TM-AS-User-Blocked-Sender: No
X-MS-Exchange-Organization-AVStamp-Mailbox: SMEXutTf;1188700;0;This mail has been scanned by Trend Micro ScanMail for Microsoft Exchange;

Santa Clara Valley Water District

SUDHNSHU TIKEKAR
Deputy Administrative Officer - IT
Santa Clara Valley Water District
5750 Almaden Expy, San Jose, CA 95118
Phone: (408) 630-2424
Fax: (408) 979-5605

Santa Clara Valley Water District

BOARD REQUEST RESPONSE (CEO Bulletin)

FC 1500 (12-05-14)

☐ BMR (FORMAL) NO.:	☒ IBMR (INFORMAL) NO.: I-15-0040	ORIGINAL BMR/IBMR DATE: 9/8/2015

STATE REQUEST:

Provide Dir. Kremen answers to the following questions regarding use of email and Outlook calendar:
Do we conduct critical business using email?
Do we have backup software?
Can people download their own copies of their .pst and other Outlook files?
Which brand of backup software do we use?
Do we tests the backup-restore process? How often?
Do we store backup copies offsite? Where? Do we use services such as Iron Mountain?
Do we recycle copies or keep them in read only mode?
How are deleted emails handled?
Who has admin or related access to emails?
What are our policies in this?

REQUESTING DIRECTOR:

☐ Estremera ☐ Hsueh ☐ Keegan ☐ Kennedy ☒ Kremen ☐ LeZotte ☐ Santos

RESPONDING STAFF:	Ext.	Date:	UNCLASSIFIED STAFF APPROVAL:	Ext.	Date:
Frank Fung, Infrastructure UM	2347	9/8/2015	Sudhanshu Tikekar	2424	9/8/2015

POLICY COMPLIANCE:

☒ Response will be e-mailed to 'CEO Bulletin' inbox within 20 days of original BMR/IBMR date[1]

☐ If due date has been previously extended, response will be e-mailed to 'CEO Bulletin' inbox by extended date.

Extended due date:

☐ Request will be delayed. Expected Completion Date:

[1] *The 20-day deadline is an internal Clerk of the Board deadline to ensure items are received by the Board within the 30-day limit set by Board Policy EL-7.9.*

RESPONSE: *(NOTE: For information on how to submit attachments, see below.)*

District email system has become the standard for conducting critical District Business. District employees rely on this system to work on projects. To prevent against email data loss, the District's email system uses a combination of disk-to-disk and disk-to-tape technology to backup email. Monthly copies of the backup are sent off site to Iron Mountain in Fremont, CA for six (6) months per the District's Records Retention Schedule.

District email policy AD 7.5 Information Management Electronic Mail (see Attachment) addresses employee compliance obligations, and appropriate use of the email systems, privacy and confidentially of information, email system security, and actions for violation of the policy.

Based on age of tape, returned copies of the backup tape are either reused or destroyed. The District uses Commvault Simpana software technology for data backup and recovery. Several times a year, IT staff conduct successful recovery of staff email from backup.

In the past due to technology limitation in supporting large size email storage, the District practiced using Microsoft personal storage table (PST) to provide staff with expandable means in storing older emails. Recent upgrades to the email system and the implementation of email archiving made the need for PST files no longer applicable. IT discourages the use of PST but does not prevent staff from creating their own PST. These PST files can reside on the local PC or the shared drives. IT does not back up the local PC but the shared drives are backed up nightly, weekly and monthly and backup tapes are stored offsite for a period of one (1) year.

Items moved to the Deleted Items folder are not permanently deleted until the folder is emptied. Over time the contents of the Deleted Items folders can consume a large amount of file storage, employees at their own discretion can permanently empty their Deleted Items Folder. Contents in the Deleted Items Folder is recoverable from email archive and/or backup.

Only essential IT staff have administrative access to emails as needed to perform essential duties of managing, maintaining, and operating the District email system. Staff who have administrative access are the engineering systems analyst, two senior information technicians, and the unit manager.

For further information, please contact Sudhanshu Tikekar at (408) 630-2424.

Responses should be:

- *Related to achieving a Board policy, if applicable;*
- *Easily understood by the Board and public, e.g., no technical jargon, spell out acronyms, etc.;*
- *Concise—no lengthy explanations unless specifically requested in the BMR/IBMR.*

REQUEST STATUS: ☒ Completed ☐ Update Only

FOR LEGAL USE ONLY

LEGAL COMMENTS:	Name:	Date:
LEGAL FINAL APPROVAL:	Name:	Date:

- *If you have additional documents you would like to provide to the Board pertaining to your response, response should include "additional information has been provided to the Board in the (enter date) non-agenda packet."*
- DO NOT include attachments to this response. As a reminder, the deadline to submit items to the Clerk of the Boards Office for the non-agenda packet is every Tuesday, 5 p.m.
- Please forward an electronic copy indicating appropriate unclassified staff approval to the ***CEO Bulletin Inbox*** no later than Monday, 5 p.m. for inclusion in that week's Bulletin.

Sudhanshu Tikekar

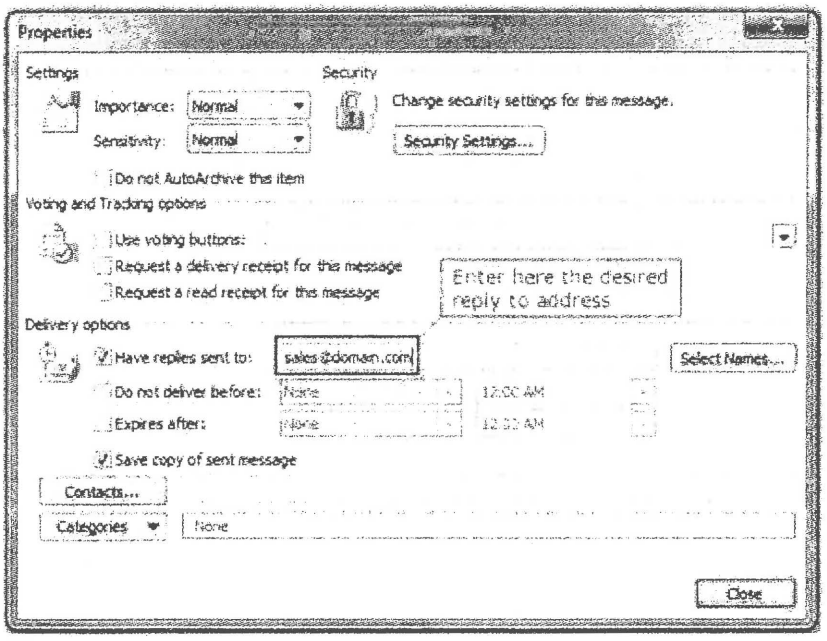
From: Sudhanshu Tikekar
Sent: Friday, October 30, 2015 8:57 AM
To: Sudhanshu Tikekar
Cc: Sudhanshu Tikekar
Subject: How to change Reply To Address

How to change Reply To Address

Office 365 (Outlook 2016 | Outlook 2013 | 2010 for Windows) - Change Reply To Address

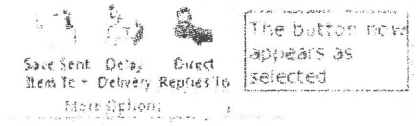
The "Reply To" address is the email address responses will be sent to when a recipient clicks "Reply". By default, the "Reply To" address will be the email address from in Outlook 2013 or Outlook 2010.

1. Start Outlook and click **New Email** or use **Reply**, **Reply All** or **Forward** options for any existing email
2. Move to the **Options** tab on the ribbon and click **Direct Replies To**:
3. In the Properties window that will open, change the email address in the **Have replies sent to:** field



Then click the **Close** button

4. You will now see that the **Direct Replies To** button is highlighted



The reply to this email will be delivered to the email address you entered

Sylvia Van Diemen

From: Employee Communications
Sent: Friday, November 13, 2015 9:01 AM
To: All Users
Subject: From IT: Use of District Email

Employee Communications

From: Sudhanshu Tikekar, Deputy Operating Officer- Information Technology **Date**: Nov. 13, 2015

Re: Use of District Email

Santa Clara Valley Water District provides employees with use of computers, e-mail and digital data devices to conduct the daily work of the District. As part of the normal use of the system, the Information Technology (IT) Division reminds employees of the following:

1. **Be aware of E-mail Message redirection of e-mail sender:**
   When you reply to an e-mail, please verify that you are sending your e-mail response to your intended recipient(s). Make sure to check the e-mail addresses in the To, CC, and BCC fields, to make sure you are replying to the intended party. E-mail client software such as Outlook provide e-mail users the flexibility to redirect responses to their e-mail to a different e-mail address.

2. **Avoid phishing attacks:**
   Phishing scams are designed to obtain or extract personal information from an e-mail respondent. Phishing attackers often use doctored and fraudulent e-mail messages to trick e-mail recipients into divulging private, personal or confidential information, such as credit card numbers, account usernames, passwords, and even social security numbers.

3. **Protect e-mail addresses:**
   Do not divulge your coworkers' e-mail addresses to vendors, friends or others outside this organization. Verify that recipients listed in the To and CC fields should be receiving messages and that you won't be revealing others' e-mail addresses in the process. Don't post your or coworkers' e-mail addresses on Internet forums or bulletin boards, on Usenet groups, in chat rooms, or in other public areas.

4. **Be aware of E-mail Spoofing:**
   E-mail spoofing is the forgery of an e-mail header so that the e-mail message appears to have originated from someone or somewhere other than the actual source. Spoofing is often used by spammers and can be accomplished by the spammer changing your "FROM" e-mail address.
   E-mail spoofing may occur in different forms, but all have a similar result: a user receives e-mail that appears to have originated from one source when it actually was sent from another source. E-mail spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information, such as a password. E-mail spammers often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations.

5. **Be smart about handling attachments:**
   E-mail attachments consume inordinate amounts of e-mail server space and network bandwidth and are often the culprits behind virus outbreaks—but they're often the easiest way to transfer files. Just be sure to follow these guidelines when e-mailing attachments:

a. Don't attach large files to an e-mail, unless necessary; anything over ten to fifteen megabytes shouldn't be sent via e-mail. Instead, use the cloud storage service of the District to share files.
b. Limit the number of files you attach to a message to five or fewer.
c. Save attachments to your hard drive and then delete the e-mail message containing the attachment.
d. Don't open unexpected attachments or those sent by unknown parties.
e. Don't annoy recipients by forwarding attachments they can't access. If an attachment requires a new or less-common application, say so in your message.

6. Other helpful resources and tips:

- http://www.pcworld.com/article/253305/minimize_your_exposure_to_e-mail_spoofing.html
- http://www.huffingtonpost.com/jason-p-stadtlander/e-mail-spoofing-explained-_1_b_6477672.html

If you suspect problems with your e-mail, please contact the IT Hotline immediately or report the issue to ITHelpdesk@valleywater.org .