



# Audit Department

500 S Grand Central Pkwy Ste 5006 • PO Box 551120 • Las Vegas NV 89155-1120  
(702) 455-3269 • Fax (702) 455-3893

Angela M. Darragh, CPA, CFE, CISA, Director

August 17, 2015

Mr. Don Burnette  
Clark County Manager  
500 South Grand Central Parkway, 6th Floor  
Las Vegas, Nevada 89106

Dear Mr. Burnette:

We recently performed a follow-up audit of the Email Service audit dated May 6, 2014. Our objective was to determine whether corrective actions were implemented to address findings included in the original audit. To accomplish our objectives, we interviewed appropriate personnel and performed detailed testing for a statistically sampled set of active email accounts for employees with a withdrawn status. Our last day of fieldwork was July 27, 2015.

We found that corrective action was taken for five of the six findings included in the original audit. Information Technology made significant progress in improving security over email. Continual automated monitoring and manual processes were implemented to provide greater assurance that there is no unauthorized access at the network and user levels, and the recovery of the email exchange system was adequately tested. However, Information Technology continues to work on implementing an email retention policy, so emails continue to be retained indefinitely.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We appreciate the cooperation and assistance provided by Information Technology during the course of this audit.

Sincerely,

A handwritten signature in blue ink that reads "Angela M. Darragh". The signature is written in a cursive style.

Angela M. Darragh, CPA  
Audit Director



AUDIT DEPARTMENT

# Audit Report

## Information Technology Email Service Follow Up

August 2015

Angela M. Darragh, CPA, CISA, CFE  
Audit Director

**AUDIT COMMITTEE:**

*Commissioner Steve Sisolak*

*Commissioner Chris Giunchigliani*

*Commissioner Lawrence Weekly*

## TABLE OF CONTENTS

<b>BACKGROUND .....</b>	<b>1</b>
<b>OBJECTIVES, SCOPE, AND METHODOLOGY .....</b>	<b>1</b>
<b>RESULTS IN BRIEF .....</b>	<b>3</b>
<b>DETAILED RESULTS .....</b>	<b>3</b>
<b>Emails Retained Indefinitely (HIGH) .....</b>	<b>3</b>

**BACKGROUND** Clark County (County) uses Microsoft Outlook to electronically communicate internally and externally. It is a vital part of County communications. The County established directives to safeguard communications and data shared through this tool. Information Technology (IT) is ultimately responsible for maintaining an operative email service and security over the service.

County Departments are responsible for notifying IT to initially authorize or disable email accounts. IT activates and deactivates accounts. Users of the County email must also be granted network access, as servers for email service reside within the County's information technology framework. Users of the County email service may include external users such as consultants, vendors, and other organizations. At the time of the audit, there were in excess of 5,400 email users.

Information Technology has moved to replication processes as a means of back-up for email data and archives, as opposed to tape back-ups. Replicas exist on County servers and at vendor facilities.

Email service is also accessible through the internet and the Outlook Web Application.

**OBJECTIVES, SCOPE, AND METHODOLOGY** The objective of this audit is to determine if corrective action was taken on the reported findings included in the *Information Technology Email Service* audit dated May 6, 2014.

We met with the Chief Information Officer and staff and obtained detailed information for the status of corrective action for each finding. We performed the following to determine the status of each finding included in the original report:

- IT Staff provided documentation consisting of scripts that identify Active Directory accounts that should be disabled for withdrawn employees. They also provided scripts used for updating personnel numbers and vendor numbers of active emails and identifying email accounts with "Send As" names. We reviewed these scripts for the ability to reasonably perform tasks.
- We selected a representative sample of withdrawn employees

from the original audit to determine if email accounts were disabled. A total of 379 withdrawn employees with active emails existed in the original audit. Based on a 95% confidence level with anticipated rate of occurrence of 1% and desired precision range of 5%, we randomly selected a sample of 92 accounts. We reviewed email accounts on the County's email exchange system to determine whether the account appeared to be active. For those accounts that appeared to be active, we reviewed the current employment status on the County's personnel system and other available information to determine whether the active email account was valid.

- We reviewed the most recent reports of updated personnel numbers and vendor numbers to verify that the scripts were running reasonably.
- We reviewed the original audit selection of five vendor accounts to verify expiration dates were added. We also obtained documentation from IT consisting of drafts of policies and procedures for retention of emails and presentations to County management.
- We reviewed a standard email notification to email account users informing them of their "Send As" privileges and actions to take if these privileges should be removed.
- We obtained a list of email accounts for which passwords never expire and passwords are not required and verified that none should have required passwords or an expiration date.
- We reviewed procedures for testing of recovery of the email exchange system for reasonableness of process of recovery.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

**RESULTS IN BRIEF** Adequate corrective action was taken for five of the six findings from the original audit report. IT policies and procedures for retention of records are in draft form and presently not approved by County Management. Indefinite retention of all emails remains a high risk for the County in the form of increased storage needs, risk of corruption of voluminous information, and risks of liability over sharing confidential information and historical availability.

Each finding includes a ranking of risk based on the risk assessment that takes into consideration the circumstances of the current condition including compensating controls and the potential impact on reputation and customer confidence, safety and health, finances, productivity, and the possibility of fines or legal penalties.

## **DETAILED RESULTS**

**Emails Retained Indefinitely (HIGH)** IT is coordinating efforts with County Management to resolve the retention of emails. Policies and procedures are in draft form and will need the approval of County Management prior to implementation.

All emails continue to be retained and storage space for emails continues to increase with replication occurring in four locations. The risks remain that efforts to retain emails indefinitely will not be feasible in the future due to unforeseen and indeterminable events such as rising costs or workforce efforts to maintain voluminous information without corruption. The County also increases the risk of liability over confidential information being shared and historical information availability.

### *Recommendation*

1. Establish policies specifying that email is not to be used as a repository for records and that email content that does that does qualify as a record is changed to some other format for retention.

### *Management Response*

We continue to make progress on establishing and implementing an email retention policy. The draft IT Directive #2 was approved by the IT

Executive Steering Committee on 7/13/15. This policy establishes a 180 day retention period for emails in user's inboxes and 7 year retention for other emails. Based on our current email storage usage of 229 terabytes for email, archives, and backup, we calculate that implementing this policy would reduce our storage needs by 27.5%, with an initial cost avoidance of \$53,525 and recurring cost avoidance of \$22,046 each year.

To implement the policy, we are identifying funding for a contract project manager who will do the following:

- Develop a marketing/communication plan (including timelines)
- Develop and deploy MS Outlook training focused on using Outlook folders
- Assist IT MS Outlook and Exchange staff in designing and testing the new retention plan.

Our anticipated completion date is April 2016.

**CLARK COUNTY INFORMATION TECHNOLOGY  
 EMAIL SERVICE FOLLOW UP AUDIT  
 Findings, Recommendations, and Corrective Actions Status  
 As of July 27, 2015**



**AUDIT DEPARTMENT**  
 Angela Darragh, CPA, CFE, CISA, CHC  
 Director

**Original Report Issuance Date: May 6, 2014**

Finding	Recommendation(s)	Corrective Actions Status
<b>3 - Emails Retained Indefinitely (HIGH)</b>		
<p>Emails sent from and received by users in the ClarkCountyNV.gov domain are never permanently deleted. County Information Technology Directive Number 2, Email Policy, states that employees must maintain a copy of emails in a separate repository or print out and manually place records in a separate file. However, there is concern that policies may not be strictly followed and emails may have become the place of record. Information Technology does not have the tools necessary to sort through voluminous emails to identify record types for retention. As a result, emails continue to be retained indefinitely.</p> <p>Storage for the email system is currently up to 14.4 terabytes of data. Replication of emails and backups is 132 terabytes and the archive and its replication is 22 terabytes. Email may be stored in four locations at any one time, and two of those locations indefinitely (archive and archive backup). The fact that users are not limited in the amount of email they can have in their active mailbox causes a greater use of storage during replication. We believe that efforts to retain emails indefinitely will not be feasible in the future due to unforeseen and indeterminable events such as rising costs or workforce efforts to maintain voluminous information without corruption. The County also increases the risk of liability over confidential information being shared and historical information availability.</p>	<ol style="list-style-type: none"> <li>1. Establish policies specifying that email is not to be used as a repository for records and that email content that does qualify as a record be changed to some other format for retention.</li> <li>2. Develop schedules for purging of e-mails in accordance with record retention policies.</li> <li>3. Set reasonable mailbox size limits for users.</li> <li>4. Provide a cost analysis of storage use and future needs for the exchange system in order for management to make appropriate decisions over data retention.</li> </ol>	<p><b>In Progress.</b> IT is coordinating efforts with County Management to resolve the retention of emails.</p> <p><b>MANAGEMENT RESPONSE:</b></p> <p>We continue to make progress on establishing and implementing an email retention policy. The draft IT Directive #2 was approved by the IT Executive Steering Committee on 7/13/15. This policy establishes a 180 day retention period for emails in user's inboxes and a 7 year retention for other emails. Based on our current email storage usage of 229 terabytes for email, archives, and backup, we calculate that implementing this policy would reduce our storage needs by 27.5%, with an initial cost avoidance of \$53,525 and recurring cost avoidance of \$22,046 each year.</p> <p>To implement the policy, we are identifying funding for a contract project manager who will do the following:</p> <ul style="list-style-type: none"> <li>• Develop a marketing/communication plan (including timelines)</li> <li>• Develop and deploy MS Outlook training focused on using Outlook folders</li> <li>• Assist IT MS Outlook and Exchange staff in designing and testing the new retention plan.</li> </ul> <p>Our anticipated completion date is April 2016.</p>

Finding	Recommendation(s)	Corrective Actions Status
<b>1 - Many Active Email Accounts Not Valid with Potential Network and Mainframe Access (HIGH)</b>		
<p>We examined all email users within the domain of ".ClarkCountyNV.gov". We found that of 5,464 email users (excluding generic users), 379 (7%) are no longer employees, and 1 test account existed.</p> <p>We also reviewed 5 vendor accounts, and none had an expiration date. Vendor accounts are a risk, as the vendor may no longer be contractually affiliated with the County but still have ability to obtain or provide information/direction that can be confidential or damaging.</p> <p>The greatest risk associated with invalid active accounts is that County network access also potentially remains active, as does other access to County applications allowed through RACF, the Mainframe system. The risk is increased for the two departments (Air Quality Management and Development Services) that have distributed responsibility as opposed to a centralized responsibility residing with Information Technology. The risk is that these departments will grant network access without being monitored by Information Technology, placing network security at risk.</p>	<ol style="list-style-type: none"> <li>1. Implement procedures to actively validate user accounts, including network access, on a consistent basis in compliance with County Information Technology Directives.</li> <li>2. Realign responsibilities for notification to disable accounts. Such notification efforts should be coordinated between Human Resources, Purchasing, and Information Technology.</li> <li>3. Provide a list of email users (internal and external users) to departments for validation on a periodic basis. Invalid accounts should be immediately disabled.</li> <li>4. Implement procedures to monitor access provided by decentralized administrators.</li> </ol>	<p><b>Resolved.</b> IT wrote scripts to identify employees with withdrawn status and deactivation of access from the network. This script is run weekly. IT also wrote scripts to identify vendors. Vendor accounts expire after 1 year. Vendors are also identified in the account information. A sponsor field was added to Service Now in order to have a contact person for verifying vendor status. Emails are sent to departments for these vendors and verified monthly. Decentralized departments are monitored by IT.</p>

Finding	Recommendation(s)	Corrective Actions Status
<b>2 - Inconsistent Identification of Internal and External Users (HIGH)</b>		
<p>Not all active accounts have sufficient information to determine whether it is valid. Of the 5,464 email accounts reviewed, 184 (3%) could not be matched to Clark County personnel data. Employees are assigned a personnel number when hired, but this information is not always available when an email account is activated. Further, departments do not provide a vendor number when requesting vendor email accounts. Without a process for validating information, it is possible for IT and department with distributed responsibility to set up an email account and grant email and network access to virtually anyone.</p>	<ol style="list-style-type: none"> <li>1. Require departments to provide personnel and vendor numbers when requesting email accounts. If the personnel number is not available at that time, the department should provide the information once it is obtained.</li> <li>2. Enter this information into user accounts in order to facilitate validation reviews of email accounts and granted network access.</li> <li>3. For vendor accounts, include a County representative sponsor and contact number for any questions.</li> </ol>	<p><b>Resolved.</b> IT wrote a script to obtain personnel and vendor numbers for identification of email account users. Manual process are in place to resolve exceptions identified in reports produced from the automated process. IT resolved the vendor identification issues by including County financial system vendor numbers. The sponsor field configured into Service Now facilitates communication to departments for resolving exceptions to vendor number identifications. Vendor email accounts are verified monthly.</p>
<b>4 - Send As Names No Longer Valid (MEDIUM)</b>		
<p>The email system contains 145 users with "Send As" privileges. These users are able to send email as if it were being sent from another individual. Information Technology does not validate these privileges once email accounts are activated. However, employees may transfer or the responsibilities may change so that they should no longer have these privileges. These privileges are usually granted on behalf of upper level management, and those users may not realize that another employee is able to send email under their name. We found that 7 users able to send as another employee were terminated employees, 4 users with individuals able to send messages on their behalf were no longer employed with the County, and 3 "Send As" names could not be verified based on the County's personnel data. The validity of County email communications may be compromised when "Send As" privileges are not closely monitored.</p>	<ol style="list-style-type: none"> <li>1. Validate "Send As" privileges with employees annually.</li> </ol>	<p><b>Resolved.</b> IT developed a script that sends out emails to users for verifying of "Send As" privileges. This process is done weekly.</p>

Finding	Recommendation(s)	Corrective Actions Status
<b>5 - Passwords Not Required and Never Expire (MEDIUM)</b>		
<p>Email accounts for 85 users are set not to require a password. Further, email accounts for 34 users are set to have network passwords that never expire. During testing, we found that all accounts currently have a password set, even if not required. However, users with accounts that do not require passwords may set a password and then change to using no password. In that case, anyone with the user name may access any programs that do not require separate passwords and the email account of that user. The user name is usually the same as the email user name that is readily available through many resources. This places a risk for unauthorized users to access, change, and/or disseminate confidential information. Allowing users to never change passwords is not in accordance with County policies over network access security.</p>	<p>1. Change the setting on each of the accounts identified above to require a password that expires within the parameters required by Information Technology Directive 1</p>	<p><b>Resolved.</b> IT has set all email accounts to expire and require passwords except for shared email accounts for conference areas. Decentralized departments are monitored by IT.</p>
<b>6 - Recovery of Exchange System Not Tested (LOW)</b>		
<p>While Information Technology does have recovery procedures, the email system replication is not tested to determine whether replicated data is recoverable. Should a disaster or a significant disruption of service occur, Information Technology is not assured that the exchange system can be recovered fully and without data corruption. The exchange system is considered a critical component of the County, as it is vital for communication. Due to the number of backups to the active email system, we believe the risk based on this weakness is relatively low.</p>	<p>1. Develop processes for testing recovery of exchange system data.</p>	<p><b>Resolved.</b> IT performed a test recovery of the exchange system. Due to the voluminous emails, a full recovery of all emails was not included in the test.</p>