City of Santa Fe

Information Technology Internal Audit

April 2021

REDW LLC
CPAs | Advisors

City of Santa Fe
Information Technology Internal Audit

Table of Contents

City of Santa Fe
Information Technology
Internal Audit

Report

INTRODUCTION

We performed the internal audit consulting services described below to assist the City of Santa Fe Information Technology and Telecom (ITT) department in evaluating the policies, procedures, processes and internal controls over various ITT areas including network, physical and workstation security, mobile device usage, user access and ITT Governance to ensure adherence with best practices and sound internal controls.

Our services were performed in accordance with the terms of our Professional Services Agreement and engagement letter for internal audit services and the applicable Standards for Consulting Services prescribed by the American Institute of Certified Public Accountants. Although we have included management's responses in our report, we do not take responsibility for the sufficiency of these responses or the effective implementation of any corrective action.

PURPOSE AND OBJECTIVES

Our internal audit focused on evaluating and testing the City of Santa Fe's ITT controls and security processes, particularly with workstation security, employee education, and incident response and employee access controls.

OBSERVATIONS, RECOMMENDATIONS AND MANAGEMENT RESPONSE

As a result of our testing, REDW identified the following observations:

1) Employee Access

Network access as well as access to individual software within each department is granted by the City's ITT department and a form is completed and signed by the Department Director prior to access being granted. For all terminations, Human Resources is responsible for sending a termination memo to ITT at which point a work order is created to document the removal of network access. Our testing determined:

- Forms and/or work order documentation was not on file for the four transferred employees we tested therefore, we were not able to determine if access had been terminated from their previous positions.

Arizona
5353 N 16th St, Suite 200
Phoenix, AZ 85016
P 602.730.3600

New Mexico
7425 Jefferson St NE
Albuquerque, NM 87109
P 505.998.3200

Oklahoma
708 N Santa Fe Ave, Suite 110-E
Edmond, OK 73003
P 405.543.1410

- 12 of 18 terminated employee accounts were not disabled on the termination date. Variances ranged from 10 to 156 days.
- For 6 of 18 terminated employee accounts, we were unable to conclude the account disable date due to a lack of documentation and inefficiencies in reporting on the helpdesk system.
- 8 of 18 employees did not have a HR termination memo to generate the termination work order. 2 of these 8 had their accounts disabled within 10 to 26 days while the remaining 6 accounts did not have adequate documentation in place to determine the disabled date.

Furthermore, five of the termination memos ITT was able to provide were received from Human Resources approximately one week or longer after the employees had terminated, which is a significant gap in time between actual employment termination and notification of accounts needing to be disabled.

Lastly, we determined there are no procedures in place to ensure departments monitor access to department software to ensure user access is appropriate for job title and function. This is especially critical on software that is web-based and therefore accessible from any device.

Potential Risk: *High* — The absence of a consistent process to ensure transfers and terminated employee access is appropriate increases the risk to high that inappropriate access may be granted for extended periods of time resulting in potential access to sensitive data.

Recommendations:

1. The Computer Access Controls policy was last updated in 2017. Update and enforce the Computer Access Control policy to ensure compliance with end user activation and de-activation for both the City network and systems access. In the policy, expand on both the employee transfer and the employee termination process to include all steps to be taken to successfully complete these processes, and communicate these processes throughout the City.
2. Implement a formal monitoring program for both network and systems accounts to ensure accounts with no activity have been reviewed and/or disabled within 30 days and document the account review process.
3. The formal monitoring program should also include controls over monitoring for department software to ensure individual departments are performing access reviews on a periodic basis (at least annually). In the event they are not performing the reviews, procedures should be in place for the ITT department to work with the department directors to get access removed.
4. Ensure Human Resources notifies the ITT department of voluntary employee terminations before the termination date to confirm network and systems access is disabled the day of termination. Having this information ahead of the termination date will allow the ITT department more time to be proactive with the employee termination process. ITT should be immediately notified of involuntary employee terminations to ensure network and system access is disabled in conjunction with the employee's exit.

Management Response: The Computer Access Control Policy-Authentication and Authorization was reviewed and updated on March 27, 2020. The REDW recommendations will be added to our policy repository for consideration during the next revision of the policy by the end of FY 2022.

2) Employee Security Awareness Training

A formal security awareness training program is in place for all newly hired employees as well as additional procedures that are performed throughout the year such as mock phishing attempts and communications regarding how to handle suspicious e-mails that have infiltrated the network. While the City has an Information Security Awareness and Training Policy that requires security awareness training for all new hires, and annual training for all employees, relevant consultants and contractors, the City has not implemented a formal and mandatory security awareness training program to continuously educate all employees on the risks associated with fraudulent emails, social engineering techniques, website browsing, mobile device security, or other cyber security risks.

During our testing of employee knowledge over security awareness, we identified the following:

- 2 of 15 employees disclosed having clicked links or downloading attachments from questionable email messages and did not know the proper procedure to report questionable email messages;
- 8 of 15 employees did not remember the last time they had security awareness training, or any training received since new hire orientation;
- 13 of 15 employees had remote access but only one out of the thirteen said remote access security training was provided;
- 6 of 15 employees did not know the risks related with USB devices; and
- One employee did not know to contact the ITT department to report a possible security incident but would contact the department supervisor.

Furthermore, multiple employees communicated they do not regularly read the emails sent by the ITT department that contain security training tips and tricks.

Potential Risk: *High* **—** The absence of a formal security awareness training program and consistent education practices to City employees regarding IT threats escalates the risk to high that employee actions could result in a network breach and potentially compromise sensitive data.

Recommendations:

1. Formulate and document a training plan to incorporate onboarding, proactive training and reactive (follow up) training for all employees, temporary workers, and contractors on a continuous basis (i.e., monthly, quarterly, etc.).
2. Consider using an online security awareness training platform that offers:
    - Short user inter-active training modules with follow up questions
    - The ability to send mock phishing emails to employees
    - Provides a secure method for employees to report suspicious messages to the ITT department for review and feedback (usually in the form of an or email plugin)
3. Establish sanctions for non-compliance when employees do not complete training.

4. Ensure management is able to measure employee training performance and set risk indicator scores for the City and employees (i.e., the City and employees will not exceed a risk percentage above 20%).
5. Update the Information Security Awareness and Training Policy with the training plan, sanctions, and risk score once the formal program has been implemented.

Management Response: The City has implemented a training platform called Localgovu that has training modules on Cyber-Security Threats to Public Entities and Protection from Ransomware and Phishing Attacks. IT is currently working with Human Resources to implement those modules in City Wide training. The Localgovu training has testing as part of the training. In addition, as part of our new Cybersecurity/Ransomware Insurance with Cowbell for the year we have committed to using Cowbell's partner Wizer cybersecurity training. We plan on using the current policy and the projects mentioned above to document the cybersecurity training plan by the end of FY 2022.

3) Windows Operating Systems and Updates

The ITT department supports over 1,300 employee workstations that are either connected to the City's network or used by remote City employees. While the majority of the population has been transferred to a new operating system, our testing over workstation security determined three of 15 workstations tested were running on an unsupported operating system and one of 15 workstations had not had Windows updates applied since December 2020. In addition, our testing determined that while updates are configured to automatically install on workstations, this process is not monitored to ensure successful installations.

Potential Risk : *High* — The presence of workstations which run unsupported operating systems increases the risk to high as these systems will not receive critical monthly security updates leaving the systems vulnerable to be compromised. In addition, the absence of a system to monitor the installation of critical security patches further increases the risk as ITT may not be aware of installation failures.

Recommendations: The City should identify and update all unsupported workstations to the most current operating system to ensure they are receiving critical security updates. In addition, a system should be implemented to monitor and alert the ITT department of any workstations that are not current or have failed critical security updates.

Management Response: The REDW recommendations appear reasonable and we will implement by the end of FY 2022. We are monitoring using LabTech and in progress to remediate the issue.

4) Workstation Security

Employee workstation security is a critical component to ensure the protection and security of the City network and confidential data. The ITT department has policies in place to address critical workstation security components such as prohibiting removable media like USB drives and requiring authorized users to obtain encrypted USB drives from ITT. Our testing over workstation security determined:

- All 15 workstations tested could access free proxy server websites which, if installed, will allow an employee anonymous web browsing bypassing City security and monitoring controls;

- Personal e-mail websites such as Gmail, Hotmail, Yahoo, etc. were not blocked on the City of Santa Fe network, which could introduce malware into the network from infected email or provide the opportunity for employees to communicate City information from an unauthorized email account;
- 13 of 15 workstations could access social media websites, which in nature are insecure and without proper social media security awareness training for employees can expose the City and employees to additional security and privacy risks;
- 3 of 15 workstations were using unencrypted non-City of Santa Fe ITT issued USB drives and in one instance, a cell phone plugged into the USB port was not scanned by the monitoring application; and
- One out of 15 workstations had continuously failed to update to the current anti-virus update leaving the machine vulnerable to new malware exploits.

Potential Risk: *High* — The absence of monitoring controls in place over workstation security increases the risk to high that employees could inadvertently download or click on malicious links while on City of Santa Fe equipment. This is further escalated to high due to the absence of security awareness training (See Observation #2).

Recommendations:

1. Block access to free proxy server websites and personal email websites at the firewall level to reduce the risk of employees compromising the City of Santa Fe network.
2. Develop a social media acceptable use policy and determine whether or not all employees are authorized to access social media from the City of Santa Fe network and which sites are acceptable. Include training on the security risks of social media for City employees. Block social media sites from unauthorized employees at the firewall level.
3. Implement automated preventive controls over the use of USB drives. These automated controls can be configured to block the use of unauthorized USB drives on City systems or automatically encrypt the drive if it is not already encrypted.
4. Ensure removable media policies are communicated to all employees as part of their security awareness training.
5. Consider only allowing authorized personnel to use City issued encrypted USB drives for business purposes to ensure City data saved on these drives cannot be accessed if the drive is lost or stolen.
6. Ensure workstation endpoint protection is actively monitored to mitigate possible security incidents that could take place due to the failure of the endpoint protection software not updating.

Management Response: We have implemented controls to block free proxy web servers. We have a policy in place that addresses social media in our technology resource acceptable use policy and plan on implementing a more comprehensive policy. The suggestions from REDW are reasonable and we will work on implementing those controls that are technologically feasible by the end of FY 2022.

5) Mobile Devices

Employees are authorized to synchronize City email to City issued mobile devices (smartphones, tablets, etc.). While, the ITT department has a Mobile Device Acceptable Use Policy outlining access control, device security and hardware support for mobile devices, there is currently no requirement for employees to acknowledge they will comply with the mobile device policies. Our testing determined:

- 2 of 10 employees synchronized City of Santa Fe email to a personal smartphone and one of these employees also acknowledged to downloading attachments to the personal device despite the policy stating only City issued mobile devices can be utilized;
- 8 of 10 employees had not read the mobile device policy and therefore did not understand the City's policies surrounding mobile device usage;
- 1 of 10 employees did not have a PIN or passcode on the City device therefore leaving their phone and City e-mail easily accessible; and
- 2 of 10 employees did not know the proper steps to take if the device was lost or stolen.

In addition, none of the 10 employees we tested were enrolled in the mobile device management solution which assists ITT with the secure management of the devices in addition to the ability to remotely wipe the device in the event of a theft or misplacement.

Potential Risk: *High* — While policies and procedures have been developed over mobile phone usage, they are not actively utilized to educate employees on City policy regarding City issued devices thus leaving the City susceptible to potential compromise by poor mobile device management. This risk is escalated to high as the mobile device management solution is not in place to assist ITT with secure management of the devices in the event of theft or misplacement.

Recommendations:

1. Enroll all City of Santa Fe smartphones into the mobile device management solution to ensure these devices can be securely managed and remotely wiped should the device be lost or stolen. If possible, configure the mobile device management solution to only allow authorized smartphones to connect to the City's email system.
2. Finalize the Mobile-Portable Computing Device Form and ensure employees authorized to use City of Santa Fe smartphones read the Mobile Device Acceptable Use Policy and sign the Mobile-Portable Computing Device Form before being issued their City mobile devices. In addition, the ITT department, in collaboration with City Legal, should review policies surrounding personal devices to determine potential risks associated with allowing employees to utilize their personal device for City e-mail and determine if policies should be updated to reflect only City issued devices will be allowed.
3. Train mobile device users on the security risks associated with mobile devices particularly with email, saving sensitive data on the device, accessing social media sites, downloading, and installing mobile applications, and other cybersecurity risks to help mitigate mobile device security risks.

Management Response: We believe the recommendations from REDW are reasonable and will continue to work on user training, providing copies of mobile device policy and rules forms, and will provide updated information to the end users on a regular basis by the end of FY 2022.

6) Security Incident Response

Data security best practices require organizations to have a formal, written, Security Incident Response Plan that is tested at least annually to ensure the ITT department can respond appropriately to security incidents, retain necessary evidence, and communicate appropriately to necessary parties regarding mitigation of incident risks. While the City of Santa Fe has a documented Security Incident Response Plan it has not been tested to ensure appropriate incident response for possible attack scenarios.

Potential Risk: *High* — Without testing, the City may be ineffective in responding and recovering from a data breach or cybersecurity attack which could be costly to the City.

Recommendations: Management should require the Security Incident Response Plan to be tested at least annually and that testing is documented. Testing can be completed with table top exercises to perform various tasks required to respond to a variety of identified incidents such as unauthorized access, malware, theft or a compromised account. Furthermore, City leadership should take proactive measures and determine should a major incident occur, such as a ransomware attack, what the City is willing to do to get their information back and what are acceptable downtimes for their systems. Planning through this in advance will help the ITT Department respond without having to make these major decisions reactively in the moment.

Management Response: Security Incident Response plan testing is on the ITT plan for the year. The REDW suggested recommendations looks like a good list to incorporate as part of the testing.

7) IT Disaster Recovery

The City of Santa Fe has a documented Disaster Recovery Plan and Business Impact Analysis which assist with identifying mission critical business activities and their associated recovery timelines in the event of a disaster. Our testing determined the Disaster Recovery Plan and Business Impact Analysis have not been updated since 2016 nor has the Disaster Recovery Plan been tested to ensure recovery times and processes are appropriate. In addition, we performed an assessment of the Disaster Recovery Plan and identified the following key elements were missing:

- The plan does not identify who can declare an event a disaster to start the disaster recovery plan process thus increasing the risk that defined leadership during the event of a disaster recovery event may not be present causing potential delays in recovery;
- There is not a communication plan in the event of a disaster to ensure relevant parties are aware of actions steps to take in the event a disaster has been declared;
- The disaster recovery strategy has not been documented to guide IT and other personnel to ensure the recovery process is successful; and
- Training has not been conducted for employees involved in the disaster recovery planning process, which is necessary to ensure everyone on the disaster recovery team is familiar with their recovery roles.

Potential Risk: *High* — The absence of updated plan documents including the Business Impact Analysis, and testing of the Disaster Recovery Plan increases the risk that in the event of a disaster the City could potentially be offline and City operations could be negatively impacted.

Recommendations:

1. Ensure both the Disaster Recovery Plan and Business Impact Analysis are updated to include any recently identified critical business processes or applications along with the required recovery time and recovery point objectives with the key elements identified above.
2. The disaster recovery strategy should be tested at least annually and testing should be documented. Testing can be completed either with table top exercises or functional recovery of different areas and applications. Testing will help ensure the City will be able to effectively recover from a declared disaster.

Management Response: Updating the Disaster Recovery plan is a high priority for the department. The plan is to hold a workshop this year to update the DR plan, hosted by the same research group that helped with the last DR plan. A DR testing plan will also be developed and testing will take place by the end of FY 2022.

8) IT Governance

IT Governance directs the IT function and strategy and assists with ensuring leadership and executive management are tuned into the IT operations and verifying they are aligned with overall strategic and business objectives City-wide. Best practice recommends governance meetings occur at least quarterly to allow for collaborative discussion on IT strategy and objectives. Our testing determined the IT Governance Committee meetings have not been held since 2017 due to turnover at the City. In addition, we determined there is no City-wide strategic plan to benchmark the IT Governance strategy and function.

Potential Risk: *Moderate* — The absence of a strong IT Governance function increases the risk that IT strategy may not be aligned with City-wide goals and objectives thus potentially resulting in failure of IT projects, over/under spending on IT resources, and the absence of accountability over the IT function.

Recommendations: ITT, in collaboration with City management, should review the IT Governance Charter to ensure it is reflective of best practices and procedures. An IT Governance Committee should be identified and quarterly meetings should be established. Minutes should be kept at each to ensure documentation of topics discussed. Lastly, the City should develop a strategic plan to ensure individual departments can align goals and objectives to overall City goals and objectives.

Management Response: IT Governance process and implementation is a high priority for the IT department and plan on implementing that as soon as possible. We are conducting IT governance using Change Control Board, budget review and informal meetings and will work on re-implementing a more formalized process by the end of FY 2022.

9) Standard user agreements

When a new employee is hired at the City, they are required to read and understand the acceptable uses of the City of Santa Fe technology resources and sign the Technology Resources Standard User Agreement which is then kept on file in the Human Resources department. Our testing determined 4 of 20 employees did not have their form on file. Communication with HR indicated there is no process in place to ensure this form is obtained upon hire.

Potential Risk: *Moderate* **—** The absence of a signed acknowledgement demonstrating employee agreement with technology resource policies increases the risk that employees may not be aware of City policies and therefore may inadvertently violate security protocols.

Recommendations: The ITT department, in collaboration with HR, should implement a process to ensure the Technology Resources Standard User Agreement form is signed by all new hires prior to providing access to network resources.

Management Response: We will assist Human Resources as requested to help support any controls needed including document retention by the end of FY 2022.

10) Remote Access

The City has implemented a secure remote access connection for authorized employees to utilize while working remotely. Employees who wish to obtain remote access must complete an authorization form and obtain approvals prior to access being granted. The ITT department, in accordance with the Remote Access Policy, must keep records of these forms on file. Our testing determined 19 of 20 employees did not have record of a remote access authorization on file either in the help desk ticket system or email archives.

Potential Risk: *Low* **—** The absence of authorization forms to document approval of remote access increases the risk that employees may not have department director approval prior to obtaining remote access.

Recommendations:

1. Ensure all employees configured for remote access have an approved authorization form on file indicating remote access is allowed. This includes any employees that were configured for remote access before the 2017 Remote Access Policy went into effect.
2. Disable all remote access accounts for employees who are not authorized for remote access or no longer need to use remote access for their job function to mitigate unauthorized access to the network.

Management Response: We are working on a strategy to mitigate the concerns documented by REDW. With ongoing Covid Pandemic telecommuting this is an issue that we will work with executive leadership to maintain both security and access as needed by the end of FY 2022.

11) IT Policies and Procedures

Policies and procedures are critical for the ITT department to ensure both ITT and City employees have clear understanding of what City requirements are surrounding several areas and processes over the IT environment. The National Institute of Standards and Technology (NIST) has several IT related best practices including what policies an IT department should have in place. During our testing over policies and procedures, we determined the ITT department has developed and approved 27 of the 31 recommended policies by NIST. The following policies had not been approved as of testing but are currently in draft form:

- Data Classification Policy
- Physical Security Policy
- Social Media Acceptable Use Policy
- Vendor Management (IT) Policy

In addition, of the 27 policies in place, 13 have not been reviewed since 2017 and one, the Technical Resource Acceptable Use Policy has not been reviewed since 2003, however, the ITT department is currently in process of reviewing outdated policies and is targeting one policy per week to get them up to date with current procedures and best practices.

Lastly, we identified several policies where policy components may be missing in accordance with NIST best practices.

Potential Risk: *Low* — While some policies are in draft form and others are outdated, ITT has already implemented procedures to update all policies thus reducing the risk to low.

Recommendations:

1. Ensure the Technical Resource Acceptable Use policy is updated to include new processes, new technologies, and IT best practices that have been implemented since policy creation to better manage employee expectations with acceptable use of the City's technology resources.
2. Establish controls to ensure all City employees have reviewed and signed the Technology Resources Standard User Agreement at the time of hire to mitigate technology risks.
3. Review and update policies annually, or as technology best practices are updated and new controls are implemented for the City to keep technology policies and procedures current.
4. Finalize the draft Data Classification, Physical Security, Social Media Acceptable Use, and Vendor Management policies to continue meeting best practice security standards.
5. Review each policy as well as the NIST best practices and consider implementing the components identified to ensure adherence with best practice.

Management Response: We will continue to update and add additional policies as recommended by REDW. The Technology Resources Standard User Agreement has been updated and is being reviewed by executive leadership. We will continue to build communication with other stakeholders to help expand policies where relevant by the end of FY 2022.

SCOPE AND PROCEDURES PERFORMED

In order to gain an understanding of the processes and operations, we interviewed the following personnel:

- Manuel Gonzales, Interim ITT Department Director
- Bradley Purdy, Chief Information Security Officer
- Larry Worstell, IT Infrastructure Services Manager
- Edward Duran, ITT End User Services Manager
- William Smith, IT Architect
- Felix Herrera, System Administrator
- Ramon Cameron, ITT End User Support Technician

In order to gain an understanding of the IT infrastructure, controls, policies and procedures, we read relevant portions of:

- City of Santa Fe Information Technology policies and procedures
- ITT Organizational Chart FY20
- The City of Santa Fe ITT Disaster Recovery Plan Report 2016, and the Infrastructure 2021 City of Santa Fe Disaster Response Summary
- Incident Response and Investigation Checklist SOP and Incident Response – Malware & Viruses SOP
- ITT Strategic Roadmap 2015 – 2018, and the ITT FY21 Strategy and the ITT Strategy Portfolios Programs Projects
- ITT Budget Procedures for FY21 (June 2020)
- IT Governance Charter
- IT Governance Committee
- City of Santa Fe IT Security Awareness Training materials (October 27, 2020)

We performed the following test work:

IT Governance – We obtained an understanding of the IT Governance function and obtained the IT Governance Charter. We evaluated whether the documentation was in alignment with IT best practices based on NIST standards with a specific focus on:

- A strong reporting structure and defined roles and responsibilities
- Involvement of City executive leadership at regular intervals
- Alignment of the ITT strategic plan to the City's business plan
- Contribution of ITT goals to the business strategic objectives
- The ITT strategic plan covered the operational budget for ITT

In addition, from the documentation we determined whether:

- There was a standing IT agenda item at executive leadership meetings
- All ITT personnel had signed a confidentiality / non-disclosure agreement at the time of hire

Policies and Procedures — We obtained the policies and procedures in place over the IT function and tested to determine if they had been reviewed on an annual basis. In addition, we performed a gap analysis based on the NIST and International Organization for Standardization Frameworks to determine if critical components were present in the policies.

IT User Agreements — We obtained a listing of all employees in place as of March 2021. From a total population of 1,251 employees, we selected 20 and tested to determine if the Technology Resource Standard User Agreement was signed by each employee at the time of hire and was retained in the employee file.

User Access Controls- New Hires — We obtained a listing of all new hires that occurred between June 1, 2020 and March 19, 2021. From a total population of 44 new hires, we selected 5 and tested to determine:

- The access form was completed and approved; and
- Access was granted timely after completion of the form.

User Access Controls- Transfers — We obtained a listing of all transfers that occurred between June 1, 2020 and March 19, 2021. From a total population of 38 transfers, we selected 4 and tested to determine:

- The approval form authorizing the change was submitted and approved; and
- The change was made properly in the system and old access was removed.

User Access Controls- Terminations — We obtained a listing of all terminations that occurred between June 1, 2020 and March 19, 2021. From a total population of 179 terminations, we selected 18 and tested to determine:

- A request to disable access was completed; and
- Access was disabled on or prior to the termination date.

User Access Reviews — We obtained an understanding of controls in place over user access to determine if annual reviews are performed to ensure user access is aligned with job title and function.

Workstation Security — We obtained a listing of all employees as of March 2021. From a total population of 1,251 employees, we selected 15 employees with a specific focus on employees who utilize IT resources daily. We then tested to determine:

- Employees did not have administrator rights on their computer;
- Security patch/update and virus pattern updates were current;
- The operating system was current;
- Controls over password protected screen savers were in place;
- The user was not able to access proxy and social media websites; and
- Security controls were in place when a USB device was plugged into the computer.

Employee Security Awareness — We gained an understanding of processes in place to ensure employees are aware of potential network security threats. Utilizing the sample selected in the Workstation Security testing, we interviewed each employee to determine:

- When they last received security awareness training;
- If they used VPN for remote access and had been trained on remote access use and security;
- If they synchronized their smartphone to City of Santa Fe email;
- If they were aware of:
    - How to recognize a security incident and where to report it
    - Social engineering techniques

- Password security and creating a strong password
- Dangers related to USB devices, and
- Risks related to email and phishing attacks

We also determined if controls were in place to monitor suspicious e-mails and filter them accordingly.

Mobile Device Security — To evaluate security controls over sensitive data on mobile devices and removable media, we utilized the sample of 15 employees from above. From the 15 employees, 10 were identified as syncing City of Santa Fe email to their mobile devices and tested to determine:

- If the employee had a PIN, biometric, or password enabled on the device;
- If the employee sends, downloads, or receives sensitive information by email;
- What the employee would do if the device was lost, stolen, or compromised; and
- If the employee had been provided and read the Mobile Device policy.

In addition, we gained an understanding of what controls are in place to monitor mobile devices issued to employees.

IT Disaster Recovery Plan — We obtained the Disaster Recovery Plan, the Business Impact Analysis, and the backup and restoration policies and procedures. We assessed each for the following:

- The plan was documented and reviewed annually;
- A Business Impact Analysis had been completed and there were calculated recovery point objectives (RTO) and recovery point objectives (RPO) for all critical apps;
- A Disaster Recovery Plan risk assessment had been completed;
- Roles and responsibilities for those involved were identified;
- The plan identified who declares an event a disaster and starts the disaster recovery process;
- There was a current call tree for employees and vendors/outside entities;
- There was a communication plan for a disaster;
- The disaster recovery strategy had been documented;
- There were detailed procedures for recovery of critical systems;
- There was an alternate site in place;
- There were back up processes in place;
- The plan had been tested annually and testing had been documented with an after-action report; and
- Annual training was conducted for all involved in the disaster recovery process.

Additionally, we selected 15 critical data backup logs from September 1, 2020 through March 31, 2021, and tested to determine the backup schedule was followed and the backup process was successful.

Security Incident Response Plan — We obtained the Security Incident Response Plan (SIRP) and policies and tested the plan to determine:

- The plan was up-to-date and adequate for responding to a cyber incident
- The plan identified a SIRP owner with defined duties
- A SIRP team had been identified along with the SIRP team's responsibilities and duties
- The plan included testing and training requirements
- The plan contained computer security incident classifications (i.e., unauthorized access, theft, compromised account, malware, etc.)
- There was a security incident notification process
- The plan contained incident severity classifications (high, low, etc.)
- There was an investigation process and included a physical evidence handling, copying, preservation, and retention processes
- There was containment, eradication and recovery processes
- The plan included a communication and reporting process

Additionally, we tested to determine if the plan had been tested and the SIRP team had been trained on their role.

Physical Security — We obtained an understanding of the data centers' physical security controls, and tested the physical security policy and procedures to determine physical controls were in place for IT work areas, data centers, server rooms, telecommunication closets as well as general access to City of Santa Fe buildings. Furthermore, we determined if the policy addressed environmental controls and fire suppression for data centers and server rooms.

Remote Access Security — We obtained the remote access policies and procedures and gained an understanding of processes in place. We then obtained a listing of all remote access users as of March 2021. From a total population of 415 remote access employees, we selected 20 and tested to determine if remote access was monitored and proper remote access documentation had been completed and approved.

* * * * *

This report is intended solely for the information and use of City of Santa Fe's management, Audit Committee and City Council members. If additional procedures had been performed, other matters might have come to our attention that would have been reported to you.

We received excellent cooperation and assistance from City of Santa Fe personnel during the course of our testing. We very much appreciate the courtesy and cooperation extended to our personnel. We would be pleased to meet with you to discuss our findings and answer any questions.

REDW LLC

Albuquerque, New Mexico
August 24, 2021