



NOTICE OF A REGULAR MEETING

Notice is hereby given that a Regular Meeting of the Governing Body of the City of Ranger, Texas, will be held on **Monday, June 23, 2025 at 5:30 P.M.** in City Hall, 400 West Main Street Ranger, Texas. The following subjects will be discussed, to wit:

Agenda Item 01: Call to Order- Mayor Robert Butler

Roll Call/Quorum Check-City Secretary Hope Delatorre
Invocation of Prayer
Pledge of Allegiance to the United States Flag
Pledge of Allegiance to the Texas Flag

Agenda Item 02: Citizen's Presentation-At this time, anyone on the list will be allowed to speak on any matter other than personnel matters or matters under litigation, for a length of time not to exceed THREE minutes. No Council/Board discussion or action may take place on a matter until such matter has been placed on an agenda and posted in accordance with law.

Agenda Item 03: Announcements from the City Commission or Staff-Comments may be made by the council or staff, **BUT NO ACTION TAKEN** on the following topics without specific notice. Those items include: Expressions of Thanks, Congratulations or Condolence; Information on Holiday schedules; Recognition of public officials, employees or citizens other than employees or officials whose status may be affected by the council through action; Reminders of community events or announcements involving an imminent threat to the public health and safety of the people of the municipality.

Agenda Item 04: Discuss/Consider: Approval of minutes of previous meetings:

- June 9, 2025 Regular Meeting

Agenda Item 05: Discuss/Consider: City Manager's Report: business regarding city administration. The City Commission may provide staff direction; however, no action shall be taken. (City Manager)

- Clean-up of Riddle Street area to facilitate water drainage.
- Grant updates to include new Application. (other than later item on CWDG equipment actions)
- Progress on Wastewater Plant upgrades/repairs.

Agenda Item 06: Discuss/Consider: Payable Bills. Listing of current bills for Commission Consideration. (Finance Director)

Agenda Item 07: Discuss/Consider: Contract with Kennedy Computer Solutions (KCS). (Finance Director)

Agenda Item 08: Discuss/Consider: Employee Health Insurance (Finance Director)

Agenda Item 09: Discuss/Consider: Resolution 2025-06-23-A— Allowing for the submission of a grant for a license plate reader and naming the City Manager, Finance Director, and Police Chief on the grant. (City Manager)

Agenda Item 10: Discuss/Consider: Resolution 2025-06-23-B—Establishing a Bank Account for the funding of the Wildfire Mitigation Grant

Agenda Item 11: Discuss/Consider: City Clean-up Code Enforcement Actions and Updates. Includes listing by property of status. (City Manager and Code Enforcement Official)

Agenda Item 12: Discuss/Consider: REDC Playground Equipment Discussion (REDC President)

Agenda Item 13: Discuss/Consider: Resolution 2025-06-12-D REDC Investment Policy (REDC President, REDC Treasurer)

Agenda Item 14: Discuss/Consider: REDC Proposal with Global Site Location Industries (REDC President)

Agenda Item 15: Discuss/Consider: Two Week City Clean-up in July with no fees for Residential Customers with current water bill. Rules would apply to include pick-up and up to medium trailer not to exceed sixteen feet. They will not accept tires, microwaves, wire of any kind, hazardous waste, or medical waste. (Mayor Butler, City Manager)

Agenda Item 16: Discuss/Consider: 2024 Water Quality Reports posted with Web Site. (Public Works Director)

Agenda Item 17: Discuss/Consider: Budget Series Updates. Status of Department Working Meetings to include 2025-2026 Budget Action Timelines. (Mayor Butler, City Manager, and Finance Director)

Agenda Item 18: Discuss/Consider: Update and Amendment of the City of Ranger Personnel Manual. The discussion will include review of key rules, policies, and procedures. (Mayor Butler)

Agenda Item 19: Discuss/Consider: Initial Flooding Mitigation Planning Discussion for 2025-2026 to include seasonal action items. (Mayor Butler, City Manager, Public Works Director)

Agenda Item 20: Discuss/Consider: Retire into Executive Session to deliberate any items as authorized by Texas Government Code Section 551.074

- Termination Appeal of Police Sergeant Todd Youngs
- Animal Control Officer Certification Completion

Agenda Item 21: Discuss/Consider: Reconvene into Open Session to take action as determined appropriate regarding:

- Termination Appeal of Police Sergeant Todd Youngs
- Animal Control Officer Certification Completion

Agenda Item 22: Discuss/Consider: Adjournment

I, the undersigned authority, do hereby certify that the above notice of meeting of the Governing Body of the City of Ranger is a true and correct copy of said notice on the bulletin board at the City Hall of the City of Ranger, a place convenient and readily available to the general public at all times, and notice was posted by 5:00 p.m., June 20, 2025 and remained posted for 72 hours preceding the scheduled time of the meeting.

Hope Delatorre

Hope Delatorre, Ranger City Secretary

The City council reserves the right to convene into Executive Session concerning any of the items listed on this agenda under the authority of the Mayor, whenever it is considered necessary and legally justified under the Open Meetings Act.

NOTICE OF ASSISTANCE

Ranger City Hall and Council Chambers are wheelchair accessible and accessible parking spaces are available.

Request for accommodation or interpretive services must be made 48 hours prior to this meeting. Please contact City Secretary's office at (254) 647-3522 for information or assistance.

This Notice was placed on the outside bulletin board on June 20, 2025 at _____

By _____.

Hope Delatorre, City Secretary



REGULAR MEETING MINUTES

A Regular Meeting of the Governing Body of the City of Ranger, Texas, was held on **Monday, June 9, 2025 at 5:30 p.m.** in City Hall, 400 West Main Street Ranger, Texas. The following subjects were discussed, to wit:

Council Members and City Staff Present:

Honorable Robert Butler	Mayor
Commissioner Jim McCullough	Place 2
Commissioner Katie Billings	Place 3
Commissioner Jared Calvert	Place 4
City Manager Charlie Archer	
Fire Chief Darrell Fox	
City Secretary Hope Delatorre	
Finance Director/Municipal Clerk Carol Stephens	
Public Works Director Daniel Plascencia	
Animal Control Officer Carrie Pilant	

Agenda Item 01: Call to Order-Mayor Robert Butler

Roll Call/Quorum Check Hope Delatorre City Secretary
Invocation of Prayer
Pledge of Allegiance to the United States Flag
Pledge of Allegiance to the Texas Flag

Agenda Item 02: Citizen's Presentation-At this time, anyone on the list will be allowed to speak on any matter other than personnel matters or matters under litigation, for a length of time not to exceed **THREE** minutes. No Council/Board discussion or action may take place on a matter until such matter has been placed on an agenda and posted in accordance with law.

There were no citizens signed up to speak.

Agenda Item 03: Announcements from City Commission or Staff-Comments may be made by council or staff, **BUT NO ACTION TAKEN** on the following topics without specific notice. Those items include: Expressions of Thanks, Congratulations or Condolence; Information on Holiday schedules; Recognition of public officials, employees or citizens other than employees or officials whose status may be affected by the council through action; Reminders of community events or announcements involving an imminent threat to the public health and safety of the people of the municipality.

Commissioner McCullough announced that the Ranger City Library was going to be hosting the Summer Reading Program. The City Secretary stated the closure of City Hall in observance of Juneteenth. The City Manager commended the City Staff for their hard work. Mayor Butler announced that on July 4th the Veteran's Commission and Ranger Veterans Support group would be having a function celebrating Independence Day which would take place at noon on Friday, July 4, 2025. Commissioner Calvert recognized City Manager Charlie Archer for his effectiveness as a leader for the City of Ranger. Chief Darrell Fox highlighted the painting done at the city park. Mayor Butler also commended the Fire Department on their clean-up of the corner of Main Street and Loop 254.

Agenda Item 04: Discuss/Consider: Approval of minutes of previous meetings:

- May 27, 2025
- May 29, 2025

Commissioner Calvert suggested splitting the minutes into two motions to allow for him to abstain from the May 29, 2025, meeting minutes vote.

Motion made by Commissioner Calvert to approve the minutes of the May 27, 2025, meeting.
Seconded by Commissioner McCullough.

Unanimously Approved

Due to Commissioner Calvert abstaining from the vote on the minutes of the May 29, 2025, meeting, the vote for the second meeting was pushed until after Commissioner Billings was appointed and sworn in.

Motion made by Commissioner McCullough to approve the minutes for the May 29, 2025, meeting.
Seconded by Commissioner Billings
Abstained by Commissioner Calvert

Motion Passed.

Agenda Item 05: Discuss/Consider: Consent Items: The Approval of Monthly Departmental Reports:

- **Library Report:** Librarian Diana McCullough
- **REDC 4A Report:** MJ Dawson
- **REDC 4B Report:** MJ Dawson
- **Municipal Court Report:** Judge Doyle Russell
- **Fire/EMS Report:** Chief Darrell Fox
- **Police Department:** Chief Charles Rodriguez
- **Public Works Report:** Daniel Plascencia
- **Finance Report:** Carol Stephens

Motion made by Commissioner Calvert to accept the departmental reports.

Seconded by Commissioner McCullough.
Unanimously Approved

Agenda Item 06: Discuss/Consider: City Manager's Report: business regarding city administration. The City Commission may provide staff direction; however, no action shall be taken. (City Manager)

- Status of Signs to Report Water Leaks with WrapStar
- Provide list of employee phones to City Commission
- Provide information that pass-through water rate agreements have been rolled over for La Casa, Morton Valley, and Staff.

The City Manager gave an update on day-to-day operations at the City of Ranger City Hall. These operations included the signs from WrapStar are completed, new chainsaws were purchased for the Public Works Department, repaired equipment, and the pass-through water rates are in effect for La Casa, Morton Valley, and Staff.

No action taken.

Agenda Item 07: Discuss/Consider: Adopt Resolution 2025-06-09-A Appointing a Commissioner to Place 3 (Mayor Butler)

Moved to Agenda Item 04.5

Katie Billings gave a brief introduction about herself to the Commission.

Motion made by Commissioner McCullough to appoint Katie Billings to Commissioner Place 3.
Seconded by Mayor Butler

Unanimously Approved

Agenda Item 08: Discuss/Consider: Oath of Office for the newly appointed Commissioner.

Municipal Clerk, Carol Stephens, administered the Oath of Office to Katie Billings.

Agenda Item 09: Discuss/Consider: Discuss reacquisition of baseball fields from Ranger Independent School District (ISD) to include purchase agreement and coordination with Ranger Youth Sports Association (RYSA). (Commissioner Doyle)

Commissioner Doyle was absent from this meeting, so Mayor Butler recommended getting a copy of the original agreement to discuss a similar arrangement to run past the legal team.

Motion made by Commissioner Calvert to have the legal team review the previous document.
Seconded by Commissioner McCullough.

Unanimously Approved

Agenda Item 10: Discuss/Consider: Status of Code Enforcement Officer; and Status of Dilapidated and Dangerous Building Actions (City Manager)

The City Manager presented pictures which indicated several properties on the loop that were in violation of multiple ordinances. One property had been identified that was outside the current city limits on the loop. The names and addresses were not released pending notification of the owners. The Code Enforcement Officer would be starting on June 16, 2025, and would be required to work under a licensed code enforcement officer for one year. He also spoke on the potential to put an emergency declaration in place to open the old dump grounds for clean-up.

Motion made by Mayor Butler to take no action.
Seconded by Commissioner Calvert.

Unanimously Approved.

Agenda Item 11: Discuss/Consider: Updating Contract with Kennedy Computer Solutions (KCS). (Finance Director)

Finance Director, Carol Stephens, discussed updating the contract with our technical support company. Due to the owner of the company being out of the country, the document was not completed.

Motion made by Mayor Butler to take no action.
Seconded by Commissioner Billings,

Unanimously Approved.

Agenda Item 12: Discuss/Consider: Ranger Economic Development Committee (REDC)-B Quotes for the City Park Playground Equipment (Commissioner Doyle, REDC President)

The REDC president, MJ Dawson, spoke with three developers regarding quotes for the equipment for the park. Mayor Butler questioned if the liability would be reduced if the manufacturer installed the equipment. Commissioner Calvert expressed the need for a 60-day waiting period per the REDC-B by-laws.

Motion made by Mayor Butler to take no action.
Seconded by Commissioner Calvert.

Unanimously Approved

Agenda Item 13: Discuss/Consider: Texas Communities Group for Code Enforcement assistance. (City Manager)

City Manager Archer discussed the potential need for assistance with Code Enforcement to get properties in town in compliance. There would be a company that could help with certification, enforcement, and hearings. The cost of the first year would be \$8200.00, which would include the

code enforcement and certifying our officer. This estimate was based on five properties in the first year. It was highlighted that the city had already identified more properties than that on the loop and some on main street. Commissioner Calvert expressed a desire to complete the tasks in house and trust in the current staff to get that accomplished.

Motion made by Commissioner Calvert to take no action.
Seconded by Commissioner Billings.

Unanimously Approved

Agenda Item 14: Discuss/Consider: Second reading for Ordinance No. 2025-06-09-A to Amend the City's existing Fee Schedule to reflect wording changes on service, reduce some existing fees, animal control fees, and incorporate language for a payment extension plan. (City Manager)

Commissioner Calvert expressed a desire to waive animal adoption fees at the discretion of the Animal Control Officer. Animal Control Officer Pilant discussed the changes she wished to make on the ordinance to the animal control fees. These changes included adoption fees, vaccination fees (with a focus on recovering the cost of vaccination in the adoption fee), multiple animal owner permits. Commissioner Calvert also suggested removing special event permits, and certain establishment licenses.

Motion made by Commissioner Calvert to remove the second part of i all of j and allow animal control fees as discussed.
Seconded by Commissioner Billings

Unanimously Approved

Agenda Item 15: Discuss/Consider: Legal Bill from Knight and Messor Fort Law Firms. (Finance Director)

Finance Director, Carol Stephens, assembled a document that included outstanding legal bills from both law firms. The legal bills were grouped in six primary groupings which included those related to the airfield legal suit, recall elections, EDC legal support, staff investigation, those related to the ECWSD, and other general legal support to the city. Carol discussed discrepancies in the invoices sent to the City of Ranger which she would attempt to clarify.

Motion made by Mayor Butler to take no action.
Seconded by Commissioner McCullough.

Unanimously Approved

Agenda Item 16: Discuss/Consider: RFP for Copier Contract Lease/Renewal (City Manager)

The City Manager expressed a need to get a third copier on the contract for the Fire Department; however, since the contract for City Hall and the Police Department had automatically renewed, only RFP for one copier lease would be included in the RFP.

Motion made by Commissioner Calvert to allow the RFP.
Seconded by Commissioner McCullough.

Unanimously Approved

Agenda Item 17: Discuss/Consider: Reopening bids for a tractor, a boom mower, and a towable woodchipper for the Wildfire Mitigation Grant. (City Manager)
Due to the lack of bids for various equipment (tractor, boom mower, and towable woodchipper), the City Manager asked the Commission to allow him to place the items back out to bid.

Motion made by Commissioner Calvert to request bids for tractor, mower, and woodchipper.
Seconded by Commissioner McCullough.

Unanimously Approved.

Agenda Item 18: Discuss/Consider: Disaster Preparedness and Coordination of Response for the City of Ranger. Update on the presiding officer for the city, assistant, manager, county POC and this year's Executive Guide. (Mayor Butler)

Mayor Butler expressed the importance of being prepared for all types of emergencies and discussed the roles being played in and by our municipalities. The mayor would be the presiding officer, the assistant manager would be the city manager, the Eastland County point of contact would be Judge Hullum. There are five (5) steps to be taken in an emergency that the Commission and the City would need to be familiar with which were included in the agenda packet.

Motion made by Mayor Butler to take no action.
Seconded by Commissioner McCullough

Unanimously Approved

Agenda Item 19: Discuss/Consider: Community Wildfire Defense Grant (CWDG) Purchase Updates. (City Manager)

The funding had not been received due to documents being needed but had been remedied that day. Once funding had been received, non-bid items could be purchased.

Motion made by Commissioner Calvert to take no action.
Seconded by Commissioner Billings.

Unanimously Approved.

Agenda Item 20: Discuss/Consider: Air Conditioner at the Ranger Animal Shelter (City Manager)

City Manager stated the entire Animal Shelter needed repair. The repairs needed included a new roof, holes in the walls, insulation issues, doors not sealing, and rust on the animal kennels. Commissioner Calvert discussed consideration of either a long-term loan or merging the animal shelters in the county.

Motion made by Commissioner Calvert to authorize the City Manager to talk about a county-wide shelter with point of contacts with Cisco and Eastland and work with staff to come up with needs based on current usage that included usage of both donations and financing.
Seconded by Commissioner McCullough.

Unanimously Approved.

Agenda Item 21: Discuss/Consider: Quarter Store Lease Agreement (Teresa Swindell)

Teresa Swindell with the Quarter Store clarified they were still looking for a Lease Agreement and would return next meeting with a list of items they were interested in for inclusion in the lease document, and a period for the lease.

Motion made by Commissioner Calvert the Commissioners send their questions or concerns to the Mayor’s office. The City Manager and the Quarter Store to address the terms to consider at a future meeting. Also allowing the Quarter Store to install a mini split at the City Manager’s approval.
Seconded by Commissioner Billings.

Unanimously Approved

Agenda Item 22: Discuss/Consider: Adjournment

Motion made by Commissioner McCullough to adjourn.
Seconded by Commissioner Billings.

Unanimously approved.

Adjourned at 19:54

These minutes were approved on the _____ day of _____ 20____

CITY OF RANGER, TEXAS

ATTEST:

Hope Delatorre, City Secretary

Robert Butler, Mayor

Manager's Report 6/23/25

2780.00 refund is being issued from North Texas State for the previous City Manager class.

Riddle Street cleanup- removed a very large pile of debris, cut down several trees along the bank of the creek, removed several large pieces of concrete that were in the path and opened up the creek on the other side of the road to allow for more water to drain.

The pump in question at the wastewater plant was taken back to replace the bearings that failed and has not been completed yet. We had two transducers that are responsible for the depth calibrations that were not responding, one was fixed and we had to order the other one. We are currently running on one pump that CSS had installed.

The Texas water development board that we applied for the grants with reached out on 6/18/25 for more information and the engineers are working on that.

The truck that the Police Dept. seized has been delivered to the City shop and we are currently checking it out to see exactly what shape it's in.

The box change from the Animal control truck was not a viable option for the former Police Chief truck as the bed is too short.

Reminder of bulk garbage pick up on every third Monday of the month, call the week before to be put on the list and it will get picked up.

City of Ranger
Expenses by Vendor Summary
May 1 through June 20, 2025

	May 1 - Jun 20, 25
Airgas USA, LLC	719.83
Amegy Bank of Texas	500.00
AT&T Mobility	734.79
Atmos Energy	483.15
Auto Zone	403.09
Battle Horse Electric LLC	3,683.30
Benchmark Business Solutions	748.23
Big Country Supply	78.38
Bound Tree Medical LLC	447.56
Brookshire's Grocery Company	482.28
Buenger & Associates, PLLC	3,960.00
Carrie Pilant	341.40
Cary Services	374.00
Certified Auto Glass	1,875.44
Charlie Archer	48.00
Chase	3,989.55
City of Abilene	200.00
Eastland County Appraisal District	6,364.18
Eastland County Veterinary Clinic	70.00
Eastland County Water Supply District	156,594.70
Eastland Heaven Sent Floral	110.00
Eastland Memorial Hospital	92.50
EHT	18,604.20
Evidence Management for Law Enforcement L	410.00
First Financial Bank	295.06
Flint Stone Services, LLC	2,200.00
Freddy Mitchell	0.00
FSS Mechanic Service	947.00
Greer's Western Store	326.80
H&R Feed & Fertilizer	90.00
Higginbothams Bartlett	805.96
IMC Waste Disposal	1,375.00
J & J Air Conditioning	1,555.97
J.T. Horn Oil Co., Inc.	917.79
James Logan	4,939.99
Jive Communications Inc.	653.74
Jose Meza	224.91
K&K Electric	105.00
Ken Charman	650.00
Kennedy Computer Solutions Inc.	5,918.00
King Insurance Agency	316.00
Lambert Little	1,239.04
Marguerite Anna Williams	1,183.00
MARK A KAISER CPA	1,500.00
Mueller Co., LLC	0.00
O'Reilly Auto Parts	79.99
Optimum Business	88.43
Pest Patrol	175.00
Petunia Jane's	245.00
PVS DX, Inc.	60.00
Ranger Economic Development Corp	7,370.58
Republic Services	29,699.66
RVS Software	798.77
Southern Petroleum Laboratories, Inc.	3,539.00
Standard Insurance Company	491.47
Tammy Archer	209.17
Texas Comptroller of Public Accounts	6,003.07
Texoma Advanced Electrical & Controls	675.00
The Gorman Progress	167.90
Tindall's Hardware	1,048.45
TML Health Benefits Pool	43,124.67
TML Intergovernmental Risk Pool	18,118.58
TMRS	14.54
TXU Energy	6,119.66
United States Postal Service	326.55
V&J Service Center	200.00

9:10 AM

06/20/25

Accrual Basis

City of Ranger
Expenses by Vendor Summary
May 1 through June 20, 2025

	<u>May 1 - Jun 20, 25</u>
W.E. Greenwood Auto Parts	282.00
White's Ace Hardware	25.00
WrapStar.US	181.00
Yellowhouse Machinery Co.	106.09
TOTAL	<u>345,707.42</u>



IT POLICY MANUAL

Network Use Requirements and Best Practices

*To Protect Your IT Network, Data, and Business
From Cybersecurity Threats and Other Risks*

Created by:

Chance Isham
KCS

Prepared for:

Charlie Archer City of Ranger

Table of Contents

IT POLICY MANUAL

INTRODUCTION

ACKNOWLEDGEMENT & RELEASE

PROHIBITED USES OF YOUR IT NETWORK

ACCOUNT MANAGEMENT, ACCESS & AUTHENTICATION POLICY

ANTI-VIRUS POLICY

PASSWORD POLICY

INTERNET POLICY

SECURITY INCIDENT REPORTING & RESPONSE

E-MAIL POLICY

COMPANY MOBILE DEVICE POLICY

PERSONAL DEVICE (“BYOD”) POLICY

INTRODUCTION

We'd like to begin by acknowledging one undeniable truth: no one likes IT policies – they're boring, technical, and take some work to understand and implement.

However, creating a solid set of rules and training team members to follow basic best practices when using any company network or device is a necessary "growing pain" that all successful small businesses have to go through in order to ensure the integrity of their IT infrastructure and the security of sensitive data.

Our goal is never to impose unnecessary restrictions on Your operations, but to protect your business from unnecessary interruptions, monetary losses and legal liabilities.

In many cases, risks like viruses, data breaches, ransomware attacks, compromised systems – and the resulting losses and liabilities that follow – *can* be minimized and even prevented when users abide by some basic IT security rules.

In addition, following the best practices described in these Policies ensures that your technology functions as intended – fast, reliable, and supportive of Your operations.

Because a security breach can result in loss of information, damage to critical applications, loss of revenue, massive legal liabilities and damage to the organization's reputation and public image, it is essential that all personnel who use or access data on Your IT Network (including employees, contractors, consultants, temporary users, and other users/workers who may have access to any account, data or device on the network) follow the requirements of the Policies in this Manual and understand what is required of them in terms of using electronic devices, network resources and company information.

These Policies may be amended and supplemented from time to time to reflect the latest industry standards, best practices and the newest solutions to the constantly evolving security threats that small businesses face every day. We will notify You of any updates by sending an e-mail with the updated policy to Your Designated IT Contact.

The definitions used in your MSA and/or Client Handbook apply to all capitalized words and phrases used in the Policies in this Manual, unless another definition is specifically provided in the Policy.

ACKNOWLEDGEMENT & RELEASE

While We are experts in cybersecurity, even the most advanced IT firms with the most up to date, cutting-edge technology suite cannot protect a network and its data where users and administrators don't do their part in following basic security measures and industry best practices. In short, the protection of Your IT Network requires that we all do our part.

The Policies contained in this Manual outline the actions required of You and Your team in order to minimize exposure to common and well-known cybersecurity risks and ensure that Your IT Network functions as intended.

To ensure compliance with these Policies, all of Our clients are encouraged to implement internal systems, procedures and policies that reflect the requirements contained herein, and to require all employees, contractors and other users to review, accept and promise compliance in writing before being granted a device and/or access to any company-owned IT infrastructure/resources.

If You need help creating internal IT policies for Your organization, give us a call at (254) 631.7741 or contact Your Account Manager, who can either help you, give You a quote for this service, or refer You to one of Our trusted partners in legal/compliance.

Having all users follow the established industry best practices outlined in this Manual is essential to Our ability to do Our job.

Accordingly, if Your IT Network or any sensitive data is breached, exposed or compromised due to actions that are not in compliance with the Policies in this Manual and/or Your failure to follow Our specific recommendations regarding any hardware, software, security measure, policy or process, You fully accept all risks associated with such actions and agree that We are not liable for any losses or damages that may result.

By working with us, You agree to release, indemnify and hold Us harmless from and against any and all liabilities, claims, causes of action, lawsuits and/or demands that arise out of or are in any way related, directly or indirectly, to Your decision not to follow the Policies set forth in this Manual, as amended from time to time, and/or Our advice or recommendation with respect to any hardware, software or security solution which We advised you to install, implement, change, replace, upgrade or delete.

In addition, any labor that We perform to mitigate issues resulting from actions that are contrary to Our recommendations and/or the Policies contained in this Manual, is considered to be outside the scope of any Managed Service Plan and is billable according to Our hourly rates set forth in Your MSA.

For example, if a cybersecurity / data breach, data loss or other damage occurs involving any hardware, software or equipment which We recommended to be installed, upgraded or replaced, You accept full responsibility for remediating any such loss, breach or damage, and further accept and agree that any labor performed by Us to repair any damage or otherwise handle any issues associated with such loss, breach or damage will be billable at Our standard hourly rates.

By signing this form below, You acknowledge that:

1. You have read and agree to all terms set forth above;
2. You have read and agree to follow and abide by the requirements and recommendations set forth in the Policies in this Manual;
3. You will implement internal/organizational policies and procedures to ensure that all employees, contractors, team members and other authorized users of Your IT Network comply with the Policies in this Manual;
4. You agree to release Kennedy Computer Solutions, Inc. from any and all liabilities for losses and damages which arise from or relate to any action not in compliance with the Policies and recommendations contained in this Manual, as detailed herein.

City of Ranger
Charlie Archer
City Manager

1
=



PROHIBITED USES OF YOUR IT NETWORK

Let's start with the easy stuff – any activities that are illegal under local, state, federal or international law are strictly prohibited. Under no circumstances are You or any of Your personnel authorized to engage in any such illegal activities while using Your IT Network.

In addition, the following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or entity protected by intellectual property (“IP”) laws of any applicable jurisdiction. IP law includes copyright, trademark, patent, trade secret and similar regulations. This includes but is not limited to:
- The installation, use or distribution of software products and subscriptions without obtaining the appropriate license that allows such activities.
- The use, reproduction and distribution of copyrighted graphics, photographs, written content, music and other copyrighted content for which You or the end user do not have an active license that allows such activities.
- Downloading, installing or otherwise introducing malicious software into Your IT Network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) or engaging in security breaches/disruptions of network communication, unless such activity is a part of the user’s normal job or duty. Examples include, but are not limited to:
 - accessing data of which the user is not an intended recipient;
 - logging into a server or account that the user is not authorized to access;
 - engaging in disruptive activities such as network sniffing, ICMP floods, denial of service, IP spoofing, forged routing information and other similar activities with a malicious purpose;
 - engaging in any form of network monitoring that intercepts data not intended for the user;
 - circumventing the security, for example the user authentication, of any host, network or account;
 - intentionally interfering with or disabling a user's terminal session via any means.
- Revealing or failing to take reasonable steps to protect passwords as required by the Password Policy. This includes allowing the use/access of accounts by anyone other than the user to whom the password is assigned (unless an exception applies, such as authorized administrative staff acting on behalf of the account owner).
- Engaging in any activity that violates the privacy rights of any employee or third party or using Your IT Network to procure or transmit materials violating laws that protect workers in the user's local jurisdiction, such as sexual harassment, non-discrimination, hostile work environment, and other similar regulations.
- Altering, modifying, or adding to any component of Your IT Network without Our express written approval. This includes but is not limited to:
 - Downloading or installing any software, patches or updates on any computer or mobile device owned or serviced by Us;
 - Altering, disconnecting or moving any hardware owned or serviced by Us;
 - Using or connecting any hardware to Your IT Network without a compatibility review by Us;
 - Engaging in any activity that may a) degrade, slow or hinder the performance of any component of Your IT Network; b) deprive an authorized user access to a device or the network; c) circumvent any Policy in this IT Policy Manual;
 - Engaging in any activity which We have advised would jeopardize or compromise the safety, security, reliability, speed, or functionality of Your IT Network.

- Downloading or installing any software or tools that reveal passwords and private information, or otherwise exploit any weakness in the security of Your IT Network. This includes any and all spyware, port scanners, password cracking programs, and similar applications.

I acknowledge that I have received and read the above Policy, and agree to follow the requirements and recommendations set forth above. I further acknowledge and agree that circumventing this Policy for the sake of convenience / ease of use, whether done by users or administrators, absolves Kennedy Computer Solutions, inc. from any liability whatsoever in connection with any losses or damages which may result from such actions.

City of Ranger
Charlie Archer
City Manager

ACCOUNT MANAGEMENT, ACCESS & AUTHENTICATION POLICY

Implementing consistent standards for account setup, management, authentication and network access reduces the risk of security incidents and is often required by regulations and third-party agreements.

The purpose of this policy is to outline the steps to ensure that user accounts are properly managed and that all users connecting to Your IT Network are appropriately authenticated.

Account Setup

The following policies apply to account setup:

- HR should confirm employee identity, title and job functions (for purpose of determining access limits) for any user to be granted access to Your IT Network.
 - Accounts must be set up with appropriate login credentials. All user names must use a consistent standard format (i.e., first initial + last name or firstname.lastname, with additional letters of the first name to be added until a unique username is created should a redundancy arise), and passwords must comply with the Password Policy.
 - All user accounts should be configured with the most restrictive set of rights, privileges and access permissions required for the performance of the user's job duties.
 - All devices connecting to Your IT Network must be configured to request authentication. If authentication cannot occur, then the machine should not be permitted to access the network.
 - Accounts must be for individual personnel only. Account sharing and group accounts are highly discouraged.
 - Users must not be given administrator or "root" access unless necessary to perform the functions of their position.
 - In the event that guests have a legitimate business need to access Your IT Network, temporary guest access may be allowed, provided that a) the request is formally made and approved by a manager with authority to do so; and b) it is specifically limited to only those resources that are required by that guest, and disabled when no longer needed.
 - All personnel requiring access to highly sensitive, proprietary or confidential information must have an individual account set up with special access permissions. Such accounts may be subject to additional monitoring or auditing at the discretion of the appropriate supervisory or executive team, and/or as required by applicable regulations or third-party agreements.
-
- Users may be granted access only if they acknowledge and accept, in writing, the requirements of all Policies in this IT Policy Manual.

Account Use & Management

- All accounts must have a unique username and password. Shared user accounts (whereby two or more users access Your IT Network under the same credentials) are not permitted.
- Passwords for all accounts must comply with ALL requirements of the Password Policy.
- Any device/account connecting to the network can have a serious impact on the security of the entire network. Accordingly, users should confirm that their antivirus software, as well as other critical software, are always upgraded to the latest versions before accessing the network.
- No one is authorized to establish, activate, modify, disable, or remove any user accounts from Your IT Network without Our express written approval.
- HR should notify Your internal IT management or KCS of all staffing changes, including employee termination, suspension, or a change in job functions, in order to ensure that a) access permissions can be adjusted so that they are always an accurate reflection of the team member's job requirements; and b) accounts of terminated employees can be disabled, and any devices used by them returned and wiped.

Monitoring & Restrictions

- We monitor user accounts for inactivity. If an account is found to be inactive for 60 days, We will notify You of pending disablement. Unless otherwise instructed, We will disable the account if it remains inactive for an additional 30 days from Our notice of inactivity.
- We periodically conduct account audit reviews to ensure that all accounts and network resources are appropriately used and managed.
- All businesses should have written policies in place regarding a) whether users' access is removed or maintained while on a leave of absence or vacation; and b) the criteria and process for modifying a user account based on name changes, position changes and permission changes.

Remote Network Access

Remote access to Your IT Network can be provided to users for convenience; however, this carries its own security risks. For that reason, We recommend setting up remote access to require the use of two-factor authentication.

In addition, the following requirements apply to all users accessing Your IT Network remotely:

- All remote access must be strictly controlled via approved encryption methods (such as VPNs) and strong pass-phrases.
- Users must never share their login and password with anyone, including family members.
- Before remotely connecting to Your IT Network, users should confirm that the remote host is not connected to any other network at the same time, except

personal networks that may be under that user's or an authorized third party's complete control.

- All devices connected to Your IT Network, remotely or otherwise, must use the most up-to-date anti-virus software approved by Us.
- All Policies in this IT Policy Manual apply to remote users the same way they apply to everyone else.

Failed Logins

Repeated login failures could be a sign of an attempt to "crack" a password to obtain unauthorized access Your IT Network and sensitive data. In order to protect Your business from password-guessing and brute-force attempts, any user account with 5 consecutive failed login attempts will be locked. Depending on Your preference, the lockout may be for a specific amount of time (less secure) or require a manual reset by Us (more secure).

While all Policies in this IT Policy Manual apply to remote users of Your IT Network, the following Policies are particularly important and should be thoroughly reviewed before accessing the network remotely: [Password Policy](#); [Internet Policy](#); [Mobile Device Policy](#); [Personal Device \("BYOD"\) Policy](#).

Account Management, Access & Authentication Policy Acknowledgement

I acknowledge that I have received and read the above Account Management, Access & Authentication Policy, and agree to follow the requirements and recommendations set forth above, and as may be supplemented or modified via amendment from time to time.

I further acknowledge and agree that circumventing this Policy for the sake of convenience / ease of use, whether done by users or administrators, absolves Kennedy Computer Solutions, Inc. from any liability whatsoever in connection with any losses or damages which may result from such actions.

City of Ranger
Charlie Archer
City Manager

ANTI-VIRUS POLICY

Any IT Network and device connected to the Internet is exposed to security risks that threaten to wipe out data, render devices inoperable, expose sensitive and confidential information, hold data hostage until a ransom is paid, and cause businesses to be exposed to lawsuits, fines and other liabilities.

Common Cybersecurity Threats

Some of the most common cybersecurity threats that affect all businesses include the following:

Malware: Malware is the general collective term used to refer to software specifically designed to damage, disrupt or gain unauthorized access to a computer, system, server or network. It includes viruses, worms, spyware, ransomware and other software/code designed to cause damage to data or gain access to a network. It is usually delivered via email, in the form of a link or file, and is "activated" when the user clicks on the link or opens the file.

Virus: Computer viruses – a type of malicious code or program written to alter the way a computer operates – cause billions of dollars' worth of economic damage each year. Viruses are designed to spread from one computer to another, and have the potential to cause widespread damage to Your IT Network, such as harming the system software by corrupting or destroying data.

Trojan Horse: A Trojan horse is a type of malware that is used by hackers and thieves to gain access to a computer or system. They infect systems by tricking the user into opening the file, which is usually disguised as legitimate software. Once activated, Trojans can enable criminals to spy on you, steal your data, gain access to your system, and otherwise damage, disrupt, and inflict harm upon your data and IT Network.

Worm: A worm is a malicious software that replicates itself and spreads through networks like a virus. They are generally designed to target pre-existing vulnerabilities in the operating system of the computers they attempt to infect in order to steal data, install backdoors that can be used to access the network, and cause other types of harm. Worms consume large amounts of bandwidth and memory, which can lead to networks, devices and servers malfunctioning due to overload. Many of the most destructive types of malware have been worms.

Spyware: Spyware is loosely defined as software with malicious behavior that aims to enter your computer, perform surveillance to gather information about a person or organization, and send such information to another entity so that they may profit from the stolen data. Spyware activity leaves you open to data breaches and associated liabilities, while also slowing down network and device performance.

Adware: Adware refers to unwanted software designed to display advertisements to the user, most often in a web browser. It usually either disguises itself as legitimate software in order to trick the user into installing it, or it may get on a computer by being secretly buried in legitimate software. Once on a device, it engages in unwanted activities such as analyzing the websites visited, displaying burdensome advertisements, and sell your browsing behavior and other information to third parties.

Keyloggers: Keyloggers are a type of monitoring software designed to record every keystroke made by a user on any website or application, and send the information to a third party. Criminals use keyloggers to steal personal, financial and other confidential information such as passwords, banking details, and trade secrets. Some keyloggers can record audio/video, GPS location, and screenshots.

Ransomware: Ransomware is a form of malware that encrypts a victim's critical data, so that the organization cannot access its files, databases, or applications. In order to restore access, the organization must pay the attacker a specified sum. Ransom amounts demanded range from a few hundred dollars to tens of thousands and more. Ransomware often spreads quickly, encrypting files across a network and target database and file servers. It can easily paralyze an entire organization. Due to its effectiveness, it has cost businesses billions of dollars in damages and payments to cybercriminals.

Steps We Take to Prevent Malware Issues

On every file server and device that We service, We ensure that anti-virus software is installed, actively running, and configured to be automatically updated. We also install e-mail virus protection software to protect each e-mail gateway and periodically scan all computer devices for malware.

Once We have installed all required software, altering the settings in any manner is strictly prohibited, as inexperienced users may cause the effectiveness of the software to be reduced or eliminated. Users are specifically prohibited from altering the automatic update frequency of the virus protection software.

If a virus is detected, We may disconnect the infected device(s) from the network to prevent propagation of malware to other devices and resulting damages, until the infection has been removed.

User Requirements

All users must take the following precautionary measures in order to avoid unnecessary business interruptions and monetary losses caused by computer viruses:

- Never open any attachments to any e-mail from an unknown, suspicious, or untrustworthy source. If anyone is unsure about an e-mail, We are always available to take a look and potentially avoid a costly and disruptive security incident.
- All SPAM, chain, or other junk mail should be deleted without opening or forwarding.
- Users must never download files from the Internet on any work devices unless specifically authorized by Us – especially not from unknown or suspicious sources.
- Removable media (such as CDs, USB drives, external hard drives) must always be scanned for viruses before using it.
- If Your service plan includes data backup, all data saved to network drives is backed up at regular intervals. Clients who have opted out of this service should take measures to back up all critical data on a regular basis and store the data in a safe place.

Incident Reporting

If any user detects or suspects that a virus that was not automatically cleaned by the anti-virus software, this should be treated as a security incident and must be immediately reported to Us by following the steps in the Security Incident Reporting & Response Policy so that any potential security issues can be mitigated before they have a chance to get out of hand or cause greater damage.

Anti-Virus Policy Acknowledgement

I acknowledge that I have received and read the above Anti-Virus Policy, and agree to follow the requirements and recommendations set forth above, and as may be supplemented or modified via amendment from time to time.

I further acknowledge and agree that circumventing this Policy for the sake of convenience / ease of use, whether done by users or administrators, absolves Kennedy Computer Solutions, Inc. from any liability whatsoever in connection with any losses or damages which may result from such actions.

City of Ranger
Charlie Archer
City Manager

PASSWORD POLICY

Since weak passwords can compromise even the most secure IT networks, this policy is designed to ensure that the passwords used in Your organization are strong, secure, and provide a reasonable level of security for your network without posing an undue burden on users. Strong passwords are the first protection for user accounts and as such, they are a mandatory element of all cybersecurity solutions.

User Account Password Policy

- Passwords must be used for all computers connected to Your IT Network.
- Passwords must be at least 10 characters in length – typically, the longer the password, the more secure it is.
- Passwords must be changed every 60-90 days.
- Passwords must contain a combination of alpha, numeric, and special characters, where the computing system permits (!@#%&* _+=?).
- Passwords should not contain information such as a name, proper name, acronym, or a dictionary word in any language.
- Passwords should never be linked to any personal information about the password owner such as an address or phone number, a birth date, social security number, relatives' names, etc.
- Passwords may not be reused for at least 1 year.
- Screensaver passwords are recommended for PCs that are only used by one user, as they increase security by removing the opportunity for an intruder or unauthorized employee to access network resources through an idle computer. Screensaver passwords are not permitted for computers shared by more than one user, as they violate the "no shared passwords" policy.

System-Level Password Policy

- All system-level passwords must be at least 12 characters in length and contain at least 3 of the following: upper case, lower case, numbers, and special characters.
- Passwords must be changed at least every 90 days.

Rules Applicable to All Passwords

- The same password should never be used for multiple accounts.
- All passwords are to be treated as strictly confidential and must not be disclosed to anyone, including co-workers, managers, or family members.
- Passwords must never be shared over the phone or disclosed on questionnaires or security forms.
- Passwords must not be shared via e-mail, instant message, text or any other form of electronic communication without encryption. Because interception of this information can result in a serious security incident, authentication credentials must always be encrypted during transmission across any network.
- Users must not use password hints from which a third party may deduce the password (for example, "mother's name", "home address", etc).
- Passwords must not be stored physically, such as written down on a notepad or post-it. Passwords may be stored in a file on a computer system or mobile device (phone, tablet) if they are appropriately encrypted.
- Circumventing password entry via auto log-ons, application remembering, embedded scripts, hard coded passwords in client software, or otherwise, is strictly prohibited unless written approval is provided by Us and any additional security measures recommended by Us have been implemented.
- Security tokens (such as smartcards, key fobs, etc.) must be immediately returned by any user whose relationship with the business was terminated for any reason.

If there is any reason to believe that the security of an account may be compromised, You must:

1. Notify Us immediately via the methods specified in the Security Incident Reporting & Response Policy
2. Change the password (ensuring that the new password is compliant with the Password Policy)
3. If applicable, take control of and protect/destroy any passwords that may have been found written down or stored electronically without encryption

Password Policy Acknowledgement

I acknowledge that I have received and read the above Password Policy, and agree to follow the requirements and recommendations set forth above, and as may be supplemented or modified via amendment from time to time. I further acknowledge and agree that circumventing this Policy for the sake of convenience / ease of use, whether done by users or administrators, absolves Kennedy Computer Solutions, Inc. from any liability whatsoever in connection with any losses or damages which may result from such actions.

City of Ranger
Charlie Archer
City Manager

INTERNET POLICY

General Internet Use & Access Policy

The following policies apply to all users and devices accessing the Internet:

- All software by which users access the Internet must be a) part of the Our Standard Technology Suite or otherwise approved by Us; b) up to date on all upgrades and incorporate all vendor-issued security patches; and c) contain our Endpoint Detection & Response software d) contain our security operations center software e) be encrypted
- PCs on Your IT Network may access the Internet only through Internet firewall or equivalent security device approved by Us.
- Bypassing any network security requirements outlined in this Policy, by accessing the Internet directly, is strictly prohibited.
- Accessing the Internet for the purposes of gaining unauthorized access to local and remote computer systems, software piracy, illegal activities, the transmission of threatening, obscene, or harassing materials, or personal solicitations, is strictly prohibited. Likewise, using the Internet to propagate malware is strictly prohibited.
- Downloading or installing any software from the Internet on any device connected to the IT Network without Our express written approval, is strictly prohibited.
- All software and files downloaded from the Internet must be scanned for viruses using the software designated or approved by Us for this purpose. If a virus is detected or suspected, We must be notified immediately so that we can take steps to mitigate any potential threat before it has a chance to cause further damage.
- If software is downloaded, it may only be used in conformity with the terms of its license and applicable intellectual property laws.
- Users should have no expectation of privacy in anything they create, store, send, or receive using the company's Internet access.
- All confidential and sensitive information transmitted over the Internet or any external network must be encrypted.
- Accessing websites containing sexually explicit material or other material deemed inappropriate in the workplace – along with any display, storing, archiving, or editing of such content on any company device – is strictly prohibited. To reduce Our clients' legal risks, We use software that identifies and blocks access to such websites. However, in the event that such a site is not automatically blocked and a user accidentally connects to same, the user must immediately disconnect from the site and the incident must be reported to Us immediately.

Incidental / Personal Use

To minimize security risks, incidental personal use of Internet access (this may include browsing for entertainment, playing games, participating in chat groups, uploading or downloading large files, streaming audio and/or video files, and other non-business purposes) should be restricted to a reasonable minimum, and should only be permitted for

company personnel (i.e. it should not extend to family members or other third parties). Storage of personal files and documents within Your IT Network should be nominal.

Personnel should be advised that a) sending or receiving files or documents that may cause legal liability to the business should be strictly prohibited; and b) all files and documents, including personal files and documents, which are stored on Your IT Network are owned by the company and may be subject to open records requests, and may be accessed in accordance with this policy.

Computer resources, network bandwidth and storage capacity are not unlimited. As such, all users should be instructed to refrain from knowingly engaging in activities that waste or unfairly monopolize resources, or which are not essential to the performance of their job duties.

Our Rights

- **Restricting Access:** In order to protect Your data and network, We may restrict access to programs, web apps and websites that harm network performance or which are known or found to be high-risk or compromised by malware. We may, in Our discretion, use technical controls to restrict users' ability to download and install software.
- **Monitoring:** We may monitor, log, and analyze any and all user activity on Your IT Network. This includes, but is not limited to, monitoring and logging all Internet sites visited by users; social media usage; any chat, newsgroup and forum activities; file downloads and uploads; application usage; and all communications sent and received by users.

Internet Policy Acknowledgement

I acknowledge that I have received and read the above Internet Policy, and agree to follow the requirements and recommendations set forth above, and as may be supplemented or modified via amendment from time to time.

I further acknowledge and agree that circumventing this Policy for the sake of convenience / ease of use, whether done by users or administrators, absolves Kennedy Computer Solutions, Inc. from any liability whatsoever in connection with any losses or damages which may result from such actions.

City of Ranger
Charlie Archer
City Manager

SECURITY INCIDENT REPORTING & RESPONSE

When it comes to security breaches – and responding to them – time is of the essence. The longer a cybersecurity incident such as a data breach or exposure goes undetected, the greater the damage such an event can cause.

As such, it is absolutely essential that any individual who finds out or suspects that a security incident has occurred, must immediately contact Us to provide a full description of the events and all available information via the following methods:

E-Mail: support@kennedycsi.com
Phone: 254.631.7741

Examples of reportable incidents / suspicious circumstances:

- You become aware that a password has been compromised.
- You have identified a virus or other malware infection.
- A theft, breach or exposure of Your data or IT Network has occurred.
- You notice that Your network security or firewall has been uninstalled or disabled; you can't restart your anti-malware program or firewall and you didn't turn it off.
- You notice an increase in error messages while completing routine tasks
- Computers are freezing, crashing or running slowly for no apparent reason
- E-mails from company addresses are being sent without Your knowledge, You are accused of sending SPAM.
- Your Internet browser suddenly displays toolbars and extensions that you don't recognize
- A password has suddenly changed without Your knowledge
- You notice that files are missing or being deleted from Your network
- You notice files are being re-named
- You receive a ransom demand
- You are unable to access files or applications

Next Steps in Responding to a Security Incident

Once a report is received, We will launch an investigation into the issue to confirm whether a theft, breach or exposure has occurred, and will follow the appropriate response procedure based on those findings.

If a breach has occurred, We may be required by Our insurer and legal team to provide access to forensic investigators and experts tasked with determining the nature and extent of the breach; the data that has been impacted or exposed; the number of individuals and/or organizations affected; and to determine the root cause of the breach or exposure.

We will also work with Your communications, legal, HR and other relevant departments in handling and communicating the events to employees and team members, the public, and any clients, end users and other parties directly affected by the breach.

Security Incident Reporting & Response Policy Acknowledgement

I acknowledge that I have received and read the above Security Incident Reporting & Response Policy, and agree to follow the requirements and recommendations set forth above, and as may be supplemented or modified via amendment from time to time.

I further acknowledge and agree that circumventing this Policy for the sake of convenience / ease of use, whether done by users or administrators, absolves Kennedy Computer Solutions, Inc. from any liability whatsoever in connection with any losses or damages which may result from such actions.

City of Ranger
Charlie Archer
City Manager

E-MAIL POLICY

E-mail has inherent security risks, which must be proactively addressed in order to avoid viruses or malicious code disrupting Your IT Network and your ability to do business. The following policies are designed to protect Your business from the most common risks associated with business e-mail use:

Anti-Virus and Monitoring

For clients on our E-mail Security Plan, we have software in place that scans all incoming and outgoing e-mails for spam and malicious code and files/attachments. If an attachment has an extension commonly associated with malware or is otherwise classified as high risk, it will be removed from the e-mail prior to delivery. In addition, e-mails from domains and IP addresses associated with malicious actors will be rejected, and messages identified as spam will be quarantined for the user to review.

Any e-mail account sending out spam will be shut down until You notify us that the issue has been addressed and the account should be reinstated. Likewise, any outgoing e-mail containing attachments with viruses or malicious code will be prevented from sending. Allowing such activities would not only harm the recipient's system, but may also result in legal liability, regulatory fines and significant damage to Your organization's reputation.

Retention and Archiving

To ensure that your Network runs optimally while giving you access to your messages for as long as possible, we have implemented the following policies regarding retention and archiving:

- E-mails, calendar entries, tasks and notes are retained for 60 months, after which they are automatically purged.
- Deleted and archived e-mails are automatically purged after 60 months from the original send/receive date.
- Archived e-mails are only accessible by the owner of the account and the system administrator.

Diligence in E-mail Communications

All team members should be trained to recognize e-mail spoofing: the criminal practice of sending e-mails with a forged header that makes it appear as though the message was sent by someone other than the actual sender. The objective is usually to induce the recipient to open the e-mail, and either download a malicious file or inadvertently provide sensitive data or make a fraudulent payment to a criminal.

Employees should be trained to identify spoofed e-mail; should never open or respond to them; and should under no circumstances download any attachments. Users must use caution when opening attachments from unknown senders, as this is how many instances of malware infection occur.

If suspicious e-mail activity has been detected, users should be trained to report it immediately to the appropriate supervisory personnel and You must in turn notify Us immediately so the issue can be addressed.

Encrypting and Protecting Sensitive Content

All data sent via e-mail should be treated as sensitive information. Users should never send work documents or information to anyone outside of the company unless it is a required part of business and the contact is known and trusted. Additionally, sensitive

information such as passwords, social security numbers, credit card and bank account numbers, pin numbers, and other information from which accounts can be hacked (think mother's maiden name, etc.) should never be sent without encryption. When data is sent encrypted, passwords to decrypt the data should not be sent via e-mail.

In order to ensure compliance with this policy, all e-mail activity on Your IT Network is subject to monitoring, logging and review.

Because there is nothing we can do to proactively monitor and protect information sent to or from personal accounts, team members should be discouraged from sending, receiving or forwarding confidential or sensitive information via personal e-mail accounts such as Gmail, Hotmail, Yahoo, etc.

Users must also comply with the Personal Device Policy for sending, forwarding, receiving, or storing information relating to your business.

Company E-mail and Personal Business

Just as storage of personal files and documents by employees on Your IT Network should be kept to a minimum, team members should also refrain as much as possible from using company e-mail accounts to send messages and files to family members, personal contacts, or other acquaintances.

Not only do such activities pose a heightened security risk, but it also increases the potential of subjecting Your organization to unnecessary legal liabilities arising from the transmission of files, messages and documents to contacts with no business relationship to your company.

It is also important to note that business e-mail is not private. All e-mails, files, and documents sent through the company network – including personal ones – are typically considered property of the organization, and may be subject to open records and similar requests.

E-Mail Conduct That Can Jeopardize Your Business

In order to protect Your business from unnecessary legal liabilities and damage / interruption to Your e-mail service, the following activities are prohibited:

- Using company e-mail to send messages that may be deemed intimidating, harassing, or offensive. This includes, but is not limited to: abusive language, sexually explicit remarks or pictures, profanities, defamatory or discriminatory remarks regarding race, creed, color, sex, age, religion, sexual orientation, national origin, or disability;
- Sending SPAM in any form, including unsolicited advertising or "junk mail" to individuals who did not specifically request such material, or creating/forwarding "chain letters" or promoting pyramid/Ponzi schemes;
- Sending unsolicited e-mails to large groups, except as may be appropriate in the ordinary scope of the sender's job duties;
- Knowingly sending or forwarding e-mails containing viruses or malicious code/software;
- Excessive use of company e-mail to conduct personal business;
- Violating copyright laws by illegally distributing protected works;
- Forging or attempting to forge e-mail messages or e-mail header information;
- Creating false identities to bypass any laws, regulations or policies;
- Using unauthorized e-mail software;
- Engaging in any activities for the purpose of circumventing this Policy, such as knowingly disabling the automatic scanning of e-mails for spam content, malicious code and attachments; or otherwise intentionally circumventing any e-mail security measures implemented or recommended by Us;

- Sending e-mails revealing any information known by the user to be confidential or proprietary, without specific authorization from the owner of the information;
- Sending e-mails that may harm or tarnish the image, reputation and/or goodwill of the organization and/or any of its employees.

E-Mail Security Incident Reporting

If You detect or suspect that an e-mail address on Your network has been compromised or that you have received malicious e-mail, You must notify Us in accordance with the Security Incident Reporting & Response Policy immediately so that any potential security issues can be mitigated before they have a chance to get out of hand or cause greater damage.

E-Mail Policy Acknowledgement

I acknowledge that I have received and read the above E-Mail Policy, and agree to follow the requirements and recommendations set forth above, and as may be supplemented or modified via amendment from time to time.

I further acknowledge and agree that circumventing this Policy for the sake of convenience / ease of use, whether done by users or administrators, absolves Kennedy Computer Solutions, Inc. from any liability whatsoever in connection with any losses or damages which may result from such actions.

City of Ranger
Charlie Archer
City Manager

COMPANY MOBILE DEVICE POLICY

As You probably already know, malware and other threats can enter IT networks through mobile devices in the same way that they infect PCs. Because a security breach can result in loss of information, damage to critical applications, and loss of revenue, it is important that all personnel who use mobile devices adhere to the requirements of this Policy.

All of Our clients are encouraged to implement internal policies that reflect the requirements contained herein, and to require all employees and other users to review and accept the terms of such policies before being granted a device and access to any company-owned IT infrastructure/resources.

Devices

This policy applies to all mobile devices belonging to Your organization that are used to access corporate resources and/or contain stored data belonging to You, Your clients and other parties. This includes but is not limited to mobile phones, tablets, laptops, notebooks, and other mobile devices owned by You and which are capable of storing corporate data and connecting to an unmanaged network.

Risks

Examples of the possible risks of using such devices to store, transfer, or access Your data and/or Your IT Network include:

- Devices and their contents being lost or stolen;
- Theft of proprietary and confidential information by an employee, contractor or third party;
- Potential legal liability for intellectual property infringement due to team members copying files and software onto personal devices without a license permitting same;
- Introduction of malware/viruses to Your IT Network via a mobile device;
- Non-compliance with applicable laws and regulations (and liability for fines, penalties and lawsuits) due to theft or exposure of financial, personal or other confidential data protected by privacy and identity theft legislation.

Registration, Monitoring & Support

- We manage network, application, and data access from all devices – including mobile devices – centrally, using technology solutions from Our Standard Technology Suite deemed suitable for this purpose. Any attempt to circumvent Our work in this regard will be deemed an intrusion attempt and will be dealt with accordingly.
- Prior to the initial use of any mobile device on Your IT Network, **the device must be registered on Your system by Us**. We will maintain a list of approved mobile devices and related applications and reserve the right to disconnect and refuse access to devices not on this list.
- We reserve the right to inspect and monitor all mobile devices attempting to connect to Your IT Network through the Internet (or other unmanaged network).
- We routinely patch and update mobile devices to ensure that all firmware, applications and operating systems are up-to-date and mobile devices are protected from vulnerabilities.
- We also perform routine security audits on mobile devices to ensure that no potential threats to the company IT Network and data are present.

- We reserve the right to temporarily restrict the ability to connect mobile devices to Your IT Network if We suspect that such equipment is being used in such a way that puts Your IT Network, its data, users, and your business at risk. We further reserve the right to limit the ability of any user(s) to download, transfer or access data to and from Your IT Network or specific components thereof.
- Users connecting mobile devices to outside infrastructure to access corporate data must employ a **personal firewall approved by Us**, along with any other security measure We deem necessary.
- Company owned laptop computers may only access the corporate network and data using an SSL, VPN, or IPSec VPN connection. Mobile VPN software must be installed on all smart mobile devices in order for users of these devices to access Your IT Network and data.
- In monitoring Your network, We may create audit trails and use the reports generated to optimize Our processes and for investigation of possible breaches and/or misuse. To identify unusual usage patterns, suspicious activity, and accounts/computers that may have been compromised, all end users' access and/or connection to Your IT Network may be monitored to record dates, times, duration of access, and the like.

Data Encryption Requirements

- All mobile devices that store corporate data **must use an approved method of encryption** to protect data.
- Laptops must employ full drive encryption with an approved software encryption package. No corporate data may exist on a laptop in clear text.

Passwords

- All mobile devices must be protected with a password that complies with the requirements of the Password Policy – including the requirements for password strength, confidentiality, storage and encryption.

Physical Security

- All users of company mobile devices must secure all such devices whether they are actually in use, being carried, or being stored while not in use.
-

- Passwords and confidential data may not be stored on unregistered personal/non-company devices.
- Corporate data must be permanently erased from all mobile devices once their use is no longer required. In such cases, please contact us immediately so We can assist with wiping this data.
- No person may perform any modifications to any hardware or software required or installed by Us without Our express written approval.

Reporting, Help & Support

- If a mobile device is lost or stolen, it must be reported to Us immediately. We use remote wipe software to disable and delete any data stored on a mobile device reported lost or stolen. Upon recovery, the device may be re-provisioned.
- While We offer support for mobile devices that meet Our hardware and software requirements, We are under no circumstances liable for any losses, damages, or issues caused by a) the use of unapproved media, hardware, or software; or b) any violation of Our policies, recommendations and requirements outlined in this Handbook or Your MSA. These limitations apply even if We are aware of the existence of nonconforming devices, software or practices.

Company Mobile Device Policy Acknowledgement

I acknowledge that I have received and read the above Company Mobile Device Policy, and agree to follow the requirements and recommendations set forth above, and as may be supplemented or modified via amendment from time to time.

I further acknowledge and agree that circumventing this Policy for the sake of convenience / ease of use, whether done by users or administrators, absolves Kennedy Computer Solutions, Inc. from any liability whatsoever in connection with any losses or damages which may result from such actions.

Charlie Archer
City Manager

PERSONAL DEVICE (“BYOD”) POLICY

While it may be unreasonable to require employees to leave their personal devices at home, certain steps must be taken in order to prevent unauthorized access to Your IT Network via employee's personal devices.

General Personal Device Security Protocols

We recommend implementing the following security protocols to minimize the risk of a data breach or other security incident:

- All personal devices that connect to Your IT Network or which store / have access to company data, should be protected with a password conforming to the requirements of the Password Policy.
- All personal devices should be configured to auto-lock after being idle for more than 5 minutes, with a password, pin, fingerprint, retina scan or unique drawing required to unlock.
- Devices should be configured to lock after 5 failed login attempts. Contact us to help with this setting, as well as for regaining access on devices that We have configured.
- “Jailbroken” devices should be restricted from accessing Your IT Network.
- Devices belonging to anyone who isn't a member of Your team should not be allowed to connect to Your IT Network.
- Access to company data via personal device should be limited to the permissions granted to the specific user. We should be contacted to set up user profiles and automatic access enforcement/restrictions on all personal devices used to access Your IT Network.
- All personal devices should use an approved method of encryption during transmission to protect data.
- Personal devices used to access Your IT Network may not be reconfigured without Our express approval.
- All users must agree in writing to immediately report any incidents or suspected incidents of unauthorized data access, data loss, and/or disclosure company resources, databases, networks, and the like.

Our Rights as Your IT Service Provider

In order to perform Our jobs, We reserve the right to do any of the following if deemed necessary to protect the security of Your IT Network and data:

- Configure and install any software We deem necessary to ensure the security of your IT Network (for example, anti-virus, remote wiping and other software) on any personal device used to connect to Your IT Network;
- Restrict or limit users' ability to download, install or use certain websites and applications;
- Limit the use of network resources by personal devices;
- Impose restrictions on users' ability to transfer data to and from specific resources on Your IT Network;

- Remotely wipe a user's personal device if needed, for example if the device is lost, the team member's relationship with the company is terminated, or if We detect a virus, data breach, policy breach, or other security threat to Your IT Network and data;
- Disconnect devices or disable services without notification;
- Periodically inspect and update personal devices to ensure that all firmware, apps, operating systems and security setting are up-to-date in order to prevent vulnerabilities and make the device more stable;
- Monitor all personal devices and activities to record dates, times, duration of access, etc. in order to identify unusual usage patterns, suspicious activity, and accounts/computers that may have been compromised;
- Treat any attempt to circumvent, bypass or contravene the security Policies as a security incident / data breach and respond accordingly. This includes terminating, without notice, any device's access to Your IT Network if We detect irresponsible, unethical, illegal activities, or actions in violation of the Policies set forth in this IT Policy Manual.

Liabilities, Risks & Disclaimers

- While We take reasonable precautions to prevent loss of personal data in the event that we must remotely wipe a device, at times these precautions fail. Accordingly, it is the user's responsibility to take additional precautions, such as backing up their personal media, email, contacts, and other data they wish to protect.
- Lost or stolen devices must be reported to Us within 24 hours. Team members should also notify their mobile carrier within 24 hours of a loss or theft.
- We are not responsible for any losses or damages if they result from a team member's use of a device that is illegal, unethical, or in violation of this Policy or Our recommendations. Any labor performed mitigating issues from such actions is outside the scope of any Managed Service Plan and is billable according to Our hourly rates set forth in Your MSA.
- All team members should execute an agreement by which they assume full liability for risks arising out of their use of their personal devices on Your IT Network. These include, but are not limited to, any loss or exposure of personal data or sensitive company information as a result of error, malware or other hardware/software failures on their personal devices.

Personal Device ("BYOD") Policy Acknowledgement

I acknowledge that I have received and read the above Personal Device "BYOD" Policy, and agree to follow the requirements and recommendations set forth above, and as may be supplemented or modified via amendment from time to time.

I further acknowledge and agree that circumventing this Policy for the sake of convenience / ease of use, whether done by users or administrators, absolves Kennedy Computer Solutions, Inc. from any liability whatsoever in connection with any losses or damages which may result from such actions.

City of Ranger
 Charlie Archer
 City Manager



MASTER SERVICE AGREEMENT

between

Kennedy Computer Solutions, Inc.

and

City of Ranger

This Master Service Agreement (hereinafter referred to as "MSA" or "Agreement") is between Kennedy Computer Solutions, Inc. ("We", "Us", "Our"), a Texas Corporation with a principal address of PO Box 1222, Eastland, TX 76448 and City of Ranger ("You"), of 400 W Main St, Ranger, TX 76470 (collectively referred to as the "Parties," "Both Parties," or "Each Party").

ARTICLE 1 – GENERAL

Applicability. The terms of this Agreement apply to a) all work that We perform on any hardware, software, equipment, accounts, network, IT system, configuration and infrastructure, and b) all products, services, properties and assets provided to You by Us or procured by Us on Your behalf (collectively, Your "IT Network").

Client Handbook and IT Policy Manual. By signing this Agreement, You agree to read and abide by the processes, procedures and policies outlined in Our Client Handbook and/or the IT Policy Manual, copies of which will be emailed to You before signing this Agreement

The **Client Handbook** contains important information about the day-to-day aspects of working with Us and the Technologies We use, such as:

- How to request Services;
 - Our response and resolution times;
-

- Issue priorities and service tiers;
- How You can request to escalate service issues;
- Designating, changing and working with Your Designated IT Contract;
- Working with your Account Manager;
- Our general hardware and software requirements and recommendations;
- How to order hardware or software;

The **IT Policy Manual** contains important requirements, recommendations and best practices that all users must follow in order to keep Your IT Network secure and functioning optimally.

By signing this Agreement, You acknowledge that failure by users or administrators to follow the policies and requirements set forth in the above documents, as amended from time to time, whether done inadvertently or intentionally for the sake of convenience / ease of use, absolves Us from any liability whatsoever in connection with any losses, claims or damages which may result from such actions.

You further acknowledge and agree that the Client Handbook and IT Policy Manual are proprietary information which constitute Our trade secrets and Confidential Information. As such they are subject to the confidentiality provisions of this Agreement and neither the contents of these documents nor any passwords provided by Us to access them may be shared with any third parties, unless otherwise required by law.

Standard Technology Suite. The Client Handbook contains a list of the technologies that We use to create a well-integrated, reliable and secure IT infrastructures for each of Our clients (Our “Standard Technology Suite”). While it is possible that We may be able to purchase and integrate hardware and software that are not listed in the Client Handbook as part of Our Standard Technology Suite, any tasks involving the installation, setup, maintenance and support relating to such products is considered outside of the scope of any Managed Service Plan, and as such may be billed at our Regular Hourly and After Hours and Emergency Rates outlined in **Appendix II**.

Independent Contractor Status. Notwithstanding any provision hereof, it is understood by both Parties that in providing the Services, We are serving as an independent contractor, and are neither an employee nor a partner, joint venturer or agent of You. With the exception of any licenses obtained by Us on Your behalf pursuant to this Agreement, neither Party shall bind or attempt to bind the other to any contract, and any such contracts entered into in violation of this provision shall be void and unenforceable. You will not provide fringe benefits of any kind to Us or Our members, employees, agents and other affiliates, including health insurance, retirement, paid vacation, or any other employee benefits. As an independent contractor, We are solely responsible for all taxes, withholdings, and other statutory or contractual obligations of any kind, including but not limited to

workers' compensation insurance. As an Independent Contractor, unless this Agreement or an applicable Service Schedule or Service Order specifically states otherwise, the manner in which the Services are to be performed, including but not limited to the scheduling of individual tasks and the specific hours to be worked by Us or Our employees, contractors and affiliates, shall be determined by Us. It is further understood that as an independent contractor, We may have other clients and may provide any services to any third party during the term of this Agreement.

ARTICLE 2 – TERM AND TERMINATION

Term and Termination. This Agreement begins on the date that it is signed by both parties ("Effective Date") and will remain in effect for **36 Months** ("Commitment Term") unless it is terminated by either You or Us in compliance with the Termination provisions below. After the expiration of the original Commitment Term, this Agreement will **automatically renew** for subsequent **Commitment Terms of the same duration as the original Commitment Term**, and will continue until terminated by You or Us as specified in the Termination clause below.

Termination by You. In the event of a Consultant Default, as defined in this Agreement, this Agreement may be terminated by You with immediate effect by providing Us written notice of the termination. In the absence of a Consultant Default, You may terminate this Agreement by providing Us with **ninety (90) days'** written notice ("Termination Notice Period") if:

- You are not on a Managed Service Plan; or
- You are on a Managed Service Plan, and You are providing Us with **90-day** notice of Your intent not to renew this Agreement upon the expiration of the Commitment Term;
- You are on a Managed Service Plan and You wish to terminate this Agreement prior to the expiration of the Commitment Term. By signing this Agreement, You acknowledge that any such termination is only valid and effective if, in addition to providing Us with **90 day's** notice, You also remit payment to Us in the full amount of any Termination Payment due, along with any other outstanding charges payable to Us, no later than the Termination Payment Due Date, as those terms are defined in the paragraph below.

By signing this Agreement, You acknowledge and agree that the pricing for Our Managed Service Plans is a special discounted fixed monthly rate based on the specific promise of a minimum commitment by You to pay all Monthly Managed Service Fees for the entire duration of the applicable Commitment Term. Managed Service Plans are NOT month-to-month subscriptions and are NOT subject to termination at Your convenience without remitting payment of a termination fee.

Accordingly, if Our Services to You include any of the monthly managed services listed in Appendix I under the "Managed Service Plan" heading, You acknowledge and agree that, if You terminate this Agreement before the end of the Commitment Term for any reason other than a Consultant default, You are legally obligated to pay the Monthly Managed Service Fee stated in Appendix II multiplied by the number of months left in the Commitment Term as of the date of your notice of termination Appendix II plus the cost of any hardware, equipment, and software licensing fees We purchased to be used in Your IT Network or became obligated to pay on Your behalf (including non-cancelable future software license payments) that were not already paid by You as part of the Onboarding Fee stated in Appendix II ("Termination Payment"), within seven (7) days of the date of Your notice of termination ("Termination Payment Due Date").

If You terminate this Agreement in accordance with this section, in no event will such termination relieve You of Your obligation to pay all charges incurred under this Agreement or any Service Order prior to such termination.

All Termination requests must be made in writing to: ar@kennedycsi.com and chance@kennedycsi.com

Termination by Us. This Agreement may be terminated by Us for any reason upon thirty (30) days' written notice to You ("Termination Notice Period"). We may terminate this Agreement in the event of non-payment, breach, or other material violation of this Agreement by You as provided in Article 14.

ARTICLE 3 – SERVICES AND SERVICE ORDERS

Scope of Services. Beginning on 4/1/2025 (the "Effective Date"), We agree to undertake and provide the Services described in the Service Schedule attached to this Agreement as Appendix I, and as specified in any Service Orders or Service Requests issued by You and approved by Us (collectively, the "Services"), at the fees and rates set forth in Appendix II. While We will always make reasonable efforts to provide support and troubleshoot issues as requested, Our obligations, response times and resolution time frames, if any, apply only to the Services listed in Appendix I, and only to those components of Your IT Network that are part of Our Standard Technology Suite and which meet Our Minimum Technology Requirements, as outlined in the Client Handbook and/or Appendix I.

Requesting Services. The process for lodging service requests is outlined in the Client Handbook, a copy of which will be emailed to You after signing this Agreement. Our Guaranteed Response Times only apply if the appropriate channels and procedures set forth in the Handbook are followed. When requesting a service, You acknowledge that You are solely responsible for the completeness and accuracy of all information provided to Us. Each Ticket, Quote, Service Request and/or Service Order is subject to and incorporates the provisions of this Agreement.

Approval of Quotes and Service Orders. All Quotes and Service Orders are subject to availability and acceptance. Service Orders will be deemed accepted by Us once We either perform the work (such as where the task is included within the scope of a Managed Service Plan) or when We provide You with a confirmation stating a) the term or estimated duration of the Service; b) the pricing, if applicable, including any monthly recurring charges as well as any non-recurring charges such as software, equipment and other costs or expenses payable in addition to Our rates; and c) any additional terms applicable to the Service Order. The Service Order will be deemed accepted by You a) if the Service is included in a Managed Service Plan or if the reasonable estimated duration of the Service is less than ten (10) hours, when the request for the Service is placed; or b) if the Service is not included within the scope of a Managed Service Plan or the Service is expected to exceed ten (10) hours in duration, once Your duly appointed representative indicates their approval and consent to the Service and the estimated pricing provided by Us.

Service Priority Levels. Determining the priority of an issue is within Our sole discretion; however, to give You an idea of what to expect, priorities are generally assigned as shown in the Client Handbook. If You wish to move a Service Request up to a higher priority than it would normally be assigned, You may request an "Emergency Upgrade" by following the instructions outlined in the Client Handbook. All Emergency Upgrades are treated as Critical Priority Issues and are billed at our emergency rate, separately and in addition to any Monthly Managed Service Fees and other applicable charges. We also reserve the right to amend Our service priority levels by providing You a revised list via the Client Handbook or other similar policy document issued by Us.

Reliance on Appearance of Validity. If any Service Order or Quote approval is signed or sent from an email address associated with You or Your business and/or approved through Your account via Our web-based portal or ordering system, You hereby acknowledge that such Service Orders shall be deemed to be signed and duly authorized by You and may rely upon the apparent validity of same.

Service Order Term. The term of any Service Order will commence on the date specified by Us when accepting the Service Order or on the date that We begin work on the Service, and shall continue for the period of time specified in the Service Order or until a) the work under the Service Order has been completed or b) the Service Order has been renewed, cancelled or terminated. For clients not on a Managed Service Plan, we reserve the right to increase rates for any Services I want to change this to at any time.

Exclusions. By signing this Agreement, You acknowledge and agree that the Services provided by Us do not cover, and We have no liability or obligation with respect to: a) any issues caused by Your use of any equipment, software or service(s) in a way that is not recommended; b) issues resulting from unauthorized changes made to the configuration or setup of Your IT Network; c) issues caused

by Your actions or those of Your employees, representatives, or contractors that have prevented or hindered Us in performing required and recommended maintenance upgrades or other Services; d) issues resulting from work performed by You or any of Your contractors other than Us on Your IT Network ("Excluded Services"). Under no event will We be liable for any claims, losses, damages or expenses relating to issues arising out of such Excluded Services; and any tasks to be performed by Us which relate to such Excluded Services must be requested pursuant to a properly executed Service Order regarding same and will be charged at our Rates specified in **Appendix II**. Work relating to issues arising out of Excluded Services is not covered under any Managed Service Plan.

Assignment and Outside Contractors. We may engage such persons, corporations or other entities as We reasonably deem necessary for the purpose of performing Services under this Agreement; provided, however, that We shall remain responsible for the performance of all such Services and shall be considered to engage with any third party persons, corporations or other entities on Our own behalf.

Service Limitations. You acknowledge that the Services provided may reasonably involve trial and error from time to time, and that information technology is a science applied often in novel or unknown circumstances and involving experiment. In particular, You acknowledge that while We will make what We consider (in Our absolute discretion) to be all reasonable endeavors to provide appropriate tests, troubleshooting, sound advice and good recommendations in order to assist You, the Services may involve tests, troubleshooting, advice and recommendations that may prove incorrect or inappropriate, particularly in an attempt to cure a problem You are having.

Reasonable Assistance Limits. We are only obliged to provide what We consider, in Our absolute discretion, to be reasonable assistance in the circumstances. If You require additional Work beyond what We consider to be reasonable assistance, You agree that such additional Work will be billed at Our Hourly Rates set forth in **Appendix II** unless otherwise agreed. Without limiting Our discretion to determine what "reasonable assistance" means under any particular set of circumstances, in general, reasonable assistance is limited to work done during Business Hours over a period of time not exceeding any period that We have estimated the Work to take based on our experience and our knowledge of the facts and circumstances at the time we agreed to perform the Work.

Standard Technology Suite. In order to make sure we can deliver quality service, We constantly work towards helping all of our clients use the technology we know, trust and love the most – We call this our "Standard Technology Suite" or "STS", the details of which are outlined in the **Client Handbook**. When entering into a Service Agreement with Us, You promise to cooperate with Us as much as practicable for Your business in adopting as much of Our STS as possible. This benefits all parties, as We always strive to keep updated on all components of Our STS and deepen our

knowledge on everything in our STS in order to keep Your IT Infrastructure high quality, well-integrated, and fast to troubleshoot and support.

While it is possible that We may be able to purchase and integrate hardware and software that are not listed in Our STS, any tasks involving the installation, setup, maintenance, servicing and support of those products is outside of the scope of any Managed Service Plan, and is billed hourly, at the rates outlined in **Appendix II**.

Other Third Party Goods and Services. At times, You may specifically request, or We may recommend the purchase of third party goods or services outside of our STS in situations where some function sought may not be fulfilled by our STS. You acknowledge that We have no control over many factors involved with the suitability, function or fitness for purpose of goods in an existing or new computer environment, such as the compatibility or ability of the goods to fit into or perform to expectations in the receiving environment, or the behavior of any third-party supplier. For many reasons outside of Our control, sometimes goods may fail to meet Your expectations, may not turn out to be fit for the purpose(s) sought, or may not function properly in all or any respects. Because such issues are to be expected when implementing any new technology in any environment, by signing this Agreement You agree to hold us harmless from any claims for losses, expenses, injuries or other damages should a product not meet your expectations.

Testing Procedures. You agree to follow Our instructions with regard to testing or troubleshooting any problems and that if those efforts do not resolve the outstanding issues, We will, subject to this Agreement, allocate such resources as We consider reasonable in the circumstances towards their resolution.

Substitute Products. If We cannot supply the products ordered by You, We may supply alternate products of equal or superior quality.

ARTICLE 4 -- SOFTWARE and THIRD PARTY VENDORS

Licenses and Indemnity. We will not install unlicensed software. Each software that is purchased and/or installed shall be accompanied by a valid license agreement. You are solely responsible for the retention of the license documentation. We will provide You with all licenses and warranty

information provided by third party suppliers of all software purchased by Us on Your behalf. Unless expressly agreed upon by Us in writing otherwise, it is at all times exclusively Your duty and responsibility to adhere to all licensing rules applicable to any software on Your IT Network, and to store all licenses for all software used by You, so that that they can be reproduced if and when required. This includes all Software installed by Us.

Breach or Unauthorized Use. To the extent allowed by law, You agree to indemnify and hold Us and each of Our members, shareholders, successors, assigns, directors, officers, employees, agents and subcontractors (the "Released Parties") harmless from and against any and all liabilities, claims, causes of action, lawsuits and/or demands of whatever kind or nature, either in law or equity, including all direct, indirect, incidental, special or consequential damages (including without limitation, damages for interruption of services, loss of business, loss of profits, loss of revenue, loss of data, or loss or increased expense of use client or any third party incurs), as well as any and all other claims, whether in an action in contract, warranty, tort (including without limitation, negligence), or strict liability, which arise out of or are in any way related, directly or indirectly, to a) any unauthorized software use by You or your employees, directors and officers, agents, representatives and contractors, b) any breach of any software license in respect of software provided to Us by You to be installed on one or more of Your computers or equipment, c) otherwise as a result of Us installing Software at Your direction and supplied by You where You are not authorized to use the Software, or d) any problem, defect or malfunction associated with any software (or related services) supplied by third parties.

Power of Attorney. If You request Us to procure software licenses on Your behalf, You agree and irrevocably appoint Us as Power of Attorney to accept terms and conditions or end user license agreement (EULA) for any and all Software requested installed by You. This enables Us to thoroughly ensure the proper acquisition, installation, and usage of all necessary Software for Your specific purpose and IT set up.

Copyright. All copyright in custom software owned by Us remains the sole property of Ours or its owner, unless alternate arrangements are made as part of a separate software agreement.

Third Party Vendors In providing Our Services, We may incorporate services and software provided by third parties ("Third Party Vendors"). These Third Party Vendors may have their own agreements (terms and conditions) and privacy policies that govern the scope of their services; Your use of their Services; Your privacy rights and their use of Your information; limits on the Third Party Vendor's liability; and other important information regarding Your rights ("Third Party Agreements"). You understand and agree that a) You may be legally bound by the Third Party Agreements of Third Party Vendors whose software and services You use; b) We are not responsible for the failure, interruption or deficiency in any service or software provided by a Third Party Vendor; and c) You will not attempt to hold Us liable for the acts or omissions of Third Party Vendors or any losses,

damages, claims or expenses resulting from the failure, interruption or deficiency in any service or software provided by a Third Party Vendor.

ARTICLE 5 – RETURNS, REFUNDS AND CLAIMS

General Returns, Refunds & Cancellation Policy. We keep a limited inventory on hand, and order most items once We receive a Service Order or an approval of a Quote from You. As a result, If You terminate or cancel a Service Order prior to the expiration of its Term, You will be responsible for all costs and expenses incurred by Us pursuant to the Service Order, including any and all software, equipment, third party contractor labor, subscription, installation and special construction costs, and any and all other costs and other fees incurred by Us as a result of the Service, in addition to any applicable Cancellation Fee. If You request to return an item for which We already placed the order, You acknowledge that a) if the item is returnable to the manufacturer or supplier, a restocking fee determined at the time of the return/cancellation request may apply; and b) if We do not receive written approval from the manufacturer or supplier that Your item is returnable, We will not be able to issue refunds for any such item.

Customized Goods Not Returnable. Where the hardware and equipment We supply have any element of customization for You, or are supplied pursuant to an order that is in Our determination special or unusual, the goods are obtained from overseas or from a supplier who is no longer trading, or are otherwise not readily returnable by Us to the manufacturer or supplier or any related services may not be cancelled, the goods are not eligible for return.

You further acknowledge that Services provided by Us that involve the task of customizing goods for particular purposes may involve substantial labor outside of the scope of any of our Managed Service Plans. All such work will be payable pursuant to Our Hourly Rates set forth in **Appendix II**, and must be paid on time, in full, without any offset or claim, whether or not We are able to achieve the desired purposes, suitability or function, provided that We have acted in good faith and have made what We consider to be all reasonable endeavors to achieve those outcomes.

Duty to Inspect; Limited Returns. You agree to inspect all products received by You immediately upon their delivery. You have seven (7) days from the date of delivery to provide Us with written notice of Your request to return or exchange any product. Your notice must include one of the following reasons for your request: a) the products are damaged or faulty; b) You were supplied with the incorrect product; or c) the quality of the product is materially lower than what was represented. If no such notice is given on time, You shall be deemed to have accepted the products and have waived the right to any return or refund. If notice is timely provided, We will assist You in attempting

to obtain a refund or exchange from the supplier or manufacturer of the product, subject to the provisions and limitations set forth in this Section. You will be responsible for payment of all costs and expenses incurred by Us in having any products shipped to You and in arranging the return of the products to a manufacturer or supplier.

Consequences of use, installation, customization or sale. To the extent allowed by law, You agree to indemnify and hold Us harmless with respect to any allegations and claims relating to any products that have been used, installed, customized, changed, donated or re-sold by You.

Refunds and Cancellations of Services. The fees paid or payable for Services already rendered by Us are non-refundable. On projects performed pursuant to a pre-determined fixed fee or quote, refunds and cancellations may be requested, and partial refunds may be issued at Our discretion, subject to an administrative and cancellation fee of 15% of the fees specified in the mutually agreed/accepted Quote or Service Order or up to \$750.00, whichever is greater. The foregoing cancellation fees are on top of and in addition to any costs and expenses We may have incurred in ordering hardware, equipment, software licenses, third party contractor labor, and other expenses which cannot be cancelled and must be paid in full.

ARTICLE 7 – YOUR RESPONSIBILITIES

Client Handbook and IT Policy Manual. By signing this Agreement, You agree to read and abide by the processes, procedures and policies outlined in the Client Handbook and the IT Policy Manual, copies of which will be emailed to You after signing of this Agreement in the form of a PDF document or an online link. We will provide Your team with Scheduled Security Training(s) on the requirements and best practices outlined in the IT Policy Manual during Orientation and Onboarding; however, should any personnel require additional training or clarification, You agree to contact us so that We can provide the requisite assistance.

Using Products and Services Only as Intended. In order for Us to be able to provide the Services in a timely and effective manner, You agree to use Your IT Network and all components thereof only as intended and advised by Us.

Updates, Communication and Timely Notification of Issues. You agree to notify Us of any issues or problems with Your IT Network or any component thereof in a timely manner, so that We can maximize Our chances to address problems and issues before they escalate and get out of hand. You further agree to keep Us informed about potential changes to Your IT Network and maintain good and prompt communication with Us at all times.

Logging of Service Requests. In order for Us to provide You with the agreed Service, You agree to follow Our process for logging of Service Requests as outlined in this Agreement, the Client

Handbook, the IT Policy Manual or other similar document which We may issue from time to time regarding Our policies, procedures and processes.

Access to Systems, Sites and People. In order to provide You with the agreed Services, You agree to give Us access to Your IT Network, as well as Your personnel, sites, and other items as and when requested by Us for the purposes of maintenance, updates and fault prevention. You agree to allow Us to install software on Your Equipment that allows Our technicians to access, monitor and/or make changes to Your systems at any time. Among other things, this type of software will allow Us to view system statuses, send and receive monitoring information, see users' desktops and control Your PCs. If the performance of Our work requires that You leave devices powered on overnight or weekends, You agree to do so upon Our request.

Third Party Authorizations. At times We may need to contact Your third party providers on Your behalf, such as Your internet provider. Some of these providers may require Your authorization to deal with Us on Your behalf. It is Your responsibility to ensure that We are able to deal freely with these providers. A sample letter to providers is attached to this Agreement in order to assist with the timely obtaining of all required authorizations.

Limitation of Liability. By signing this Agreement, You acknowledge and agree that We shall not be liable for any loss, damage, injury, claim, expense or liability resulting from Your failure to follow the above requirements of this Article.

ARTICLE 8 – BILLING AND PAYMENTS

Charges and Billing. You shall pay all Charges for the Services as specified in **Appendix II**. Monthly recurring charges, including but not limited to **Monthly Managed Service Fees** and any additional recurring subscriptions or license fees ("MRC") are payable in advance; all other Charges are payable monthly in arrears. All charges shall be payable in U.S. Dollars. Invoices are payable no later than thirty (30) days from the invoice date ("Due Date") and shall be exclusive of any applicable taxes.

"Charges" means the fees, rates, costs, expenses and charges for the goods and Services provided by Us, as specified in **Appendix I** and/or the applicable Service Order. Unless otherwise agreed to by the Parties in writing, Charges for each Service Order shall begin to accrue on the date that work on the Service is commenced by Us. Charges for the Services are subject to change at any time if third party charges in connection with a Service are increased or newly charged to Us.

Late Payments. If You are late in making payment, You shall pay a late fee on any late payments at the lesser of one and a half percent (1.5%) per month or the maximum rate allowed by applicable law. If We use a collection agency or attorney to collect a late payment or returned payment, You

agree to pay all reasonable costs of collection or other action. These remedies are in addition to and not in limitation of any other rights and remedies available to Us under the Agreement, at law or in equity.

Taxes and Other Fees. All Charges for the Services are exclusive of any taxes and other fees and surcharges. You shall be responsible for payment of all applicable taxes that arise in any jurisdiction, including, without limitation, value added, consumption, sales, use, gross receipts, excise, access, and bypass ("Taxes").

Invoice Disputes. To the extent that You dispute any portion of an invoice in good faith, You shall notify Us in writing and provide detailed documentation supporting Your dispute within thirty (30) days of the invoice date; otherwise, Your right to any billing adjustment shall be waived. In the event of a billing dispute, You shall timely pay all undisputed amounts. If the dispute is resolved against You, You shall pay all amounts due plus interest from the original Due Date. You may not offset disputed amounts from one invoice against payments due on the same or another account or invoice.

Changes and Fee Estimates. Our Hourly Rates and Monthly Managed Service Fees are subject to change by Us on the anniversary of the Effective Date of this Agreement, with any annual increases not to exceed 5% of the past year's rate or fee, while allowing for rounding up to the nearest \$5 for any labor cost. Any fee estimates provided by Us at Your request are for informational purposes only, and may differ from the rate(s) ultimately payable by You pursuant to a subsequent invoice, Service Order or Service Schedule.

Refunds and Cancellations. The fees charged under this Agreement are non-refundable. No refunds will be given after We have commenced work pursuant to this Agreement or any Service Order or Service Schedule.

ARTICLE 9 – LIMITED WARRANTY

Limited Warranty. We warrant, for a period of thirty (30) days following delivery of any Services hereunder (the "Warranty Period") that all Services will be performed in a professional manner and in accordance with generally applicable industry standards. Our sole liability (and Your exclusive remedy) for any breach of this Warranty shall be for Us to re-perform any deficient Services, or, if We are unable to remedy such deficiency within fifteen (15) days of being notified of same, to void the invoice for the deficient Services. We shall have no obligation with respect to any Warranty claim if (1) We are notified of such claim after the Warranty Period, or (2) the claim is the result of third-party hardware, software or services; Your actions, including those of Your employees, agents, members, representatives, affiliates and contractors; the actions or omissions of any person or entity not under

Our direct supervision or control; or (3) the claim is otherwise caused by factors outside Our reasonable control.

THIS SECTION IS A LIMITED WARRANTY, AND THIS SECTION AND THIS AGREEMENT SET FORTH THE ONLY WARRANTIES MADE BY US. WE MAKE NO OTHER WARRANTIES, EXPRESS OR IMPLIED, WHETHER WRITTEN OR ORAL, EITHER IN FACT OR BY OPERATION OF LAW, BY STATUTE OR OTHERWISE, WITH RESPECT TO ANY GOODS AND/OR SERVICES PROVIDED HEREUNDER, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF RELIABILITY, USEFULNESS, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THOSE ARISING FROM THE COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE, OR ANY WARRANTIES REGARDING THE PERFORMANCE OF ANY SOFTWARE OR HARDWARE PROVIDED OR INSTALLED BY US. YOU MAY HAVE OTHER STATUTORY RIGHTS; HOWEVER, TO THE FULL EXTENT PERMITTED BY LAW, THE DURATION OF STATUTORILY REQUIRED WARRANTIES, IF ANY, SHALL BE LIMITED TO THE WARRANTY PERIOD.

Upon Your request, We will pass along to the You any third-party warranties relating to any goods purchased and/or installed by Us.

ARTICLE 10 – INDEMNITY & LIMITATION OF LIABILITY

Aggregate Limit of Liability. In recognition of the relative risks and benefits to both You and Us, the risks have been allocated such that both Parties agree, to the fullest extent permitted by law, that We shall not be liable for any indirect, incidental, special or consequential damages (including without limitation, damages for interruption of services, loss of business, loss of profits, loss of revenue, loss of data, or loss or increased expense of use client or any third party incurs), whether in an action in contract, warranty, tort (including without limitation, negligence), or strict liability (“Losses”), even if We have been advised of the possibility of such liabilities. Limitations of liability, waivers and indemnities in this Agreement are business understandings between the Parties and shall apply to all legal theories of recovery. We shall not be responsible for any Losses, damages, injuries, claims or expenses of any nature which may occur as a result of the use of or the failure of any third-party software or hardware. In no event shall the aggregate amount You may recover from Us under this Agreement for any and all Losses, damages, injuries, claims, or expenses arising out of or in any way related to the Services and/or this Agreement, from any cause or causes, including but not limited to Our negligence, errors, omissions, strict liability, breach of contract or breach of warranty, exceed the total Insurance Proceeds paid to Us or on Our behalf pursuant to Our insurance policies applicable to and covering the alleged Loss. The term “Insurance Proceeds” as used in this paragraph refers to sums paid by Our insurer(s) in satisfaction of a claim, and excludes any fees, costs and expenses of investigation, claims adjustment, defense, and appeal which may be paid under Our policies. The foregoing sum represents Our total liability for all of Your claims and Losses.

You agree that You will not seek damages in excess of these contractually agreed-upon limitations. The limitations set forth in this section shall not apply to personal injury or damage to tangible property caused by Our gross negligence or willful misconduct.

Cyber Security Testing. You understand the serious implications to Your business of malicious emails and/or websites designed to obtain sensitive data ("phishing"). As part of managing this risk, You allow and authorize Us to create simulated phishing emails and/or webpages to be sent to Your business environment, without advance notice to You, in order to determine Your security weaknesses. These simulated attacks help clients understand the different forms a phishing attack can take, identifying features, and to avoid clicking malicious links or leaking sensitive data in malicious forms, in addition to assisting Us in improving Your cybersecurity.

Cybersecurity Breach Waiver of Liability.

YOU UNDERSTAND, ACKNOWLEDGE AND AGREE THAT IN THE EVENT OF A DATA BREACH, VIRUS OR RANSOMWARE ATTACK OR OTHER CYBERSECURITY INCIDENT, WHILE WE WILL MAKE REASONABLE EFFORTS TO ASSIST YOU WITH CONTAINMENT AND REMEDIATION IF INCIDENT RESPONSE AND BREACH REMEDIATION ARE SPECIFICALLY LISTED AS PART OF OUR SERVICE TO YOU, ANY DAMAGES WHICH MAY RESULT FROM SUCH ATTACK, INCLUDING BUT NOT LIMITED TO DOWN-TIME, LOSS OF DATA, THIRD-PARTY LOSSES AND CLAIMS, FINES, PAYMENT OF THE RANSOM, AND ANY OTHER LIABILITIES, LOSSES, COSTS, EXPENSES, FEES, FINES AND DAMAGES DUE TO SUCH BREACH SHALL BE EXCLUSIVELY YOUR RESPONSIBILITY.

E-Mail Backup, Storage and Data Retention. Unless You are receiving email backup and archiving services under the Managed Service Plan section of **Appendix I**, Our Email Services do not include any archive or backup services. If these services are not included within the Services rendered to You, then it is Your sole and exclusive responsibility to maintain independent backups of Your email messages at all times. You acknowledge and agree that We shall have no liability to You or any third party for any loss, damage, or destruction of Your email messages, contacts, distribution lists, or other data or content stored in connection with any email accounts or services. Upon request, We can assist You in setting up a backup service with a third party of Your choice. You understand that if You request any email account to be deleted, that any data from that account will not be recoverable. It is Your responsibility to request Us to backup any data before deleting the account. Our Standard rates will be charged for any time spent setting up backup services and creating a copy of a mailbox. At any time, You may request in writing for Us to provide a list of all email accounts charged to the You for review.

WE WILL NOT BE LIABLE FOR ANY (a) SUSPENSION OR LOSS OF THE EMAIL SERVICE, (b) USE OF THE EMAIL SERVICE, (c) INTERRUPTION OF THE EMAIL SERVICE OR INTERRUPTION OF YOUR BUSINESS, (d) ACCESS DELAYS OR ACCESS INTERRUPTIONS TO THE EMAIL SERVICE; (e) LOSS OR LIABILITY RESULTING FROM ACTS OF OR EVENTS BEYOND OUR CONTROL (f) DATA NON-DELIVERY, MIS-DELIVERY, CORRUPTION, DESTRUCTION OR OTHER MODIFICATION; (g) LOSS OR LIABILITY RESULTING FROM THE UNAUTHORIZED USE OR MISUSE OF YOUR ACCOUNT OR PASSWORD; OR (h) APPLICATION OF ANY DISPUTE POLICY. WE WILL NOT BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING LOST PROFITS) REGARDLESS OF THE FORM OF ACTION WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES ("EMAIL LOSSES"). IN NO EVENT SHALL OUR MAXIMUM AGGREGATE LIABILITY FOR ANY EMAIL LOSSES EXCEED \$1,000. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, IN SUCH STATES, OUR LIABILITY SHALL BE LIMITED TO THE MAXIMUM EXTENT PERMITTED BY LAW.

Declined Services. We may, from time to time, recommend additional products, services and/or managed IT/security solutions designed to improve Your overall IT Network and security platform or address specific developments in the field of information technology or cybersecurity. We may also recommend additional products and services in response to a change in Your business, users or operations that in Our opinion necessitates or is reasonably served by an upgrade or modification of the products and services being provided.

While We strive to evolve Our technology platform and services to accommodate new developments at minimal inconvenience to Our clients, adding new products and services does entail additional charges and fees, including but not limited to setup fees, equipment charges, new/additional licensing and software subscription fees, ongoing management fees, and more.

All recommendations made by Us are made with Your best interest in mind, in terms of network efficiency, integration, fast and effective troubleshooting, and reducing information technology / cybersecurity risks.

While You are always free to elect not to follow Our recommendations, if You refuse a recommended product or service on account of cost, or for any other reason, You agree that by doing so, You fully accept all risks associated with not following Our recommendations. You further agree, to the extent allowed by law, to release, indemnify and hold Us harmless from and against any and all liabilities, claims, causes of action, lawsuits and/or demands of whatever kind or nature, either in law or equity, including all direct, indirect, incidental, special or consequential damages (including without limitation, damages for interruption of services, loss of business, loss of profits, loss of revenue, loss of data, or loss or increased expense of use client or any third party incurs), as well as any and all

other claims, whether in an action in contract, warranty, tort (including without limitation, negligence), or strict liability, which arise out of or are in any way related, directly or indirectly, to any hardware or software which We advised you to change or upgrade, or any other decision by You to not follow Our recommendations with regard to improving Your IT Network. If a cybersecurity/data breach, data loss or other damage occurs involving any hardware, software or equipment which We recommended to be upgraded or replaced, You accept full responsibility for remediating any such loss, breach or damage, and further accept and agree that all labor to repair any damage or otherwise handle any issues associated with such loss, breach or damage will not be covered under any Managed Service Plan and will be charged to You at Our Hourly Rates set forth in **Appendix II**.

You agree to not hold Us responsible or legally liable for the Your decision to not follow Our recommendations and/or any future consequences relating to or arising out of that decision.

Vulnerability During Implementation. Both Parties understand that the Services are not fully operational, and protection of Your IT Network is incomplete, until Onboarding and Implementation is finished and all hardware and software solutions are fully implemented and deployed. You understand that the IT Network will be vulnerable to cybersecurity risks during both the initial Onboarding and Implementation phase, as well as during subsequent phases of procurement, installation and deployment of new hardware, software or other security measures being added to Your Services during the Commitment Term ("Implementation Period"). By engaging Our Services, You agree that we are not liable for any claims, suits, causes of action, liabilities, losses, costs, expenses and damages, including indirect or incidental damages and attorney fees, arising out of or relating to any cybersecurity breach or other incident occurring during any Implementation Period. Such cybersecurity breach or incident may include, but is not limited to any data breach (including but not limited to incidents involving theft of information), privacy violations, damage to or destruction of electronic information, virus or ransomware attack, alteration of electronic information, intentional and/or unintentional release of private information, cyber attacks on data held by you or any vendors or other third parties, cyber attacks including breaches of your network (that occur anywhere in the world), lost income due to network and business interruption, cyber extortion and fraud, and any fines, fees and penalties related to any such incidents.

Release and Indemnification. Subject to the limitations set forth in this Agreement, including the Limited Warranty and Limitation of Liability articles above, each Party ("Indemnifying Party"), to the extent allowed by law, agrees to release, indemnify, defend and hold harmless the other Party, its directors, officers, employees, and agents, successors and assigns ("Indemnified Party"), from and against all claims, losses, expenses, fees, damages and liabilities, including reasonable attorney fees and disbursements, costs, and judgments, sustained in any action commenced by any third party in connection with the Indemnifying Party's performance of, or failure to perform, its obligations and duties under this Agreement, except for those damages, costs, expenses and liabilities arising from the negligence or willful misconduct of the Indemnified Party; provided, however, that We are

not obligated to indemnify You, and You shall, to the extent allowed by law, defend and indemnify Us hereunder, for any claims by any third party, including any clients and/or customers of You, arising from services provided by You that use, incorporate or otherwise involve any of the Services being provided by Us hereunder, including but not limited to (a) the violation of any applicable law by the You or the Your clients and/or customers; (b) damage to property or personal injury (including death) arising out of the acts or omissions of Your clients and/or customers; (c) termination or suspension of Services of You or Your clients and/or customers due to a Client Default; or (d) claims by any third party, including without limitation Your clients and/or customers, arising out of or related to the use or misuse of any Service. In all claims for Indemnity under this paragraph, the Indemnifying Party's obligation shall be calculated on a comparative basis of fault and responsibility. Neither party shall be obligated to indemnify the other in any manner whatsoever for claims, losses, expenses, or damages resulting from the other party's own negligence.

Indemnification Procedures. The Indemnified Party shall promptly notify the Indemnifying Party in writing of any such suit or claim, and shall take such action as may be necessary to avoid default or other adverse consequences in connection with such claim. The Indemnifying Party shall have the right to select counsel and to control the defense and settlement of such claim; provided, however, that the Indemnified Party shall be entitled to participate in the defense of such claim and to employ counsel at its own expense to assist in handling the claim, and provided further, that the Indemnifying Party shall not take any action in defense or settlement of the claim that would negatively impact the Indemnified Party. The Indemnified Party shall provide cooperation and participation of its personnel as required for the defense at the cost and expense of the Indemnifying Party.

ARTICLE 11 – INSURANCE

Insurance. We agree to maintain the following insurance coverages for Us, for so long as We are providing Services to You pursuant to this Agreement:

- **Professional liability insurance**, in commercially reasonable amounts providing reasonable coverages for network security/data protection liability, including liabilities for financial losses resulting or arising from acts, errors or omissions in Our rendering of any professional services described in this Agreement. Such insurance shall include both **first-party coverage** (for direct losses, including breach response costs, business interruption, and cyber extortion) and **third-party coverage** (for liabilities arising from claims by customers, vendors, or other third parties, including regulatory defense and penalties)."
 - **Worker's compensation and disability insurance** in compliance with statutory requirements.
-

Prior to commencement of Services and upon request, We agree to provide You with certificates of insurance, evidencing that such coverages are in full force and effect. We will provide You with renewal certificates at such times as You may reasonably request. We will make available copies of all such policies for review upon Your written request.

Client Insurance Requirement. As a condition of entering into this Agreement, you also agree to procure and maintain first-party cyber insurance, from a reputable insurance broker, in commercially reasonable amounts, providing coverage for claims involving data breaches (including but not limited to incidents involving theft of information), privacy violations, damage to or destruction of electronic information, alteration of electronic information, intentional and/or unintentional release of private information, cyber attacks on your data held by vendors and other third parties, cyber attacks including breaches of your network (that occur anywhere in the world), lost income due to network and business interruption, cyber extortion and fraud, and any fines, fees and penalties related to the cyber incident.

You agree to provide Us with satisfactory proof of insurance upon request, and to immediately notify Us in writing of any lapse, cancellation, or modification of the insurance coverage required herein. Failure to maintain insurance, provide Us with required notifications, and failure to obtain new cyber insurance in accordance with the requirements of this section within thirty (30) days of a lapse or cancellation shall constitute a Client Default and a material violation of this Agreement.

ARTICLE 12 – CONFIDENTIALITY AND DATA PROTECTION

Confidentiality. Each Party acknowledges that, in connection with this Agreement, it may be furnished with, or given access to, certain confidential and/or proprietary information of the other Party, and that, subject to the provisions of this section, such information shall not be disclosed by the Party receiving the information to any third party, unless such disclosure is required under Texas Government Code Chapter 552, Public Information Act, and shall not be used by either Party for purposes other than those contemplated by this Agreement.

Information Subject to Confidentiality. Confidential Information may include, but is not limited to, the following:

- Any materials regardless of form furnished by either Party to the other for use;
 -
-

Any information furnished by any Party that is stamped "confidential," "proprietary," or with a similar legend, or any information that any Party makes similar reasonable efforts to maintain secret;

- Any business or marketing plans, strategies, customer lists, operating procedures, design formulas, know-how, processes, programs, software, inventories, discoveries, improvements of any kind, sales projections, strategies, pricing information; and other confidential trade secrets, data and knowledge of either Party;
- Any information belonging to employees, agents, members, shareholders, owners, customers, suppliers, vendors, contractors, business partners and affiliates of either Party;
- Any non-public inventions the rights to which have not been assigned to the Party receiving the information;
- Any non-public and proprietary technical information belonging to either Party, the rights to which have not been assigned to the party receiving the information;
- **Our Standard Technology Suite;**
- And other proprietary information owned by either Party which are valuable, special and/or unique assets of that Party.

Any templates, schematics, processes or any technical documentation provided by Us shall be deemed Our Confidential Information and proprietary information without any marking or further designation. You may use such information solely for Your own internal business purposes.

We shall maintain the confidentiality of information in Our possession regarding individual protected health information in accordance with applicable law, and shall not release such information to any other person or entity, except as required by law.

Non-Disclosure. Neither Party will disclose or use, either during or after the term of this Agreement, in any manner, directly or indirectly, any Confidential Information of the other Party, for their own benefit or the benefit of any third party. Neither Party will use, share, divulge, disclose or communicate in any manner whatsoever any Confidential Information to any third party without the prior written consent of the other Party, except to the extent specifically permitted under this Agreement.

Both Parties will protect all Confidential Information of the other, and will treat it as strictly confidential, unless and until: a) said information becomes known to third parties not under any obligation of confidentiality to the party whose confidential information is at issue ("Disclosing Party"), or becomes publicly known through no fault of the other party (the "Receiving Party"); or b) said information was already in the Receiving Party's possession prior to its disclosure, except in cases where the information has been covered by a preexisting Confidentiality Agreement; or c) said

information is subsequently disclosed by a third party not under any obligation of confidentiality to the Disclosing Party; or d) said information is approved for disclosure by prior written consent of the Disclosing Party; or e) said information is required to be disclosed by court order or governmental law or regulation, provided that the Receiving Party gives the Disclosing Party prompt notice of any such requirement and cooperates with the Disclosing Party in attempting to limit such disclosure; or f) said information is proven independently developed by the Receiving Party without recourse or access to the information; or g) disclosure is required in order for a party to comply with its obligations under this Agreement, provided that prior to disclosure, the Receiving Party gives the Disclosing Party prompt notice of any such requirement and cooperates with the Disclosing Party in attempting to limit such disclosure.

A violation of this Section shall be a material violation of this Agreement.

Employees and Agents. The Parties further agree to disclose the Confidential Information to their officers, directors, employees, contractors and agents (collectively, the "Agents") solely on a need-to-know basis and represent that the Party receiving Confidential Information has taken appropriate measures imposing on such Agents a duty to (1) hold any Confidential Information received by such Agents in the strictest confidence, (2) not to disclose such Confidential Information to any third party, and (3) not to use such Confidential Information for the benefit of anyone other than the party to whom it belongs, without the prior express written authorization of the party disclosing same.

Data Protection. We may have access to Your computer and communications systems and networks for the purposes set forth in this Agreement. If any data is made available or accessible to Us or Our employees, agents or contractors, which pertains to Your business or financial affairs or to Your projects, transactions, clients, customers, partners, vendors or any other person or entity, We will not store, copy, analyze, monitor or otherwise use that data except for the purposes set forth in this Agreement and any valid Service Schedule or Service Order. We will comply fully with all applicable laws, regulations, and government orders relating to personally identifiable information ("PII") and data privacy with respect to any such data that We receive or have access to under this Agreement or in connection with the performance of any Services for You. We will otherwise protect PII and will not use, disclose, or transfer such PII except as necessary to perform under this Agreement or as specifically authorized by the data subject or in accordance with applicable law. To the extent that We receive PII related to the performance of this Agreement, We will protect the privacy and legal rights of Your personnel, clients, customers and contractors.

ARTICLE 13 -- NON-SOLICITATION

Non-Solicitation of Personnel. You agree that, as long as this Agreement is in effect, and for thirty-six (36) months following termination of same (the "Restricted Period"), You may not, directly or indirectly, individually or on behalf of any person or entity, solicit or contact any employee, contractor,

vendor, supplier, affiliate or business partner of Ours ("Business Personnel") with a view to inducing or encouraging such Business Personnel to discontinue, curtail, or not engage in any business relationship with Us.

Injunctive Relief. You hereby acknowledge that 1) if You violate any of Your duties under this Agreement, We may suffer irreparable damage; and 2) that monetary damages will be inadequate to compensate Us for such damage resulting from the breach. Therefore, in the event of a breach, We shall be entitled to seek injunctive relief and/or preliminary injunction against You, without the need to post a bond, in addition to any other remedies at law or equity, to enforce such provisions.

ARTICLE 14 – DEFAULT

Default by You. You are in default of this MSA if You (a) fail to cure any monetary breach within **ten (10) days** of receiving notice of the breach from Us; (b) fail to cure any non-monetary breach of any terms of this Agreement or applicable Service Order within **fifteen (15) days** of receiving notice of the breach from Us; or (c) file or initiate proceedings or have proceedings filed or initiated against You seeking liquidation, reorganization or other relief (such as the appointment of a trustee, receiver, liquidator, custodian or such other official) under any bankruptcy, insolvency or other similar law (each such event shall be a "Client Default").

In the event of a Client Default, We may suspend Services to You until You remedy the Client Default, or We may terminate this Agreement and/or any or all of the Services being provided hereunder with immediate effect and without penalty or obligation to issue any refund. We may at Our sole option, but without any obligation, cure a non-monetary breach at Your expense at any point and invoice You for the same. These remedies are in addition to and not a substitute for all other remedies contained in this Agreement or available to Us at law or in equity.

Default by Us. We are in default of this Agreement if We fail to cure any non-monetary breach of any material term of this Agreement within **ninety (90) days** of receiving written notice of the breach from You ("Consultant Default"); provided, however, that You expressly acknowledge that malfunctioning of hardware, software and equipment, other service-related failure or degradation in performance, and issues caused by events and circumstances beyond Our control are not subject to a claim of a Consultant Default. Your sole and exclusive remedy for any failure of Service is limited to the remedies set forth in this Agreement. In the event of a Consultant Default, You may immediately terminate the Services and this Agreement upon written notice to Us. Any termination shall not relieve You of Your obligations to pay all charges incurred hereunder prior to such termination.

ARTICLE 15 – OFFBOARDING

Offboarding Assistance. If either Party terminates this Agreement, or at the end of the Commitment Term, We will make our team available to provide You with assistance ("Offboarding Assistance") in the orderly termination or transfer of the services to another designated provider ("Offboarding"). If You are on a **Managed Service Plan**, We will render up to ten (10) hours of **Offboarding Assistance** free of charge. If You are not on a **Managed Service Plan**, **Offboarding Assistance** is available at Our Hourly Rates set forth in **Appendix II**. The availability of **Offboarding Assistance** is conditioned upon all of the following requirements being met no less than fourteen (14) calendar days prior to the expiration of the applicable Termination Notice Period, or the Commitment Term, or if this Agreement is being terminated with immediate effect, no later than seven (7) calendar days following the date of the notice of termination ("**Offboarding Assistance Request Deadline**"):

- a. You complete and return to Us the **Offboarding Assistance Request Form** provided to You in the Client Handbook, or any other similar form We may request You to complete that lists Your duties, acknowledgements and releases, cutoff dates, and the specific services that are being terminated;
- b. If You are not on a **Managed Service Plan**, You submit payment in advance for the first ten (10) hours of **Offboarding Assistance** at our regular Hourly Rates;
- c. If You request transfer of services to a new IT service provider, then the new provider is designated and their contact information is supplied to Us on the Request to Cancel Services Form;
- d. You return or pay for all Supplied Equipment being used on Your premises, unless ownership of same has been transferred to You pursuant to the terms of this Agreement;
- e. You remit payment for all amounts payable to Us under this Agreement or any Service Order, including any current invoices, past-due payments owed for Services rendered, and any Termination Payment required to be made under this Agreement.

Failure to comply with all of the foregoing requirements within the applicable time frame stated above may result in a) **Offboarding Assistance** being unavailable, and b) the final and permanent deletion, termination, and cancellation of any or all of Your Services, accounts, licenses, subscriptions and all data, content, credentials and other information associated with same after seven (7) days following the effective date of the termination of this Agreement or the missed **Offboarding Assistance Request Deadline**, whichever occurs later.

Offboarding Assistance Request Form. By signing this Agreement, You certify that You will read and comply with all terms, deadlines, and responsibilities outlined above and in the **Offboarding Assistance Request Form** provided in the Client Handbook. In order to take advantage of Our

Offboarding Assistance services, and to ensure that important licenses, accounts and information are not irrevocably lost before We terminate any Service, You must complete and return, via e-mail to ar@kennedycsi.com the Offboarding Assistance Request Form or any other similar form or any other similar form We may request You to complete that lists Your duties, acknowledgements and releases, cutoff dates, and the specific services that are being terminated, by the Offboarding Assistance Request Deadline.

Offboarding Timeframe. Offboarding assistance will only be available until the end of the applicable Termination Notice Period or the Commitment Term; or, if this Agreement is being terminated with immediate effect, for fourteen (14) calendar days following the date of the notice of termination ("Offboarding Completion Deadline"). You acknowledge and agree that We will not render Offboarding Assistance outside of these time frames, unless Our invoice for any such assistance is paid for in advance of any such services being rendered.

Cooperation and Designation of New Service Provider. Due to the limited time available for offboarding, You agree to fully cooperate with Us in every step of downloading, backing up and/or transferring Your accounts and data. This includes but is not limited to a) completing and returning to Us the Offboarding Assistance Request Form or other updated service cancellation We may provide; b) providing immediate responses to Our requests for information and access; c) following Our instructions in a timely manner; and d) designating a new managed service provider whose contact is shared with Us via the Service Cancellation Form.

Failure to Cooperate. Failure to provide us with a properly executed Offboarding Assistance Request Form, failure to cooperate with Us and timely providing Us with requested access/information, delays in designating a new managed service provider, and/or failure of Your new managed service provider to diligently cooperate or communicate with Us during the offboarding process so that all tasks may be completed during Regular Business Hours prior to the Offboarding Completion Deadline, may result in a) Offboarding Assistance being unavailable, b) additional charges billed at Our After-Hours and Emergency Rates in effect at the time of termination; and c) the final and permanent deletion, termination, and cancellation of any or all of Your services, subscriptions, licenses, accounts and all data, content, credentials and other information associated with same.

Completion. Offboarding is considered complete when You have complied with all of Your payment and cooperation obligations under this Agreement, and We have a) transferred all accounts, subscriptions and licenses to You or Your designated IT service provider; b) provided You with all passwords, credentials and login information; c) provided You with a copy of all data on the virtual server or transferred ownership of the server account(s) and any associated hardware to You. You understand that upon completion of Offboarding, We will no longer have any control over the management and security of Your IT Network, and therefore, to the extent allowed by law, You agree

to release, indemnify, defend and hold Us harmless from and against all claims, losses, expenses, fees, damages and liabilities, including reasonable attorney fees and disbursements, costs, and judgments, arising out of or relating to Your IT Network, commenced by any party, after the completion of Offboarding.

ARTICLE 16 – MISCELLANEOUS

Notices. All notices and other communications required or permitted under this Agreement shall be in writing, and shall be deemed delivered when sent by e-mail or registered mail, addressed to the address of the Party to be noticed as set forth on the signature page of this Agreement, or to such other address or e-mail address as such party last provided to the other by written notice conforming to the requirements of this paragraph.

Entire Agreement. This Agreement, together with all attachments, schedules, exhibits and other documents that are incorporated by reference herein, including the Client Handbook and IT Policy Manual, constitute the entire agreement between the Parties, represent the final expression of the Parties' intent and agreement relating to the subject matter hereof, contain all the terms and conditions that the Parties agreed to relating to the subject matter, and replaces and supersedes all prior discussions, understandings, agreements, negotiations, e-mail exchanges, and any and all prior written agreements between the Parties. Any subsequent changes to the terms of this Agreement may be amended or waived only with the written consent of both Parties, and shall be effective upon being signed by both Parties.

Severability. If any provision of this Agreement is declared by any court of competent jurisdiction to be illegal, void, unenforceable or invalid for any reason under applicable law, the remaining parts of this Agreement shall remain in full force and effect, and shall continue to be valid and enforceable. If a court finds that an unenforceable portion of this Agreement may be made enforceable by limiting such provision, then such provision shall be deemed written, construed and enforced as so limited.

Successors and Assigns. You shall not transfer or assign, voluntarily or by operation of law, your obligations under this Agreement without Our prior written consent. This Agreement may be assigned by Us (i) pursuant to a merger or change of control affecting Us, or (ii) to an assignee of all or substantially all of Our assets. Any purported assignment in violation of this section shall be void.

Survival. All provisions that logically ought to survive termination of this Agreement, including but not limited to applicable Warranties, Limitation of Liability, Indemnity, Choice of Law, Forum Selection, and Confidentiality provisions, shall survive the expiration or termination of this Agreement.

No Waiver. The failure of any Party to insist upon strict compliance with any of the terms, covenants, duties, agreements or conditions set forth in this Agreement, or to exercise any right or remedy arising from a breach thereof, shall not be deemed to constitute waiver of any such terms, covenants, duties, agreements or conditions, or any breach thereof.

Force Majeure. Either Party who fails to timely perform their obligations under this Agreement ("Nonperforming Party") shall be excused from any delay or failure of performance required hereunder if caused by reason of a Force Majeure Event as defined herein, as long as the Nonperforming Party complies with its obligations as set forth below.

For purposes of this Agreement, "Force Majeure Event" means any event, circumstance, occurrence or contingency, regardless of whether it was foreseeable, which is a) not caused by, and is not within the reasonable control of, the nonperforming Party, and b) prevents the Nonperforming Party from its obligations under this Agreement. Such events may include, but are not limited to: acts of war; insurrections; fire; laws, proclamations, edicts, ordinances or regulations with a material effect on the Nonperforming Party's business and/or ability to comply with its obligations under this Agreement; epidemics, pandemics and disease outbreaks; strikes, lock-outs or other labor disputes; riots; explosions; and hurricanes, earthquakes, floods, and other acts of nature.

The obligations and rights of the Nonperforming Party so excused shall be extended on a day-to-day basis for the time period equal to the period of such excusable interruption. When such events have abated, the Parties' respective obligations under this Agreement shall resume. In the event that the interruption of the Nonperforming Party's obligations continues for a period in excess of thirty (30) days, either Party shall have the right to terminate this agreement upon ten (10) days' prior written notice to the other Party.

Upon occurrence of a Force Majeure Event, the Nonperforming Party shall do all of the following: a) immediately make all reasonable efforts to comply with its obligations under this Agreement; b) promptly notify the other Party of the Force Majeure Event; c) advise the other Party of the effect on its performance; d) advise the other Party of the estimated duration of the delay; e) provide the other Party with reasonable updates; and f) use reasonable efforts to limit damages to the other Party and to resume its performance under this Agreement.

Choice of Law. This Agreement shall be governed and construed in accordance with the laws of the State of Texas, and all claims relating to or arising out of this Agreement, or the breach thereof, whether sounding in contract, tort or otherwise, shall likewise be governed by the laws of the State of Texas.

Choice of Forum. The Parties hereby agree that all demands, claims, actions, causes of action, suits, proceedings between the parties shall be filed, initiated, and conducted in a court of competent jurisdiction in the State of Texas. Any litigation must be filed and litigated in a state or federal court located in the State of Texas. Each Party hereby consents and submits to the exclusive jurisdiction of those courts for purposes of any such proceeding and waives any claims or defenses of lack of jurisdiction of, or proper venue by, such court.

Attorney Fees. In the event that any arbitration, suit or action is instituted to resolve a dispute pertaining to matters covered under this Agreement, or enforce any provision thereof, the prevailing Party in any such dispute or proceeding shall be entitled to recover from the losing Party all reasonable fees, costs and expenses of enforcing any right of such prevailing Party under or with respect to this Agreement, including without limitation, all reasonable fees and expenses of attorneys and accountants, court costs, and expenses of any appeals.

Headings Not Controlling. Headings used in this Agreement are for reference purposes only and shall not be used to modify the meaning of the terms and conditions of this Agreement.

Counterparts. The Parties agree that this Agreement may be executed in counterparts, each of which shall be deemed an original, and all of which together shall be deemed one and the same Agreement. The Parties further agree that e-signatures carry the same weight and effect as traditional paper documents and handwritten signatures; therefore, this Agreement may be electronically signed via any e-signature service compliant with the Electronic Signatures in Global and National Commerce (ESIGN) Act and the Uniform Electronic Transactions Act (UETA) as of the Effective Date of this Agreement.

EXECUTED BY THE CITY OF RANGER on this the _____ day of June, 2025

Charlie Archer
City Manager

EXECUTED BY KENNEDY COMPUTER SOLUTIONS, INC on this the _____ day of June,
2025

Chance Isham
President



APPENDIX I

SERVICE SCHEDULE

I. Service Plan Selection – Managed Or Hourly

Managed Service Plans. Our clients on Managed Service Plans receive ongoing, unlimited support during regular business hours for certain selected Services for the duration of their Commitment Term, as detailed in the table below, for a fixed Monthly Managed Service Fee.

Out-of-Scope Services & Non-Managed Clients – Hourly Rates. If You are not on a Managed Service Plan, or a Service is being requested by You that is not included in Your Managed Service Plan (detailed in Section II below), the Service(s) requested will be performed pursuant to Our Hourly Rates set forth in **Appendix II**.

Acknowledgement of Service Plan Selection. The table and provisions of **Section III – Managed Service Plan** only apply if You are on a Managed Service Plan. Please check the box below to confirm whether or not You are enrolling in a Managed Service Plan:

We wish to receive the Managed Services marked as "included" in the table in **Section III** below.

If You choose not to receive any managed services, and instead elect to call on Us as needed, with all Services being charged at Our Hourly Rates, skip this Section, and proceed directly to **Section IV – Hourly and Project-Based Services**.

II. Service Location

We agree to provide on-site Services at the following Location(s):

- City Hall - 400 W. Main St. Ranger, Texas 76470

Additional locations may be added. Please note that adding new offices may incur additional Onboarding and Implementation Fees, charges for additional hardware and software, and may require an amendment of this Agreement to reflect the added Services and the new Monthly Managed Service Fee, if any, based on the number of new users, new services and new equipment added.

III. **Managed Service Plan**

We agree to perform all of the Services indicated as "Included" in the table below on an ongoing basis for the duration of the Commitment Term (the "Managed Service Plan"), for the Monthly Managed Service Fee stated in **Appendix II**, plus any additional applicable charges. Please review the table below carefully, to ensure that all monthly managed Services you wish to receive are marked "YES" under the "Included" column on the right.

Additional services not listed / marked as "Included" in the table below are not considered part of Your Managed Service Plan; however, they may be requested and will be provided, subject to availability and approval, at the Rates set forth in **Appendix II**, or as otherwise detailed in a custom Quote, Proposal or Service Order.

You may request to upgrade Your Managed Service Plan to include any of the Services not marked as "Included" below at any time by e-mailing quotes@kennedycsi.com for a Quote. You understand that any changes made to the managed services, such as adding users, devices, locations, hardware/software, licenses, subscriptions, or changing the services in any way, will require the mutual execution of an amended **Appendix I** detailing the new services, as well as an amended **Appendix II**, reflecting the new pricing. Changes to the scope will not be implemented or take effect until the amended appendices have been executed and any required up-front payments have been received by Us.

Though We may occasionally provide a Service not explicitly included in the table below without charge, whether We do so – and under what circumstances – is within Our sole discretion.

DESCRIPTION	FREQUENCY	INCLUDED
-------------	-----------	----------

GENERAL		
Document software and hardware changes	As performed	YES
IT Documentation Management	As needed	YES
Test backups with restores	As needed	YES
Quarterly Business Reviews	As needed	YES
CLIENT SUPPORT		
Unlimited Onsite Help Desk Support - Monday - Friday 8am - 5pm CST during business hours excluding holidays	As needed	YES
Client Help Desk Portal	As needed	YES
Incident Response Plan	As needed	YES
24/7/365 Unlimited Remote Help Desk Support	As needed	YES
SERVERS		
Manage Servers	Ongoing	YES
Check print queues	As needed	YES
Monitor all Server services	Ongoing	YES
Keep Service Packs, Patches and Hot fixes current as per company policy	Monthly	YES
Check event log of every server and identify any potential issues	As things appear	YES
Monitor hard drive free space on server	Ongoing	YES

Exchange Server user/mailbox management	As needed	YES
Monitor Active Directory replication	As needed	YES
Monitor WINS replication	As needed	YES
SQL server management	As needed	YES
Reboot servers if needed	As needed	YES
Run defrag and checks on all drives	As needed	YES
Scheduled off time server maintenance	As needed	YES
Install supported software upgrades	As needed	YES
Determine logical directory structure, Implement, MAP, and detail	As needed	YES
Set up and maintain groups (accounting, admin, printers, sales, warehouse, etc)	As needed	YES
Check status of backups	Daily	YES
Alert Client to dangerous conditions <ul style="list-style-type: none"> • Memory running low • Hard drive showing sign of failure • Hard drive running out of disk space • Controllers losing interrupts • Network Cards report unusual collision activity 	As needed	YES
Educate and correct user errors (deleted files, corrupted files, etc.)	As needed	YES
Clean and prune directory structure, keep efficient and active	As needed	YES
DISASTER RECOVERY		
Disaster Recovery of Server(s)	As needed	YES
DEVICES		
Manage Desktops	Ongoing	YES
Manage Network Printers	Ongoing	YES
Manage Other Networked Devices	Ongoing	YES
Manage PDA's/Smartphones	Ongoing	YES
NETWORKS		

Check router logs	As needed	YES
Performance Monitoring/Capacity Planning	Ongoing	YES
Monitor DSU/TSU, switches, hubs and internet connectivity, and make sure everything is operational (available for SNMP manageable devices only)	Ongoing	YES
SECURITY		
Check firewall logs	As needed	YES
Confirm that antivirus virus definition auto updates have occurred	As needed	YES
Confirm that antispysware updates have occurred	As needed	YES
Confirm that backup has been performed on a week day daily basis	As needed	YES
Create new directories, shares and security groups, new accounts, disable/delete old accounts, manage account policies	As needed	YES
Permissions and file system management	As needed	YES
Set up new users including login restrictions, passwords, security, applications	As needed	YES
Set up and change security for users and applications	Ongoing	YES
Monitor for unusual activity among users	As needed	YES
APPLICATIONS		
Ensure Microsoft Office Applications are functioning as designed	As needed	YES
Ensure provided cybersecurity applications are functioning as designed	As needed	YES
Ensure Adobe Acrobat applications are functioning as designed	As needed	YES
Ensure backup software is functioning as designed	As needed	YES
VENDOR MANAGEMENT		
Manage the following vendor relationships:	As needed	YES
• Phone, Telco & Internet	As needed	YES
• Copiers	As needed	YES

• Proprietary Software Applications	As needed	YES
PROFESSIONAL SERVICES	As Needed	
Technology Solution Design & Development	As needed	NO
Onsite Implementation	As needed	NO
Project Management	As needed	NO
VOIP Phone System Support	As needed	NO
CYBERSECURITY MANAGEMENT		
Continuous Cybersecurity Awareness Training	As needed	YES
Phishing Simulation & Training	As needed	YES
Dark Web Monitoring	As needed	NO
Endpoint Encryption at Rest	As needed	YES
Endpoint Detection & Response (EDR)	As needed	YES
Managed Detection & Response (MDR)	As needed	YES
Managed 24/7 Security Operations Center (SOC)	As needed	YES
Endpoint Remote Monitoring & Management	As needed	YES
Privileged Access Management	As needed	YES
Multi-Factor Authentication (MFA)	As needed	YES
Ongoing Cybersecurity Risk Assessments	As needed	YES
Vulnerability Scanning & Remediations	As needed	YES
Password Management	As needed	YES
Secure Remote Access	As needed	YES
Email Phishing Protection	As needed	YES
Email Account Takeover Protection for Office 365	As needed	YES

Email Encryption	As needed	YES
Microsoft Office 365 Account Management	As needed	YES
Microsoft Office 365 Security Hardening	As needed	YES
Microsoft Office 365 Backup	As needed	YES
Microsoft Office 365 Archiving	As needed	YES
Microsoft Document Sharing	As needed	YES
Microsoft Apps: (Outlook, OneDrive, SharePoint, Teams, Word, Excel, PowerPoint, Exchange, Intune, Defender, Entra ID)	As needed	YES
IT Policy Management	As needed	NO
MANAGED SERVICE SECURITY ENHANCEMENTS		
Managed Firewall as a Service	As needed	YES
Penetration Testing	As needed	NO
DMARC Monitoring & Management	As needed	NO
Zero Trust Application Control	As needed	NO
Security Incident & Event Management (SIEM)	As needed	NO
Security Orchestration Automation & Response (SOAR)	As needed	NO
Managed Extended Detection & Response (MXDR)	As needed	NO
Security Operations Center (SOC) 24/7 Monitoring	As needed	YES
Secure Access Service Edge (SASE)	As needed	NO
Zero Trust Network Access (ZTNA)	As needed	NO
Change Management as a Service	As needed	NO
Managed Print Services	As needed	NO
Compliance Management	As needed	NO

COVERED EQUIPMENT	QUANTITY	NOTES
MANAGED COMPUTERS	8	
MANAGED PRINTERS		
MANAGED NETWORKS	1	
MANAGED SERVERS		
MANAGED CELL/PDA		
MANAGED BDR		
MANGED PHONE SYSTEM		

Service Hours. With respect to all Services marked "Included" above, all non-emergency work performed to maintain Your current systems during Our Regular Business Hours of **Monday-Friday 8:00 a.m. – 5:00 p.m. US Central Time** ("Business Day" or "Regular Business Hours") is included in the Monthly Managed Service Fee stated in **Appendix II** and will not incur additional charges, unless specifically listed under the exclusions below. This does not include **mileage** for non-local travel and additional hardware requested to be purchased and installed, all of which will be billed separately and in addition to any Monthly Managed Service Fees.

If a request for a Service is received by Us prior to the end of the Business Day but the work required to resolve the issue exceeds the amount of time remaining in the Business Day, We will ask

You whether You would like Us to either a) work on the issue after Regular Business Hours, with all time being billed to You at the After-Hours Support Rates set forth in the table below, or b) work on the issue during Regular Business Hours only, beginning with the next Business Day, at no additional charge to You. If We are unable to obtain Your preference, We may use Our discretion, based on the seriousness and apparent urgency of the issue, as to whether to perform the labor after hours at the applicable after-hours rates, or suspend work until the next business day or until You make Your preference known.

If You request an urgent need that cannot wait until the next Business Day, After-Hours or Emergency Rates will apply to all work performed outside of Regular Business Hours.

Minimum Technology Requirements. In order for Your IT Network to qualify for any of Our Managed Service Plans, the following requirements must be met:

- All Servers with Microsoft Windows Operating Systems must be running Windows 2016 Server or later, and have all of the latest Microsoft Service Packs and Critical Updates installed.
- All Desktop PCs and Notebooks/Laptops with Microsoft Windows Operating Systems must be running Windows 11 or later, and have all of the latest Microsoft Service Packs and Critical Updates installed.
- All Server and Desktop Software must be Genuine, Licensed and Vendor-Supported.
- The environment must have a currently licensed, up-to-date and Vendor-Supported Server-based Antivirus Solution protecting all Servers, Desktops, Notebooks/Laptops, and Email.
- The environment must have a currently licensed, Vendor-Supported Server-based Backup Solution that can be monitored, and send notifications on job failures and successes.
- The environment must have a currently licensed, Vendor-Supported Hardware Firewall between the Internal Network and the Internet.
- All Wireless data traffic in the environment must be securely encrypted.
- There must be an outside static IP address or dynamic DNS address assigned to a network device, allowing VPN access.

Costs required to bring Your current environment up to these Minimum Technology Requirements are included in the Onboarding Fee stated in **Appendix II**.

Excluded Products and Services. The following products and Services are specifically excluded from all Managed Service Plans. Hardware, parts and equipment will be provided to You at cost, and all labor will be billed at Our Hourly Rates set forth in **Appendix II** in addition to any Monthly Managed Service Fees:

- The cost of any parts, equipment, or hardware.
 - The cost of any Software, Licensing, or Software Renewal, Subscription or Upgrade Fees of any kind.
 - The cost of any Third Party Vendor- or Manufacturer-Support or Incident Fees of any kind.
 - The cost to bring Your IT Network up to Our Minimum Technology Requirements.
 - Failure of any hardware, software, equipment or component of Your IT Network due to acts of God, building modifications, power failures or other adverse environmental conditions or factors.
 - Service and repairs made necessary by the alteration or modification of any equipment or component of Your IT Network other than as expressly authorized by Us in writing. This includes alterations, software installations or modifications of equipment performed by You or any of Your employees, agents, representatives or contractors other than Us.
 - Programming (modification of software code) and program (software) maintenance unless specified in the table in Section I above or an amendment thereof.
 - Training Services of any kind unless specifically provided for in writing.
 - The cost of replacement of or parts required for repairs on printers, screens or peripherals, (PDA's, Point of Sale Scanners, Digital Cameras, Cell Phones, and other accessories), unless otherwise specified in a written agreement between You and Us.
 - Consumables such as printer maintenance kits, toner, ink, batteries, paper, etc.
 - Costs of replacing chronically failing equipment. (Occasionally equipment which has initially passed Our Minimum Technology Requirements can reveal itself to become chronically failing – repeatedly breaking down and consistently causing user and business interruption even after repairs are accomplished. Should this occur, while rare, You agree to work constructively with Us to replace the equipment at additional cost).
 - Response, remediation and recovery efforts relating to Cybersecurity Incidents (defined below) that are not specifically listed as included in Your Managed Service Plan, or which exceed the number of hours of Cybersecurity Incident work included with Your Services.
-

Cybersecurity Incidents. Even with reasonable protection measures in place, it is possible that Your IT Network may be affected by significant cybersecurity events or incidents that prompt the need for immediate response, remediation and recovery. Such events may include, but are not limited to data breach incidents (including but not limited to incidents involving theft of information); privacy violations; virus or ransomware attacks; cyber attacks on data held by you or any vendors or other third parties; large scale third party software failures or interruptions; and other occurrences that may damage or jeopardize the integrity, confidentiality, or availability of information or Your IT Network or constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies ("Cybersecurity Incident").

You understand and agree that any labor involved in responding to and remediating Cybersecurity Incidents is outside the scope of Your Managed Service Plan and is billed hourly, at Our Hourly Incident Response Rates set forth in **Appendix II**. Should the Cybersecurity Incident result in the need to purchase new hardware or equipment, You understand and agree that the purchase price of same shall be Your responsibility unless otherwise agreed to by both Parties in writing.

In order to minimize downtime and potential losses, You agree to fully comply with any cybersecurity breach or incident response policy or procedure We may issue to You, and to timely cooperate with all of Our instructions and requests for access, assistance and information as we respond to, remediate and launch recovery efforts during and following a Cybersecurity Incident. Failure to cooperate as required herein shall constitute a material violation of this Agreement.

Security Trainings. All of Our clients are provided an IT Policy Manual containing important policies that must be followed in order to keep Your IT Network safe, secure, and functioning as intended.

Reporting. During our business reviews, We will provide you with a list of open service requests along with a comprehensive report containing the following metrics recorded,

- Number and type of service requests opened and closed in the last month
 - Total pending service requests
 - Upcoming Warranty Expirations
 -
-

Upcoming License Renewals

- Recommendations

We may modify the metrics as We improve Our reporting, and as may be requested by You.

Quarterly Business Audit. Our Services to clients on a Managed Service Plan include Quarterly Business Audits for the Term of this Agreement, in which we discuss and analyze items such as last quarter's metrics; your objectives for the upcoming quarter and year; changes in budget; desired changes in technology; and any questions you may have for Us regarding Your IT Network and Services.

If You need to re-schedule a Quarterly Business Audit, You agree to give us at least 5 Business Days' notice by sending an e-mail to qbr@kennedycsi.com. If You don't give us at least 5 Business Days' notice, that quarter's Business Audit will be counted as used.

IV. Hourly And Project-Based Services

Hourly Rates. If You are not on a Managed Service Plan, or You are requesting a Service that is not included in the Managed Service Plan detailed in Section I above, it will be performed pursuant to Our Hourly Rates set forth in **Appendix II**.

Quoted Projects. At times, service requests and projects that are outside the scope of Your Managed Service Plan can be performed more cost effectively as a Quoted Project, i.e. a project performed pursuant a written proposal and agreement setting forth the scope of work with the estimated costs, rather than pursuant to Our Regular Hourly Rates. Services handled on a Quoted Project basis include, but are not limited to a) wiring and installation of new office complexes; b) moving offices from one location to another; c) other services that require extensive labor that does not fall under the maintenance of your current programs and infrastructure. If the Parties agree that a service should be performed as a Quoted Project rather than a task billed hourly, such Quoted Projects will be performed at the costs, fees and terms set forth in a separate Statement of Work or other written instrument signed by You and Us.

EXECUTED BY THE CITY OF RANGER on this the _____ day of June 2025.

Charlie Archer
City Manager

EXECUTED BY KENNEDY COMPUTER SOLUTIONS, INC on this the _____ day of June 2025.

Chance Isham
President

APPENDIX II

PRICING AND RATE SCHEDULE

I. **Onboarding Fee**

All of Our Services begin with Onboarding and Implementation. This initial setup phase takes place within the first 90 days of the Term of the Master Service Agreement, and consists of the following:

- Consulting with You and finalizing Your hardware and software needs;
- Installing initial software and hardware;
- Obtaining licenses and ensuring proper setup of Your accounts;
- Going over Our processes and procedures;
- Training Your team on best practices and important aspects of working with Us.

The following Onboarding and Implementation Fee is payable for the above Services:

\$0 - With 3 year contract, cloud migration, and network upgrade agreed upon.

Please note that the above Onboarding and Implementation Fee is payable solely to cover the initial labor and charges for hardware and software required to ensure that Your IT Network is set up to Your specifications and in a way that supports Our work moving forward. This is in addition to any applicable Monthly Managed Service Fees and Rates listed below. Any costs and fees associated with additional devices and licenses added after the Onboarding and Implementation phase are not covered by the Onboarding and Implementation Fee and may be subject to an additional charge.

II. Managed Service Plan – Monthly Managed Service Fee

The Managed Services listed in **Appendix I** are provided at the following fees:

Number of Users	Fee Per User / Month ("Cost Per Seat")	Total Monthly Managed Service User Fee	
8	\$275	\$2,200	

Number of Devices	Fee Per User / Month ("Cost Per Seat")	Total Monthly Managed Service Device Fee			
Number of Servers	Fee Per User / Month ("Cost Per Seat")	Total Monthly Managed Service Server Fee			
Number of Firewalls	Fee Per User / Month ("Cost Per Seat")	Total Monthly Managed Service Firewall Fee			
Number of Add-On	Fee per add-on service	Total Monthly Add-On Service Fee			

Any services, tasks, and goods not specifically listed as included in **Appendix I** are excluded from the Monthly Managed Service Fee, and will be invoiced separately at the Rates specified in the table below, or as otherwise agreed by You and Consultant pursuant to a written Proposal, Quote or Service Request.

Additional Users, Devices and Services. If You wish to add new users, devices or services to the Managed Service Plan, the Monthly Managed Service Fee will be subject to an increase based on the number of users added, their specific needs, the number and types of devices and

licenses/subscriptions being added, as well as the overall impact of the increase on system resources (including potential necessity to upgrade hardware and certain services), and other important factors. You acknowledge and agree that in all instances when Services are modified, an amended Pricing Appendix reflecting such changes must be executed by both Parties prior to implementation of any changes, the purchase of the new devices and/or the onboarding of new users.

Reducing Number of Users. For some software licenses, it may be necessary to consent to a 12-month commitment, or You may elect a 12-month commitment term for some or all users with such license ("License Commitment Term") in order to obtain a discount on the total amount paid for the license. In cases where such a commitment is made, You acknowledge and agree that a) if You wish to reduce the number of users on Your Managed Service Plan, You must provide us with written notice of the specific user accounts You wish to cancel; and b) You will continue to be responsible for paying all remaining months on any applicable License Commitment Terms as a lump sum payment due at the time the termination of the license ("License Termination Fee"). If the license fees were included in Your Monthly Managed Service Fee, the amount of the Monthly Managed Service Fee will be updated to reflect the modified user count when the licenses expire // when the License Termination Fee is received.

Annual Fee Increase. In order to account for rising operating costs, cost of inflation and price increases by our vendors and suppliers, the Monthly Managed Service Fee provided above is subject to an annual increase of 3-5% each calendar year, on the anniversary of the signing of this Agreement. Our Hourly Services fees will increase annually by 5% rounded up to the nearest \$5. The fee increase applies to all contracts regardless of term, and will be communicated to You no less than 30 days in advance of the increase. As We guarantee that the rate of increase will never exceed 5%, a change in MRC as described this paragraph shall not serve as grounds for terminating this Agreement.

III. Hourly Services – Rate Schedule

Hourly Rates. For tasks and projects that fall outside of the scope of Your Managed Service Plan contained in Appendix I, or if You are not on a Managed Service Plan, Our services are billed at the following rates, unless otherwise specified in a custom Quote, Proposal, Service Order or other agreement between You and Us:

Tier 1 Support \$100/Hour	Tier 2 Support \$125/Hour	Tier 3 Support \$175/Hour	Emergency/After-Hours \$150-350/hour based on Tiered Support
Basic Desktop and Remote Support	Specialty Software Support	Server Software Upgrades	Ransomware Recovery
Basic Network Support	Advanced Onsite, Remote and Desktop Support	Server, Network, and System Changes	Remote and Desktop Support

Incident Response Rates. Incident response due to a cybersecurity breach may require us to engage additional 3rd party vendor support. Especially, if insurance companies are involved. Incident response rates can vary between \$350-\$600 per hour with a typical initial engagement retainer fee of \$5,000-\$10,000 based on the nature of the incident.

All on-site visits will be billed with a 1-hour minimum charge. All remote support is billed in half-hour increments.

Support Tiers. Our Support Tier levels and how issues are moved from lower to higher support tiers are outlined in Your Client Handbook.

Tier Designation. The designation of a technician's support level as Tier 1, Tier 2, and Tier 3 shall be determined solely at the discretion of KCS. This designation will be based on the technician's number of years of experience within the industry and their tenure with KCS. We reserve the right to evaluate and adjust these designations as deemed necessary without notice.

IV. Mileage

For tasks and projects within the scope of Your Managed Service Plan contained in **Appendix I**, all travel is included. For tasks that are outside the scope of Your Managed Service Plan, or if You are not on any Managed Service Plan, all Non-Local Travel is billed at the current IRS rates for mileage reimbursement plus Our Hourly Rates for any travel time accrued. Out-of-state travel may incur

additional charges, including but not limited to airfare (economy), vehicle rental, parking and meals that are subject to reimbursement by You.

Non-Local Travel is defined as any trip more than 30-miles one way from Our Eastland, TX office location.

Billable time for on-location Services begins when Our personnel leave their office, and ends when personnel arrive back at their office. For all Services within Your Managed Service Plan, local travel (less than 30 miles one-way) is included within the Monthly Managed Service Fee.

V. **Emergency & After-Hours Support**

If You are on a Managed Service Plan, all work performed on tasks that are both a) included in the Managed Service Plan (see **Appendix I**) and b) performed during normal working hours from 8am-5pm US Central Time, Monday through Friday, excluding Holidays ("Regular Business Hours"), is included in the Monthly Managed Service Fee specified above.

Onsite work performed outside of Regular Business Hours, i.e. on weekends, Holidays, and weekdays before 8:00 A.M or after 5:00 P.M. US Central Time, is not included in any unlimited remote helpdesk hours in any Managed Service or Break/Fix Plan and will be billed at Our After-Hours and Emergency Rate of \$150-350/hour based on Tiered support level. M-Sat is 1.5x, Sunday is 2x, and Holiday is 2x.

While We strive to meet the needs of all of Our clients – even after hours and on holidays – We cannot guarantee the same response times for after-hours requests as standard business hours, unless the request is clearly indicated as an Emergency and is submitted via the appropriate channels outlined in the Client Handbook. If You experience an emergency and require immediate service outside of our Regular Business Hours, You must follow the instructions in the Client Handbook for submitting an Emergency request. All such requests must clearly state the urgency of the issue and the desired timeline for a resolution. You agree that all Emergency and After-Hours Support will be billable at Our Emergency and After-Hours Rate, and that Support may not be available on Major holidays such as Christmas day or Thanksgiving Day.

The following holidays are observed by Us (if a Holiday falls on a Saturday or Sunday, then the Holiday will be observed on the Friday preceding, or the Monday following, said Holiday):

- Christmas Day
- Christmas Eve
- New Year's Day
- Good Friday
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- Black Friday

EXECUTED BY THE CITY OF RANGER on this the _____ day of June 2025.

Charlie Archer
City Manager

EXECUTED BY KENNEDY COMPUTER SOLUTIONS, INC on this the _____ day of June 2025.

Chance Isham
President

May 9, 2025

City of Ranger
400 West Main St
Ranger, TX 76470-1219

Dear Hope DeLaTorre,

Thank you for your continued partnership with the TX Health Benefits Pool. We're proud to serve public organizations like yours, with a Board of Trustees made up of current or former local government officials. This special leadership structure helps make sure your voice is heard when shaping your healthcare coverage.

The overall risk profile of the Pool remains strong, thanks to your efforts in educating our members about the programs and services available with Pool coverage. Based on the Pool's positive performance, I'm happy to announce that we are only making a few limited changes to our benefits this year.

Here's a list of the changes and improvements for the upcoming 25/26 plan year:

- **Benefit Change – Direct Primary Care (DPC) Plan:** The DPC plan will now include copays for physicians outside of the DPC office. Members enrolled in a DPC plan will pay \$0 for an office visit with their DPC provider. If they choose to see a different primary care provider, a \$50 copay will apply. Specialist visits will be a \$75 copay. Other types of services (surgery, major imaging, etc.) will apply toward the \$3,000 deductible.
- **Member Rewards-** We will be sunsetting the Member Rewards program, with its last effective date for all groups being December 31, 2025.
- **NEW – Twin Health:** Our pilot program helps members with type 2 diabetes live healthier lives and potentially reverse their condition through a partnership with Twin Health. Early results and feedback is excellent.
- **NEW – Next Level Weight Loss Program:** This program helps members lose weight through compounded GLP1 medications, starting at \$199 a month.
- **Lantern:** Formerly known as Surgery Plus, Lantern provides high-quality, affordable surgical care with significant savings for your employees. TXHB will be adding the following services to Lantern: **Endoscopies, Colonoscopies, Tonsillectomies, and Pain Management**
- **TXHB Well:** We will continue offering free onsite biometric screenings through Circle Wellness, along with \$150 for members who complete certain preventive or healthy activities

Your marketing representative Heather VonGonten will contact you soon to discuss your renewal options, budget, and ways to help your employees save on healthcare costs with products like FSAs or HSAs.

Open enrollment is scheduled for 08/01/2025 - 08/15/2025. We offer easy self-service and phone enrollment options to make the process simple for your employees.

To ensure a smooth transition, please provide your renewal decision at least 90 days before your anniversary date of 10/01/2025. Heather can help you complete the renewal form. You can reach Heather at 512-719-6519 or Heather.VonGonten@txhb.gov.

Thank you for trusting us with your employee healthcare coverage. We look forward to serving you and your employees again this year.

Sincerely,



Jennifer Hoff
Executive Director



BOARD OF TRUSTEES

Chair

Mike Smith, Region 5
City Manager, City of Jacksboro

Vice Chair

Joe Cardenas, Region 7
Asst. City Manager, City of Uvalde

Joseph Price, Region 2

City Manager, City of Canyon

Elena Quintanilla, Region 3

City Administrator, Town of Ransom Canyon

Rex Thee, Region 4

City Manager, City of Monahans

Tony Aaron, Region 6

City Administrator, City of Early

Sterling Naron, Region 8

City Administrator, City of Hudson Oaks

Warren Anglin, Region 9

Mayor Pro-Tem, City of Groesbeck

Ashley Wayman, Region 10

City Administrator, City of Rollingwood

John Green, Region 11

Mayor Pro-Tem, City of Portland

Wendi Delgado, Region 12

Director of Operations, City of South Padre Island

Jeff Jordan, Region 13

Mayor, City of Kaufman

Fabrice Kabona, Region 14

City Manager, City of Madisonville

Wendy Hudman, Region 15

City Accountant, City of Carthage

Jon Sherwin, Region 16

Director of Public Works, City of West Orange

Glen Metcalf, Appointee

Former City Manager, City of Canyon

Jay Stokes, Appointee

City Manager, City of Deer Park

Larry Fields, Appointee

Former City Manager, City of Graham

Lew White DDS, Appointee

Mayor, City of Lockhart

Mike Slye, Appointee

Former City Manager, City of Kaufman

Stephen Haynes, Appointee

Mayor, City of Brownwood

Mike Stelly, Appointee

Chief of Police, City of West Orange



Renewal Notice and Benefit Verification Form

Ranger

Original

Plan Year 10/01/2025 - 09/30/2026 (12 Months)

IMPORTANT NOTICE: A signed renewal is required by the due date in your cover letter. If TX Health Benefits Pool does not receive the fully executed renewal notice by the indicated due date, you will no longer have an option to change benefits which will result in renewal of the benefit plans listed below at the new rates and the current employer contributions.

Medical

Employer Group Medical Plan

Plan	Benefit Percent	In Net Ded	Out Net Ded	In Net OOP	Office Visit	Rates	Current	New
Coplay-3K-7K ER-DAW1&2	80/50	\$3000	\$6000	\$7000	\$30	EE Only	\$748.24	\$748.24
						EE + Spouse:	\$1,518.94	\$1,518.94
						EE + Child(ren):	\$1,316.90	\$1,316.90
						EE + Family	\$2,207.28	\$2,207.28

In Network Deductible applies towards In Network OOP.

Medical and Dental Plan Accumulators will be based on Plan Year.

Monthly Employer Contribution Amounts

TX Health Benefits Pool requires 75% employer contribution toward employee medical – Minimum employer contribution is \$561.18.

Please enter your monthly employer contribution amounts for active employees here, in dollars or percentages:

Plan	EE Only		EE+Spouse*		EE+Child(ren)*		EE+Family*	
	Amount	% of Rate**	Amount	% of Rate**	Amount	% of Rate**	Amount	% of Rate**
Coplay-3K-7K ER-DAW1&2	\$ _____ or _____ %		\$ _____ or _____ %		\$ _____ or _____ %		\$ _____ or _____ %	

*If entering contributions in dollars, the dependent tier(s) must include the EE Only amount paid by employer in addition to any employer paid amounts for dependents. Percentages for dependent tier(s) will apply to the dependent tier amount less the EE Only amount.

**NOTE: If a contribution percentage is provided, it will be rounded up to the nearest penny.

Are there different contributions based on other factors (ex: hourly vs salary, department or location based)? If so, please explain here:

Dental

Rates	Current (Vol Dental IV)	New (Vol Dental IV)
EE Only:	\$37.86	\$37.86
EE + Spouse:	\$89.04	\$89.04
EE + Child(ren):	\$81.44	\$81.44
EE + Family:	\$113.64	\$113.64

Please enter your monthly employer contribution amounts for active employees here, in dollars or percentages:

EE Only:		EE+Spouse*:		EE+Child(ren)*:		EE+Family*:	
Amount	% of Rate**	Amount	% of Rate**	Amount	% of Rate**	Amount	% of Rate**
\$ _____ or _____ %		\$ _____ or _____ %		\$ _____ or _____ %		\$ _____ or _____ %	

*If entering contributions in dollars, the dependent tier(s) must include the EE Only amount paid by employer in addition to any employer paid amounts for dependents. Percentages for dependent tier(s) will apply to the dependent tier amount less the EE Only amount.

**NOTE: If a contribution percentage is provided, it will be rounded up to the nearest penny.

Vision

<u>Rates</u>	<u>Current (Vol Premium)</u>	<u>New (Vol Premium)</u>
EE Only:	\$12.58	\$12.58
EE + Spouse:	\$23.92	\$23.92
EE + Child(ren):	\$25.18	\$25.18
EE + Family:	\$32.10	\$32.10

Please enter your monthly employer contribution amounts for active employees here, in dollars or percentages:

<u>EE Only:</u>		<u>EE+Spouse*:</u>		<u>EE+Child(ren)*:</u>		<u>EE+Family*:</u>	
<u>Amount</u>	<u>% of Rate**</u>	<u>Amount</u>	<u>% of Rate**</u>	<u>Amount</u>	<u>% of Rate**</u>	<u>Amount</u>	<u>% of Rate**</u>
\$ _____ or _____ %		\$ _____ or _____ %		\$ _____ or _____ %		\$ _____ or _____ %	

*If entering contributions in dollars, the dependent tier(s) must include the EE Only amount paid by employer in addition to any employer paid amounts for dependents. Percentages for dependent tier(s) will apply to the dependent tier amount less the EE Only amount.

****NOTE:** If a contribution percentage is provided, it will be rounded up to the nearest penny

Basic Life and AD&D: Plan 8 (\$10,000)

	<u>Current Rate</u>	<u>New Rate</u>
Life:	\$0.178	\$0.178
AD&D:	\$0.040	\$0.040

Note: Plan requires 100% Participation and is 100% EMPLOYER paid.

Additional Employee Life and AD&D

<u>Age of Employee</u>	<u>Current Rate per \$1000</u>	<u>New Rate per \$1000</u>
Under 30	0.041	0.041
30 - 34	0.052	0.052
35 - 39	0.091	0.091
40 - 44	0.129	0.129
45 - 49	0.198	0.198
50 - 54	0.332	0.332
55 - 59	0.595	0.595
60 - 64	0.913	0.913
65 - 69	1.513	1.513
70 and over	2.431	2.431

Note: Plan is EMPLOYEE paid.

Dependent Life: Plan 3 (\$10,000/\$2,000)

<u>Current Rate</u>	<u>New Rate</u>
\$2.76 per dependent unit	\$2.76 per dependent unit

Note: Plan is EMPLOYEE paid.

COBRA Eligibility and Administration (Continuation of Coverage)

COBRA Eligible? Yes
 COBRA Administration through TX Health Benefits Pool? Yes

NOTE: Employer will be charged a flat monthly fee of \$80 per month regardless of how many members are utilizing COBRA, as well as \$10 per month for each member who elects COBRA.

Benefit Waiting Period

90 days after date of hire

Required Annual Eligibility and Enrollment Information

Please provide the following information:

- 1. Will you allow Employee Self Service (ESS) via TXHB Online for Open Enrollment and Qualifying Life Events? No Yes
- 2. Our records indicate that Employer Member DOES NOT currently have an Ordinance or Resolution authorizing the offering of Elected Official Benefit Coverage. Please contact your Account Executive/Account Manager if this needs to be updated.

Signature Section

The undersigned employer hereby acknowledges that for an employee to receive coverage, TX Health Benefits Pool must receive enrollment information within thirty-one (31) days of the date of hire or within thirty-one (31) days of the coverage effective date, whichever is later, regardless of whether the Employer has a waiting period or a waiting and orientation period. If an enrollment is not submitted within this timeline, the employee cannot be added to the Plan until the next Open Enrollment period or a qualifying event occurs.

Employer Member Additional Acknowledgements and Agreements

- 1. Employer Member acknowledges and agrees that its signature on this Renewal Notice and Benefit Verification Form indicates its binding selections for renewal services through TX Health Benefits Pool.
- 2. Employer Member acknowledges that certain benefit service selections require completion and execution of additional forms and agreements and agrees that it will work with all due diligence and in good faith to complete, execute, and return all necessary forms and agreements to TX Health Benefits Pool prior to the beginning of the Group's open enrollment.
- 3. Employer Member acknowledges that TX Health Benefits Pool will only allow open enrollment for renewal services in good faith and without receiving all necessary signed benefit service forms and agreements if:
 - A. A signed Renewal Notice and Benefit Verification Form with all necessary Employer Member selections and information has been received; and
 - B. Employer Member has in good faith attempted but failed to approve and return the applicable benefit service forms and agreements timely.
- 4. Employer certifies that it has adopted an Employee Flexible Benefits Plan under Section 125 of the Internal Revenue Code. This Plan is offered to all eligible employees who are qualified by employment status.
- 5. Employer certifies that it will provide notice of the creditable status of the coverage it offers to new enrollees prior to the effective date of their coverage, as required by the Medicare Modernization Act.
- 6. TX Health Benefits requires groups to enroll 100% of their benefit eligible employees. This is also known as the 100% Participation Rule. Employers may have employees that wish to waive Medical coverage through TX Health Benefits Pool, however, waivers may only be granted for the reasons enumerated in your Plan Book.

Please sign by the due date and return this completed form via email to your Account Executive/Account Manager or marketing@txhb.gov.

756000645

Tax ID Number

Authorized Signature

Date

Printed Name

Title

The rates are based on census information five months prior to plan year. If the census changes by more than 10%, TX Health Benefits Pool reserves the right to revise rates due to census change and underwriting impact

Rates are subject to change due to intervening events such as action taken by the TX Health Benefits Pool Board of Trustees, legislation passed during the plan year, or other events affecting benefits.

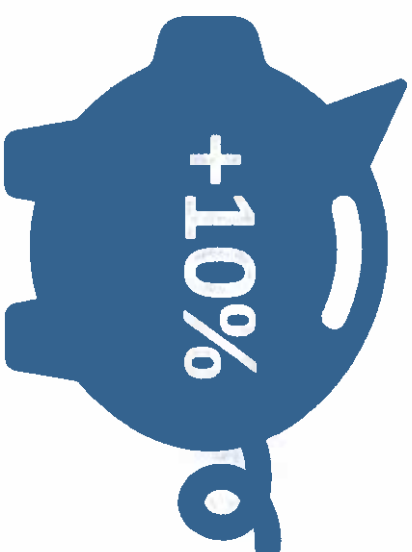
Supplemental benefits cannot be accessed without accessing the TX Health Benefits Pool Medical Benefit Plan.

YOUR RENEWAL QUOTE INCLUDES PROPRIETARY INFORMATION THAT SHOULD NOT BE SHARED WITH OTHER COMPETITORS OR USED TO CIRCUMVENT THE REQUIREMENTS OF TEXAS COMPETITIVE BIDDING LAWS. IN THE EVENT YOU RECEIVE A RENEWAL QUOTE AND LATER DECIDE TO ISSUE AN RFP, THE RENEWAL QUOTE MAY NOT BE SHARED WITH ANY OTHER COMPETITORS AS DOING SO WOULD DISADVANTAGE TX HEALTH BENEFITS POOL IN THE COMPETITIVE PROCESS. TX HEALTH BENEFITS POOL ALSO RESERVES THE RIGHT TO REVISE PREVIOUSLY ISSUED RATES IN RESPONSE TO YOUR RFP.

Texas Health Benefits Pool 5 Year Average Rate Increase



TX Health Benefits Pool



Industry Average

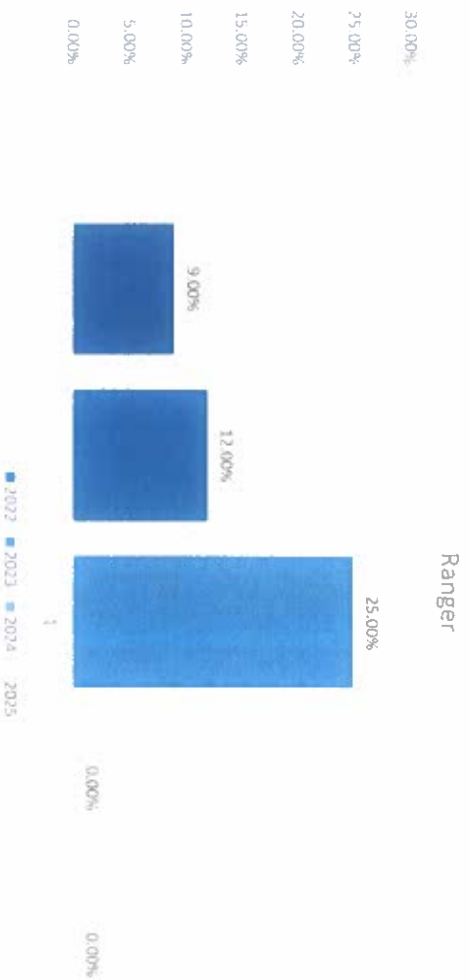
5 Year Rate Average According to Milliman

City of Ranger

Historical Premium Rate and Benefit Modification

2021	2022	2023	2024	2025	Overall Average
9.00%	12.00%	25.00%	0.00%	0.00%	9.20%

Average Renewal Increase % from 2021 - 2025



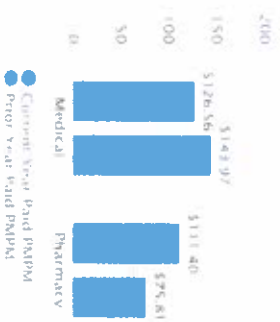
Rolling 12 Months

This information below is designed to assist you in understanding how your medical plan has been used during the 12-month reporting period. However, this information should not be considered the sole determinant in estimating future medical plan renewal costs.

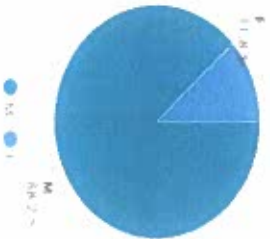
Rolling 12 Month - US0

Population Change

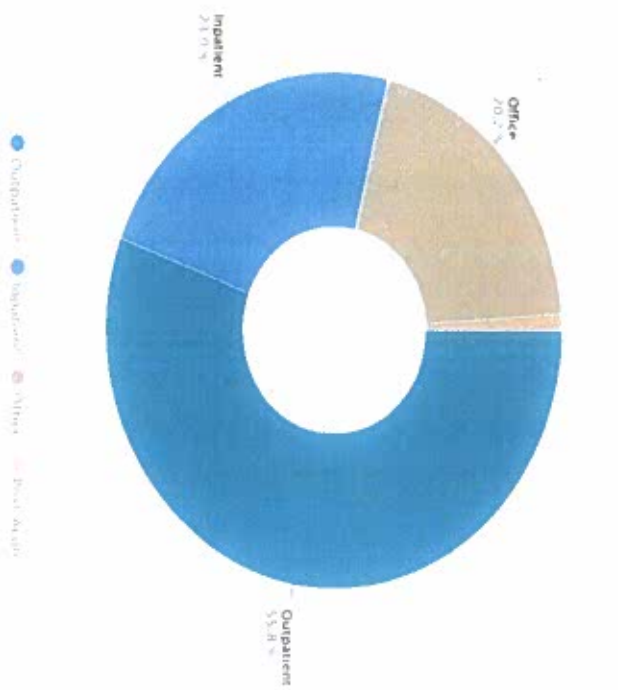
Total Paid Amount Per Member Per Month



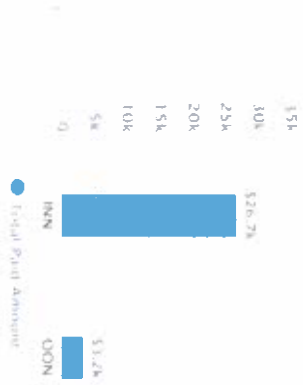
Gender



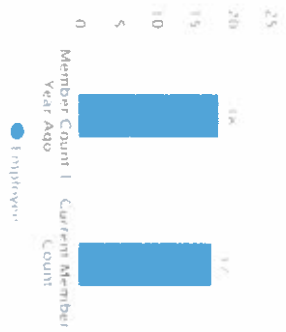
Total Paid Amount by Point of Service



Total Paid Network Status



Medical Enrollee Member Count - Year Over Year



Valued Partnership

We serve you, not shareholders

The right plan at the right price

A dedicated account team

Nationwide network

Access to a virtual doctor visit, anywhere, anytime

Two wellness programs

Personalized concierge assistance

TX HB

Your Dedicated TXHB Team

City of Ranger

Heather VonGonten
Account Executive

Phone
512-719-6519

Email
Heather.VonGonten@txhb.gov

Jackie Acevedo
Account Manager

Phone
512-719-6513

Email
Jackie.Acevedo@txhb.gov

Adrienne Milligan
Health & Wellness

Phone
512-719-6712

Email
adrienne.milligan@txhb.gov

TX HB



Renewal Notice and Benefit Verification Form

Ranger

Original

Plan Year 10/01/2025 - 09/30/2026 (12 Months)

IMPORTANT NOTICE: A signed renewal is required by the due date in your cover letter. If TX Health Benefits Pool does not receive the fully executed renewal notice by the indicated due date, you will no longer have an option to change benefits which will result in renewal of the benefit plans listed below at the new rates and the current employer contributions.

Medical

Employer Group Medical Plan

Plan	Benefit Percent	In Net Ded	Out Net Ded	In Net OOP	Office Visit	Rates	Current	New
Copay-3K-7K ER-DAW1&2	80/50	\$3000	\$6000	\$7000	\$30	EE Only:	\$748.24	\$748.24
						EE + Spouse:	\$1,518.94	\$1,518.94
						EE + Child(ren):	\$1,316.90	\$1,316.90
						EE + Family:	\$2,207.28	\$2,207.28

In Network Deductible applies towards In Network OOP.

Medical and Dental Plan Accumulators will be based on Plan Year.

Monthly Employer Contribution Amounts

TX Health Benefits Pool requires 75% employer contribution toward employee medical – Minimum employer contribution is \$561.18.

Please enter your monthly employer contribution amounts for active employees here, in dollars or percentages:

Plan	EE Only:		EE+Spouse*:		EE+Child(ren)*:		EE+Family*:	
	Amount	% of Rate**	Amount	% of Rate**	Amount	% of Rate**	Amount	% of Rate**
Copay-3K-7K ER-DAW1&2	\$ _____ or _____ %		\$ _____ or _____ %		\$ _____ or _____ %		\$ _____ or _____ %	

*If entering contributions in dollars, the dependent tier(s) must include the EE Only amount paid by employer in addition to any employer paid amounts for dependents. Percentages for dependent tier(s) will apply to the dependent tier amount less the EE Only amount.

**NOTE: If a contribution percentage is provided, it will be rounded up to the nearest penny.

Are there different contributions based on other factors (ex: hourly vs salary, department or location based)? If so, please explain here:

Dental

Rates	Current (Vol Dental IV)	New (Vol Dental IV)
EE Only:	\$37.86	\$37.86
EE + Spouse:	\$89.04	\$89.04
EE + Child(ren):	\$81.44	\$81.44
EE + Family:	\$113.64	\$113.64

Please enter your monthly employer contribution amounts for active employees here, in dollars or percentages:

EE Only:		EE+Spouse*:		EE+Child(ren)*:		EE+Family*:	
Amount	% of Rate**	Amount	% of Rate**	Amount	% of Rate**	Amount	% of Rate**
\$ _____ or _____ %		\$ _____ or _____ %		\$ _____ or _____ %		\$ _____ or _____ %	

*If entering contributions in dollars, the dependent tier(s) must include the EE Only amount paid by employer in addition to any employer paid amounts for dependents. Percentages for dependent tier(s) will apply to the dependent tier amount less the EE Only amount.

**NOTE: If a contribution percentage is provided, it will be rounded up to the nearest penny.

Vision

<u>Rates</u>	<u>Current (Vol Premium)</u>	<u>New (Vol Premium)</u>
EE Only:	\$12.58	\$12.58
EE + Spouse:	\$23.92	\$23.92
EE + Child(ren):	\$25.18	\$25.18
EE + Family:	\$32.10	\$32.10

Please enter your monthly employer contribution amounts for active employees here, in dollars or percentages:

<u>EE Only:</u>		<u>EE+Spouse*:</u>		<u>EE+Child(ren)*:</u>		<u>EE+Family*:</u>	
<u>Amount</u>	<u>% of Rate**</u>	<u>Amount</u>	<u>% of Rate**</u>	<u>Amount</u>	<u>% of Rate**</u>	<u>Amount</u>	<u>% of Rate**</u>
\$ _____ or _____ %		\$ _____ or _____ %		\$ _____ or _____ %		\$ _____ or _____ %	

*If entering contributions in dollars, the dependent tier(s) must include the EE Only amount paid by employer in addition to any employer paid amounts for dependents. Percentages for dependent tier(s) will apply to the dependent tier amount less the EE Only amount.

****NOTE:** If a contribution percentage is provided, it will be rounded up to the nearest penny

Basic Life and AD&D: Plan 8 (\$10,000)

	<u>Current Rate</u>	<u>New Rate</u>
Life:	\$0.178	\$0.178
AD&D:	\$0.040	\$0.040

Note: Plan requires 100% Participation and is 100% EMPLOYER paid.

Additional Employee Life and AD&D

<u>Age of Employee</u>	<u>Current Rate per \$1000</u>	<u>New Rate per \$1000</u>
Under 30	0.041	0.041
30 - 34	0.052	0.052
35 - 39	0.091	0.091
40 - 44	0.129	0.129
45 - 49	0.198	0.198
50 - 54	0.332	0.332
55 - 59	0.595	0.595
60 - 64	0.913	0.913
65 - 69	1.513	1.513
70 and over	2.431	2.431

Note: Plan is EMPLOYEE paid.

Dependent Life: Plan 3 (\$10,000/\$2,000)

<u>Current Rate</u>	<u>New Rate</u>
\$2.76 per dependent unit	\$2.76 per dependent unit

Note: Plan is EMPLOYEE paid.

COBRA Eligibility and Administration (Continuation of Coverage)

COBRA Eligible? Yes
 COBRA Administration through TX Health Benefits Pool? Yes

NOTE: Employer will be charged a flat monthly fee of \$80 per month regardless of how many members are utilizing COBRA, as well as \$10 per month for each member who elects COBRA.

Benefit Waiting Period

90 days after date of hire

Required Annual Eligibility and Enrollment Information

Please provide the following information:

- 1. Will you allow Employee Self Service (ESS) via TXHB Online for Open Enrollment and Qualifying Life Events? No Yes
- 2. Our records indicate that Employer Member DOES NOT currently have an Ordinance or Resolution authorizing the offering of Elected Official Benefit Coverage. Please contact your Account Executive/Account Manager if this needs to be updated

Signature Section

The undersigned employer hereby acknowledges that for an employee to receive coverage, TX Health Benefits Pool must receive enrollment information within thirty-one (31) days of the date of hire or within thirty-one (31) days of the coverage effective date, whichever is later, regardless of whether the Employer has a waiting period or a waiting and orientation period. If an enrollment is not submitted within this timeline, the employee cannot be added to the Plan until the next Open Enrollment period or a qualifying event occurs.

Employer Member Additional Acknowledgements and Agreements

- 1. Employer Member acknowledges and agrees that its signature on this Renewal Notice and Benefit Verification Form indicates its binding selections for renewal services through TX Health Benefits Pool.
- 2. Employer Member acknowledges that certain benefit service selections require completion and execution of additional forms and agreements and agrees that it will work with all due diligence and in good faith to complete, execute, and return all necessary forms and agreements to TX Health Benefits Pool prior to the beginning of the Group's open enrollment.
- 3. Employer Member acknowledges that TX Health Benefits Pool will only allow open enrollment for renewal services in good faith and without receiving all necessary signed benefit service forms and agreements if:
 - A. A signed Renewal Notice and Benefit Verification Form with all necessary Employer Member selections and information has been received; and
 - B. Employer Member has in good faith attempted but failed to approve and return the applicable benefit service forms and agreements timely.
- 4. Employer certifies that it has adopted an Employee Flexible Benefits Plan under Section 125 of the Internal Revenue Code. This Plan is offered to all eligible employees who are qualified by employment status.
- 5. Employer certifies that it will provide notice of the creditable status of the coverage it offers to new enrollees prior to the effective date of their coverage, as required by the Medicare Modernization Act.
- 6. TX Health Benefits requires groups to enroll 100% of their benefit eligible employees. This is also known as the 100% Participation Rule. Employers may have employees that wish to waive Medical coverage through TX Health Benefits Pool, however, waivers may only be granted for the reasons enumerated in your Plan Book

Please sign by the due date and return this completed form via email to your Account Executive/Account Manager or marketing@txhb.gov.

756000645

Tax ID Number

Authorized Signature

Date

Printed Name

Title

The rates are based on census information five months prior to plan year. If the census changes by more than 10%, TX Health Benefits Pool reserves the right to revise rates due to census change and underwriting impact.

Rates are subject to change due to intervening events such as action taken by the TX Health Benefits Pool Board of Trustees, legislation passed during the plan year, or other events affecting benefits.

Supplemental benefits cannot be accessed without accessing the TX Health Benefits Pool Medical Benefit Plan.

YOUR RENEWAL QUOTE INCLUDES PROPRIETARY INFORMATION THAT SHOULD NOT BE SHARED WITH OTHER COMPETITORS OR USED TO CIRCUMVENT THE REQUIREMENTS OF TEXAS COMPETITIVE BIDDING LAWS. IN THE EVENT YOU RECEIVE A RENEWAL QUOTE AND LATER DECIDE TO ISSUE AN RFP, THE RENEWAL QUOTE MAY NOT BE SHARED WITH ANY OTHER COMPETITORS AS DOING SO WOULD DISADVANTAGE TX HEALTH BENEFITS POOL IN THE COMPETITIVE PROCESS. TX HEALTH BENEFITS POOL ALSO RESERVES THE RIGHT TO REVISE PREVIOUSLY ISSUED RATES IN RESPONSE TO YOUR RFP.



RESOLUTION 2025-06-23-A

A RESOLUTION OF THE CITY OF RANGER, TEXAS, APPROVING SUBMISSION OF A GRANT FOR LICENSE PLATE READERS FOR USE BY THE RANGER POLICE DEPARTMENT, AND NAMING THE CITY MANAGER AS SIGNATORY, FINANCE DIRECTOR AS FINANCIAL OFFICER, AND POLICE CHIEF AS PROJECT DIRECTOR FOR SUCH GRANT.

WHEREAS, the Ranger City Commission finds it in the best interest of the citizens of Ranger that the License Plate reader project be operated in the 2025 fiscal year; and

WHEREAS, the City of Ranger agrees to provide applicable matching funds for the said project as required by the DJ-Edward Byrne Memorial Justice Assistance Grant Program grant application; and

WHEREAS, the City of Ranger agrees that in the event of loss or misuse of the Office of the Governor funds, the City of Ranger assures that the funds will be returned to the Office of the Governor in full; and

WHEREAS, the Ranger City Commission designates the City Manager as the grantee's authorized official. The authorized official is given the power to apply for, accept, reject, alter or terminate the grant on behalf of the applicant agency; and

WHEREAS, the Ranger City Commission designates the Finance Director as the grantee's Financial Officer and the Police Chief as the grantee's Project Director.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COMMISSION OF THE CITY OF RANGER, TEXAS:

Approves submission of the grant application for the License Plate Readers to the Office of the Governor.

PASSED AND APPROVED this 23rd day of June, 2025.

Robert Butler, Mayor

ATTEST:

Hope Delatorre, City Secretary



Resolution No. 2025-06-23-B

**A RESOLUTION OF THE CITY OF RANGER, TEXAS, AUTHORIZING
THE OPENING OF A NEW BANK ACCOUNT FOR THE FUNDING FROM
THE WILDFIRE MITIGATION GRANT**

WHEREAS: the City of Ranger has been entered into a grant for the purpose of Wildfire Mitigation; and

WHEREAS: the City of Ranger has applied for financing to assist with purchasing of equipment until the grant is issued; and

WHEREAS: the financing cannot be issued without a designated account for the funding for the Wildfire Mitigation Grant; and

WHEREAS: the City of Ranger must maintain current online banking administrator,

**NOW THEREFORE, BE IT RESOLVED BY THE CITY COMMISSION OF THE CITY
OF RANGER:**

Section 1: A new account be opened at the First Financial Bank for the purpose of financing for the Wildfire Mitigation Grant

PASSED AND APPROVED this 23th day of June, 2025.

Attest:

Hope Delatorre, City Secretary

Robert Butler, Mayor

RESOLUTION NO. 2025-06-09-D

A RESOLUTION OF THE CITY OF RANGER, TEXAS, ADOPTING THE RANGER ECONOMIC DEVELOPMENT CORPORATION 4A & 4B INVESTMENT POLICY “REDC 4A & 4B” ATTACHED HERETO AS EXHIBIT “A”; DECLARING THAT THE CITY COUNCIL HAS COMPLETED ITS REVIEW OF THE INVESTMENT POLICY AND INVESTMENT STRATEGIES OF THE REDC 4A & 4B INVESTMENT POLICY AND THAT EXHIBIT “A” RECORDS ANY CHANGES TO THE PREVIOUS INVESTMENT POLICY OR INVESTMENT STRATEGIES; PROVIDING A REPEALING CLAUSE; PROVIDING A SEVERABILITY CLAUSE; AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, in accordance with the Public Funds Investment Act, Chapter 2256, Texas Government Code, the City Commission of the City of Ranger, Texas by resolution adopted an investment policy; and

WHEREAS, Section 2256.005, Texas Government Code requires the City Council to review the investment policies and investment strategies not less than each fiscal year end and to adopt a resolution or order stating the review has been completed and recording any changes made to either the investment policies or investment strategies.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF RANGER, TEXAS:

SECTION 1. That the REDC 4A & 4B Investment Policy attached hereto as Exhibit “A” is hereby adopted and shall govern the investment policies and investment strategies for the REDC 4A & 4B, and shall define the authority of the investment officials of the City and REDC 4A & 4B from and after the effective date of this resolution.

SECTION 2. That the City Commission of the City of Ranger has completed its review of the investment policies and investment strategies and any changes made to either the investment policies or investment strategies are recorded in Exhibit “A” hereto.

SECTION 3. That all provisions of the resolution of the City of Ranger, Texas, in conflict with the provisions of this resolution be, and the same are hereby repealed, and all other provisions not in conflict with the provisions of this resolution shall remain in full force and effect.

SECTION 4. That should any word, sentence, paragraph, subdivision, clause, phrase or section of this resolution be adjudged or held to be void or unconstitutional, the same shall not affect the validity of the remaining portions of said resolution which shall remain in full force and affect.

SECTION 5. That this resolution shall become effective immediately from and after its passage.

DULY RESOLVED AN ADOPTED BY THE City Commission of the City of Ranger, Texas, on this the 23rd day of June, 2025.

CITY OF RANGER, TEXAS

Robert Butler, Mayor

ATTEST:

Hope Delatorre, City Secretary

City of Ranger, Texas
INVESTMENT POLICY AND STRATEGY
Adopted June 23, 2025

I. INTRODUCTION

It is the policy of the Ranger Economic Development Corporation Parts 4A & 4B (REDC 4A & 4B) that after allowing for the anticipated cash flow requirements of the REDC 4A & 4B and giving due consideration to the safety and risk of investment, all available funds shall be invested in conformance with these legal and administrative guidelines, seeking to optimize interest earnings to the maximum extent possible. The investment of these funds shall be handled as its highest public trust.

Investments shall be made in a manner which will provide the maximum security of principal while meeting the daily cash flow needs of the REDC 4A & 4B and conforming to the Public Funds Investment Act (the "Act") Texas Government Code Chapter 2256, which requires each Entity to adopt a written investment policy regarding the investment of its funds and funds under its control. It is the intent of the REDC 4A & 4B to be in complete compliance with local laws and the Act.

Effective cash management is recognized as essential to good fiscal management. Investment interest is a source of revenue to the REDC 4A & 4B funds. The receipt of a market rate of return will be secondary to the requirements for safety and liquidity. The earnings from investment will be used in a manner that best serves the interests of the REDC 4A & 4B.

The purpose of this Policy is to set specific investment policy and strategy guidelines. Direct specific investment parameters for the investment of public funds in Texas are found in the Act. The Public Funds Collateral Act, Chapter 2257, Texas Government Code, specifies collateral requirements for all public Texas funds deposits.

II. SCOPE

This investment policy applies to all financial assets of the REDC 4A & 4B. These funds are accounted for in the Comprehensive Annual Financial Report (CAFR).

In all other investments the assets will be segregated by fund.

III. OBJECTIVES

It is the policy of the REDC 4A & 4B that all funds shall be managed and invested with four primary objectives, listed in order of their priority: safety, liquidity, diversification and yield. Investments are to be chosen in a manner which promotes diversity. To match anticipated cash flow requirements the maximum weighted average maturity (WAM) of the overall portfolio may not exceed six months.

Safety [PFIA 2256.005(b)(2)]

The primary objective of the investment activity is the preservation of capital. Each investment transaction shall be conducted in a manner to avoid capital losses, whether from security defaults, safekeeping, or erosion of market value. Investments in high credit quality securities and decisions based on anticipated cash needs are primary factors in providing safety. The objective will be to mitigate credit and interest rate risk.

- a. Credit Risk and Concentration of Credit Risk – The REDC 4A & 4B will minimize credit risk, the risk of loss due to the failure of the issuer or backer of the investment, and concentration of credit risk, the risk of loss attributed to the magnitude of investment in a single issuer, by:
 - Limiting investments to the safest types of investments.
 - Diversifying the investment portfolio so that potential losses on individual issuers will be minimized.
- b. Interest Rate Risk – the Entity will manage the risk that the interest earnings and the market value of investments in the portfolio will fall due to changes in general interest rates by:
 - Diversifying maturities and staggering purchase dated to minimize the impact of market movements over time.
 - Structuring the investment portfolio so that investments mature to meet cash requirements for ongoing operations, thereby avoiding the need to liquidate investments prior to maturity.

Liquidity [PFIA 2256.005(b)(2)]

The investment portfolio shall be structured to meet all expected obligations in a timely manner. This shall be achieved by matching investment maturities with forecasted cash flow liabilities and maintaining additional liquidity for unexpected liabilities.

Diversification

The portfolio shall be diversified by institution, market sector and maturity as much as possible.

Yield (Optimization of Interest Earnings) [PFIA 2256.005(b)(3)]

The benchmark for the commingled portfolio shall be the comparable six-month period U.S. Treasury Bill, designated for its comparability to the expected average cash flow pattern and the Policy maximum weighted average maturity (WAM) limit of six months. The investment program shall seek to augment returns above this threshold consistent with risk limitations identified and the REDC 4A & 4B prudent investment strategy.

Cash management is the process of managing funds to ensure maximum cash availability and reasonable yield on short-term investments. The REDC 4A & 4B shall strive for a cash management program which includes timely collection of accounts receivable, vendor payments in accordance with invoice terms, and prudent investment of assets.

IV. INVESTMENT STRATEGY

As required by the Public Funds Investment Act, the REDC 4A & 4B shall describe the investment objectives for each fund or group of funds under its control.

The REDC 4A & 4B shall maintain two separate account portfolios for investment purposes which incorporates the specific uses and the unique characteristics of the funds in the portfolio. The investment strategy has as its primary objective assurance that the anticipated liabilities are matched and adequate investment liquidity provided. The REDC 4A & 4B shall pursue a conservative portfolio management strategy based on a buy-and-hold philosophy. This may be accomplished by creating a laddered maturity structure with some extension for yield enhancement. The maximum maturity of any security will be two years, and the maximum dollar weighted average maturity of six months or less will be calculated using the stated final maturity date of each security.

The investment strategy for debt service funds shall have as its primary objective the timely payment of debt service obligations. Successive debt service dates will be fully funded before any investment extensions are made.

V. DELEGATION OF RESPONSIBILITY

No unauthorized person may engage in an investment transaction and all transactions shall be executed as provided under the terms of this Policy and its supporting procedures.

Investment Officer(s)

The REDC 4A & 4B President and Treasurer will be designated as Investment Officers, by City Commission resolution, responsible for investment decisions and activities. The Investment Officer(s) are responsible for creating and maintaining the portfolio in accordance with this Policy, providing timely quarterly reporting to the Commission, and establishing supporting procedures. The REDC 4A & 4B may further contract with a Securities and Exchange Commission (SEC) registered investment adviser for non-discretionary management of the portfolio.

All investment officers shall attend at least ten hours of training, from sources approved by the City Commission, within twelve months of designation as investment officer and shall attend eight hours of training every two successive fiscal years.

Investment Officers shall refrain from personal and business activity that could conflict with proper execution of the investment program, or which could impair their ability to make impartial investment decisions. Disclosure shall be made to the City Manager. An Investment Officer who has a personal business relationship within the two levels of blood or marriage with an organization seeking to sell an investment to the REDC 4A & 4B who meets the parameters established in the Act, shall file a statement disclosing that relationship to the City Commission and the Texas Ethics Commission.

City Commission Responsibilities

The City Commission holds ultimate fiduciary responsibility for the portfolio. It will designate investment officer(s), receive and review quarterly reporting, approve and provide for investment officer training, annually approve broker/dealers, and annually review and adopt the Investment Policy and Strategy.

VI. PRUDENCE AND CONTROLS [PFIA 2256.006]

The standard of prudence to be applied to all REDC 4A & 4B investments shall be the “prudent person” rule, which states:

“Investments shall be made with judgment and care, under circumstances then prevailing, which persons of prudence, discretion and intelligence exercise in the management of their own affairs, not for speculation, but for investment, considering the probable safety of their capital as well as the probable income to be derived.”

In determining whether an investment officer has exercised prudence with respect to an investment decision, the determination shall be made taking into consideration the investment of all funds under the REDC 4A & 4B control over which the officer has responsibility rather than consideration as to the prudence of a single investment.

The Investment Officer, acting in accordance with written procedures and exercising due diligence, shall be responsible but not liable for a specific security credit risk or market price changes, provided that these deviations are reported immediately, and that appropriate action is taken to control adverse developments.

Internal Controls

The Investment Officer is responsible for establishing and maintaining internal controls to reasonably assure that assets are protected from loss, theft, or misuse. The concept of reasonable assurance recognizes that the cost of a control should not exceed the benefits likely to be derived, and the valuation of costs and benefits requires ongoing estimates and judgments by management.

The internal controls shall address the following points at a minimum:

- Control of collusion,
- Separation of transaction authority from accounting and record keeping,
- Safekeeping of owned and pledged securities,
- Clear delegation of authority,
- Written confirmation for all transactions, and
- Review, maintenance and monitoring of security procedures both manual and automated.

Annually the Investment Officer will perform an internal compliance audit to ensure compliance with the requirements of this Policy and the Act. Annually, the City’s external auditor shall review the quarterly reports.

Cash Flow Forecasting

Cash flow forecasting is designed to protect and sustain the cash flow requirements of the REDC 4A & 4B. The Investment Officer will analyze needs and maintain a cash flow plan to monitor and forecast cash positions for investment purposes.

Competitive Bidding

All security transactions will be made on a documented competitive bid basis to assure the REDC 4A & 4B is receiving the best available market rates. When-issued US agency securities should be compared to other securities available in the secondary market to determine competitiveness.

Monitoring Credit Ratings

The Act requires that securities requiring a specific credit rating must be liquidated if the rating falls below the minimum rating. The Investment Officer shall monitor, on no less than a monthly basis, the credit rating on all authorized investments in the portfolio for which the policy requires a credit rating. The rating should be based upon independent information from a nationally recognized rating agency. If any security falls below the minimum rating required by Policy, the Investment Officer shall notify the City of Ranger Mayor, City Manager, and Finance Director of the loss of rating, and liquidation options within two days.

Monitoring FDIC Status for Mergers and Acquisitions

A merger or acquisition of brokered certificates of deposit (CDs) into one bank reduces Federal Deposit Insurance Corporation (FDIC) coverage. The Investment Officer shall monitor, on no less than a weekly basis, the status and ownership of all banks issuing brokered certificate of deposit (CD) securities owned by the REDC 4A & 4B based upon information from the Federal Deposit Insurance Corporation (FDIC) (fdic.gov). If any bank has been acquired or merged with another bank in which brokered certificate of deposits (CDs) are owned by the REDC 4A & 4B, the Investment Officer or Adviser shall immediately liquidate any brokered certificate of deposit (CD) which places the REDC 4A & 4B above the Federal Deposit Insurance Corporation (FDIC) insurance level.

Indemnification

The Investment Officer, acting in accordance with written procedures and exercising due diligence, shall not be held personally responsible for a specific investment's credit risk or market price changes, provided that these deviations are reported immediately, and the appropriate action is taken to control adverse developments.

Limits of Liability

Provides for the defense and indemnification of any REDC 4A & 4B employee who is made a party to any suit or proceeding, other than by actions of the REDC 4A & 4B, or against whom a claim is asserted by reason of their actions taken within the scope of their service as an appointed officer of the REDC 4A & 4B. Such indemnity shall extend to judgments, fines, and amounts paid in settlement, of any such claim, suit, or proceeding, including any appeal thereof.

This protection shall extend only to officers who have acted in good faith and in a manner which they reasonably believe to be in, or not opposed to, the best interest of the REDC 4A & 4B.

Ethics and Conflicts of Interest [PFIA 2256.005(i)]

Officers and employees involved in the investment process shall refrain from personal business activity that could conflict with the proper execution and management of the investment program, or that would impair their ability to make impartial decisions. Employees and Investment Officers

shall disclose any material interests in financial institutions with which they conduct business. They shall further disclose any personal financial/investment positions that could be related to the performance of the investment portfolio.

An Investment Officer of the REDC 4A & 4B who has a personal business relationship with an organization seeking to sell an investment to the REDC 4A & 4B shall file a statement disclosing that personal business interest. An Investment Officer who is related within the second degree by affinity or consanguinity to an individual seeking to sell an investment to the REDC 4A & 4B shall file a statement disclosing that relationship. A statement required under this subsection must be filed with the Texas Ethics Commission and the City Commission.

VII. AUTHORIZED INVESTMENTS

Assets of the REDC 4A & 4B may be invested only in the following instruments as further defined by the Act. If changes are made to the Act they will not be authorized until this Policy is modified and adopted by the City Commission. All investment transactions will be made on a competitive basis.

- A. Obligations of the United States Government, its agencies, and instrumentalities with a maximum stated maturity of two years excluding mortgage-backed securities.
- B. Fully insured or collateralized depository certificates of deposit from banks in Texas, with a maximum maturity of two years insured by the Federal Deposit Insurance Corporation (FDIC), or its successor, or collateralized in accordance with this Policy.
- C. AAA-rated, Texas Local Government Investment Pools which strive to maintain a \$1 net asset value (NAV) AND as defined by the Act and authorized by resolution of the City Commission.
- D. AAA-rated, SEC registered money market mutual funds in compliance with Securities and Exchange Commission (SEC) Rule 2a-7 and striving to maintain a \$1 net asset value.
- E. FDIC insured, brokered certificates of deposit securities from a bank in any US state, delivered versus payment (DVP) to the REDC 4A & 4B safekeeping agent, not to exceed twelve months to maturity. Before purchasing, the Investment Officer must verify the Federal Deposit Insurance Corporation (FDIC) status of the bank on www.fdic.gov to assure that the bank is Federal Deposit Insurance Corporation (FDIC) insured.
- F. Federal Deposit Insurance Corporation (FDIC) insured or collateralized interest bearing and money market accounts from any Federal Deposit Insurance Corporation (FDIC) insured bank in Texas.
- G. Share certificates from credit unions doing business in Texas which are fully insured by the National Credit Union Share Insurance Fund and with a maximum stated maturity of twelve months.
- H. General debt obligations of any US state or political subdivision rated A or better with a stated maturity not to exceed one year.

Delivery versus Payment

All securities shall be purchased on a delivery versus payment (DVP) settlement basis. Funds shall not be released until receipt of the security by the REDC 4A & 4B approved safekeeping depository. The depository shall provide the REDC 4A & 4B with proof of ownership or claim by an original document delivered to the REDC 4A & 4B.

VIII. REPORTING

Quarterly Reporting

The Investment Officers shall prepare and submit a signed quarterly investment report to the City Commission in accordance with the Act giving detail information on each portfolio and bank position and summary information to permit an informed outside reader to evaluate the performance of the investment program. The report will include the following at a minimum:

- A full description of each individual security or bank/pool position held at the end of the reporting period including the amortized book and market value at the beginning and end of the period,
- Unrealized gains or losses (book value minus market value),
- Overall change in market value during the period as a measure of volatility,
- Weighted average yield of the portfolio and its applicable benchmarks,
- Earnings for the period (accrued interest plus accretion minus amortization),
- Allocation analysis of the total portfolio by market sector and maturity, and
- Statement of compliance with the investment portfolio with the Act and the Investment Policy signed by the Investment Officer(s).

Market prices for the calculation of market value will be obtained from independent sources.

IX. FINANCIAL COUNTER-PARTIES

Depository

At least every five years, a banking services depository shall be selected through a competitive request for proposal [application] or bid process in accordance with the Texas Government Code 105. In selecting a depository, the services, cost of services, credit worthiness, earnings potential, and collateralization by the institutions shall be considered. If securities require safekeeping, the RFP/bid will request information on safekeeping services. The depository contract will provide for collateral if balances exceed the Federal Deposit Insurance Corporation (FDIC) insurance balance per tax identification number.

All time and demand deposits in any depository of the REDC 4A & 4B shall be insured or always collateralized in accordance with this Policy.

Other banking institutions, from which the REDC 4A & 4B may purchase certificates of deposit or place interest bearing accounts, will also be designated as a depository for depository/collateral purposes. All depositories will execute a depository agreement and have the Bank's Board or Bank Loan Committee pass a resolution approving the agreement if collateral is required.

Security Broker/Dealers

All brokers/dealers who desire to transact business with the REDC 4A & 4B must supply the following documents to the Investments Officer(s).

- Financial Industry Regulatory Authority (FINRA) certification and CRD #
- Proof of Texas State Securities registration

Each broker/dealer will be sent a copy of the REDC 4A & 4B investment policy. If material changes are made to the policy, the new policy will be sent to the broker/dealer.

Each local government pool must be provided a copy of the REDC 4A & 4B current Investment Policy and certify a review of the Policy stating that the pool has controls in place to assure only Policy approved investments will be sold to the REDC 4A & 4B.

A list of qualified broker/dealers will be reviewed and approved at least annually by the City Commission. In order to perfect the delivery versus payment (DVP) process the banking services depository, or its brokerage subsidiary, will not be used as a broker. A list of authorized brokers and dealers is attached in Exhibit A.

XI. COLLATERAL

Time and Demand Deposits Pledged Collateral

All bank time and demand deposits shall be collateralized above the Federal Deposit Insurance Corporation (FDIC) coverage by pledged collateral. To anticipate market changes and provide a level of security for all funds, collateral will be maintained and monitored by the pledging depository at a market value of 102% of the deposited principal and accrued interest on the deposits. The bank shall monitor and maintain the margins daily.

Collateral pledged to secure deposits shall be held by an independent financial institution outside the holding company of the depository. If required, the collateral agreement with the depository shall be approved by resolution of the Bank Board or Bank Loan Committee. The Custodian or bank shall provide a monthly report of collateral directly to the REDC 4A & 4B.

All collateral shall be subject to inspection and audit by the City or its independent auditors.

Authorized Collateral

Only the following securities are authorized as collateral for time and demand deposits or repurchase agreements:

- A. Federal Deposit Insurance Corporation (FDIC) insurance coverage.
- B. Obligations of the United States, its agencies or instrumentalities, or evidence of indebtedness of the United States guaranteed as to principal and interest including collateralized mortgage obligation (CMO) and mortgage-backed security (MBS) which pass the bank test.
- C. Obligations of any US State, county, city, or other political subdivision of any state having been rated as investment grade (investment rating no less than "A" or its equivalent) by two nationally recognized rating agencies.
- D. Letter of Credit from the Federal Home Loan Bank (FHLB).

Preference will be given to pledged collateral securities.

XI. SAFEKEEPING

All purchased securities are to be cleared to the REDC 4A & 4B safekeeping agent on a delivery versus payment (DVP) basis. All safekeeping arrangements shall be approved by the Investment Officer and an agreement of the terms executed in writing. The independent third-party safekeeping agent shall be required to issue safekeeping receipts to the REDC 4A & 4B listing each specific security, rate, description, maturity, Committee on Uniform Security Identification Procedures (CUSIP) number, and other pertinent information.

XII. INVESTMENT POLICY ADOPTION [PFIA 2256.005(e)]

The REDC 4A & 4B Investment Policy shall be reviewed and adopted by resolution of the City Commission no less than annually. It is the REDC 4A & 4B s intent to comply with state laws and regulations. The REDC 4A & 4B investment policy shall be subject to revisions consistent with changing laws, regulations, and needs of the REDC 4A & 4B. Any changes made to the Policy must be noted in the adopted resolution.

EXHIBIT A. List of Approved Broker/Dealers/Financial Institutions

First Financial Bank

P.O. Box 19

106 W. Main Street

Ranger, TX 76470

L.O.G.I.C.

325 North St. Paul Street, Suite 800

Dallas, TX 75201

TexPool

1001 Texas Ave, Suite 1400

Houston, TX 77002

TexSTAR First Southwest Asset Management, Inc.

325 North St. Paul Street, Suite 800

Dallas, TX 75201

Hilltop Securities, Inc.

Asset Management

717 N. Harwood St., Suite 3400

Dallas, TX 75201

MEMBER CONTACT INFORMATION:

Ranger EDC
Mary Dawson
400 W. Mains Street
Ranger, Texas 76470

EMAIL: doingitallforangel@outlook.com
PHONE: (254) 433-2575

ACCOUNT MANAGER INFORMATION:

Logan Ledesma
Director of Business Development

EMAIL: logan@gslisolutions.com
PHONE: (469) 778-2606 ext. 3

WHAT'S INCLUDED:



- ★ 12- months of email nurture educating 40,000 companies on why they should consider Texas as their next location.
- ★ Choose-Texas.com website - community profile
- ★ Project Coach - works with you to submit on leads
- ★ Monthly reporting - tracking valuable data on contact behavior
- ★ Special Profile on Your Community in the Choose-Texas Magazine Directory
- ★ "Texas Elite Cities for Business" feature
- ★ Exhibition at any of the available trade show - receive leads if unable to attend
- ★ Access to VIP JAM Sessions.
- ★ Two educational webinars on site selection best practices

TOTAL INVESTMENT= \$7,900

If approved and signed by December 17, 2024, GSLI will bonus a free 30-minute Community Connection Podcast (value of \$3,950).

TERMS AND CONDITIONS:

- The company listed above is financially responsible for payment.
- Client acknowledges that a monthly finance charge of 1.5% (18% annually) will be charged on all balances past due 30 days or more.
- Client agrees to pay all reasonable legal fees, court costs, and collection costs incurred as a result of non-payment

I have read and agree to all the terms as stated above.

Authorized Company Representative

Date



We Thank You For Your Contribution In Growing The Economy Of The Great State of Texas!



Global Site Location Industries, LLC
2711 LBJ FREEWAY | SUITE 1032 | DALLAS, TEXAS 75234

Budget Series – Departmental Meetings

The schedule below outlines the proposed Department budget working meetings. These meetings will not require a quorum, and the results will be briefed to the commission as part of regularly scheduled or called meetings specific to the budget.

- 1) June 24, 8-10. Admin meeting. City Secretary, Finance Director, and City Manager
- 2) June 24, 10-12. Municipal courts meeting.
- 3) June 24, 12-2. Police Department.
- 4) June 24, 2-4. Cemetery and Parks.

- 5) June 25, 9-11. Streets.

- 6) July 1, 9-11. Water.
- 7) July 1, 11-1. Wastewater.
- 8) July 1, 1-3. Sanitation.
- 9) July 1, 3-5. Utility Billing.

Other meetings may be scheduled as needed for follow-up or collecting additional information.

The meetings will be held at city hall in the council area.

Budget and Tax Rate Meetings Timeline:

Audit presentation will be added when completed.

Each meeting will require a quorum. The proposed schedule is as follows: (This schedule may be adjusted to meet the needs of the city.)

- Budget workshop: August 11 (TBD)
 - 1st Public Hearing of Proposed Budget: August 19 (4:30 pm)
 - 1st Public Hearing of Proposed Tax Rate: August 19 (5:00 pm)
 - Regular Meeting with first reading of Proposed Budget and Tax Rate Ordinance : Regular Meeting August 25 (5:30 pm)
 - 2nd Public Hearing of Proposed Budget: September 2 (4:30 pm)
 - 2nd Public Hearing of Proposed Tax Rate: September 2 (5:00 pm)
 - Regular Meeting with second and final readings of Proposed Budget and Tax Rate Ordinance : Regular Meeting September 11 (5:30 pm)
-

Ranger City Secretary

From: Mayor
Sent: Friday, June 20, 2025 11:46 AM
To: Ranger City Secretary
Subject: Flood Mitigation Planning Information

Draft Information on Flood Mitigation Planning Discussion. Needed for city planning and future grant requests.

1. Overview and Current Assessment.
 1. Historical flooding reviews
 2. Watershed studies
 3. Flood mapping
 4. Preparedness studies (include engineering requirements)
2. Flood Mitigation Goals.
 1. Reduce or mitigate flood risk to life and property through structural or non-structural projects.
3. Flood Mitigation Projects with Cost Projects.
 1. Low water crossings
 2. Build infrastructure – channels, ditches, ponds, and stormwater pipes.
 3. Storm drain improvements.
 4. Flood walls/levees.
 5. Property or easement acquisition.
 6. Elevation of individual structures.
4. Flood Management Strategies.
 1. Routine flood mitigation maintenance.
 2. City funded.
 3. County flood programs.
 4. Grant programs.
5. Planning Summary.
 1. Outline a proposed one-year initial timeline.
 2. Outline recurring timelines.
 3. Outline coordination and grant goals.

Thank you,

Robert D Butler

Robert Butler
Mayor
City of Ranger, Texas
Email: mayor@rangertx.gov

MEMBER CONTACT INFORMATION:

City of Ranger Economic Development Corporation
 Mary Jane Dawson
 400 W. Main St
 Ranger TX 76470

 EMAIL: rangedc@outlook.com
 PHONE: (254) 433-2575

ACCOUNT MANAGER INFORMATION:

Logan Ledesma
 Community Assessment Director

 EMAIL: logan@gslisolutions.com
 PHONE: (469) 778-2606

WHAT'S INCLUDED:



- ★ 12- months of email nurture educating 40,000 companies on why they should consider Texas as their next location.
- ★ Choose-Texas.com website - community profile
- ★ Project Coach - works with you to submit on leads
- ★ Monthly reporting - tracking valuable data on contact behavior
- ★ Special Profile on Your Community in the Choose-Texas Magazine Directory
- ★ "Texas Elite Cities for Business" feature
- ★ Exhibition at any of the available trade show - receive leads if unable to attend
- ★ Access to VIP JAM Sessions.
- ★ Two educational webinars on site selection best practices

TOTAL INVESTMENT= \$7,500

ARCIT Grant Leverage Statement

By participating in the ARCIT grant program in conjunction with the Choose Texas Network, members may unlock additional funding that can be used beyond membership dues. These funds can be applied toward future economic development initiatives such as video production, marketing materials, trade show support, and other approved promotional activities that align with the goals of community exposure and business attraction.

TERMS AND CONDITIONS:

- The company listed above is financially responsible for payment.
- Client acknowledges that a monthly finance charge of 1.5% (18% annually) will be charged on all balances past due 30 days or more.
- Client agrees to pay all reasonable legal fees, court costs, and collection costs incurred as a result of non-payment.

I have read and agree to all the terms as stated above.

Authorized Company Representative

Date





We Thank You For Your Contribution In Growing The Economy Of The Great State of Texas!



Global Site Location Industries, LLC
2711 LBJ FREEWAY | SUITE 1032 | DALLAS, TEXAS 75234