1st Reading:
2nd Reading: **SPONSOR: CLAUSS**

ORDINANCE NO. ____

BILL NO. 22-44

AN ORDINANCE AUTHORIZING THE MAYOR TO EXECUTE A SECOND AMENDMENT TO THE PURCHASE CONTRACT WITH REGIONAL JUSTICE INFORMATION SERVICE, REJIS COMMISSION FOR VPN CONNECTION RELATED TO THE MUNICIPAL COURT MANAGEMENT SOFTWARE.

WHEREAS, via Ordinance No. 3524, the City entered into a Purchase/Installation/Maintenance Contract with Regional Justice Information Service, REJIS Commission ("REJIS") for municipal court management software (the "Purchase Contract"); and

WHEREAS, via Ordinance No. 4143, the City amended the Purchase Contract to update and more adequately reflect the licenses/products utilized from REJIS; and

WHEREAS, per REJIS, the Municipal Court will need additional (secure) access into the REJIS system tunnel which can be obtained by VPN (Virtual Private Network) access in addition to the Firewall; and

WHEREAS, REJIS provided a City a quote to provide the VPN connection; and

WHEREAS, at the May 5, 2022 Board of Aldermen Committee Meeting, the Police/Municipal Court Committee discussed the VPN quote from REJIS and staff's request to amend the Purchase Contract to provide the same; and

WHEREAS, the Board of Aldermen desires and finds it in the best interest of the City to amend the Purchase Contract to authorize additional (secure) access into the REJIS system tunnel through VPN connection.

NOW, THEREFORE, BE IT ORDAINED BY THE BOARD OF ALDERMEN OF THE CITY OF FENTON, MISSOURI, AS FOLLOWS:

Section 1. The Board of Aldermen hereby authorizes the Mayor to execute on behalf of the City an amendment to the Purchase Contract with REJIS to provide VPN connection substantially in the form of Exhibit 1, attached hereto and incorporated herein by reference. All other provisions of the Purchase Contract shall remain in full force and effect.

Section 2. This ordinance shall be in full force and effect after the date of its passage and approval.

PASSED this 26th day of May 2022.

_____
JOE MAURATH, MAYOR

APPROVED 26th day of May 2022.

_____
JOE MAURATH, MAYOR

ATTEST:

_____
Jane Hungler, City Clerk

Motion to approve. Roll Call vote:
Ayes:
Nays:
Absent:
Abstain:

EXHIBIT 1

SECOND AMENDMENT TO THE CITY OF FENTON, MISSOURI PURCHASE/INSTALLATION/MAINTENANCE CONTRACT

THIS SECOND AMENDMENT TO THE PURCHASE/INSTALLATION/MAINTENANCE CONTRACT (the "Second Amendment") for municipal court management services made and effective as of _____, 2022 by and between the City of Fenton, a Missouri municipal corporation, hereinafter referred to as City, and Regional Justice Information Service, REJIS COMMISSION, located at 4255 West Pine Blvd., St. Louis, Missouri 63108, hereinafter referred to as "SELLER,"

WHEREAS, via Ordinance No. 3524, the City entered into a contract with Seller for municipal court management software (the "Purchase Contract"); and

WHEREAS, via Ordinance No. 4143, the City amended the Purchase Contract to update and more adequately reflect the licenses/products utilized from REJIS (the "First Amendment"); and

WHEREAS, the Municipal Court will need additional (secure) access into the REJIS system tunnel which can be obtained by VPN (Virtual Private Network) access in addition to the Firewall; and

WHEREAS, the parties desire to again amend the Purchase Contract to authorize REJIS to provide the City VPN connections.

WITNESSETH: That the parties hereto, for the considerations hereinafter set forth, agree as follows:

1. The chart contained in Section 1, Municipal Court Management Software, is hereby amended by adding a new third chart as set forth in Exhibit A, attached hereto and incorporated herein by reference.

2. Exhibit A to the Purchase Contract is hereby amended by adding a new Attachment 4 – VPN Connection Terms as set forth in Exhibit B, attached hereto and incorporated herein by reference.

3. The parties hereby reaffirm that all other provisions of the Purchase Contract and First Amendment not specifically amended herein shall remain in full force and effect and shall be deemed incorporated herein and binding on the parties.

4. The Purchase Contract together with the First Amendment and this Second Amendment represents the entire agreement among the parties and Seller agrees that it has not relied on any representations or warranties of the City, oral or written, other than expressly identified in the Purchase Contract, as amended.

IN WITNESS WHEREOF, the parties hereto execute this Second Amendment the day and year first above written.

CITY OF FENTON

By: _____ Date: _____
JOE MAURATH, MAYOR

ATTEST:

_____
CITY CLERK

Regional Justice Information Service, REJIS COMMISSION.

Signature: _____

By: _____

Title: _____

Date: _____

Exhibit A

REJIS
When Data Matters

REJIS Commission
4255 W Pine Blvd
Saint Louis MO
63108
(314) 535-1950

Proposal

#1431

Customer: 30183 Fenton Municipal Court

Prepared for:

Lauren Rabbit, Court Clerk
Fenton Municipal Court
625 New Smizer Mill Road
Fenton, MO 63026

TOTAL

$140.25

Expires: 7/3/2022

Date	Client Service Rep:
4/4/2022	Karen E Karl

Quantity	Item	FRQ	Rate	Amount
1	**WN-0111 VPN Connection - Client Based VPN Connection Main (per user) - 12/13/2021 - 12/31/2022** Please issue soft token.	ANN	$37.25	$37.25
1	**WN-0067 VPN Connection - Client Based VPN Connection Lic (per user)**	OTO	$8.00	$8.00
1	**PRO-378 VPN Connection-Client Based VPN Connection Setup Fee (per user)-1/1/22-12/31/22** WAN/LAN Support - Fixed Fee		$95.00	$95.00

Subtotal	$140.25
Tax (0%)	$0.00
Total	$140.25

Frequency information is provided to assist the customer in determining ongoing costs.

Frequency Codes:
OTO - One Time Only MTH - Monthly QTR - Quarterly SA - Semi Annually ANN - Annually

EXHIBIT B

Attachment 4 – VPN Connection Terms

Proposal Notes:

REJIS will assist the Fenton Municipal Court Clerk with VPN access.

REJIS VPN Policy:

6.2.2 Network Remote Access

Purpose
The purpose of this policy is to define standards for connecting to the REJIS network or to REJIS client sites via the REJIS Internet connection, or a dialup or wireless connection. These standards are designed to minimize the potential exposure to REJIS from damages which may result from unauthorized use of REJIS resources. Damages could include the loss of sensitive or company/client confidential data, intellectual property, damage to public image, or damage to critical REJIS internal systems.

Scope
This policy applies to all REJIS employees, contractors, vendors, clients, and agencies with a REJIS owned or personally owned computing device used to connect to the REJIS Network. This policy applies to remote access connections used to do work on behalf of REJIS, including reading or sending email and viewing Intranet web resources. Remote access implementations that are covered by this policy include, but are not limited to, and Internet VPN connections. The end user is responsible for implementing any restrictions. REJIS Network Services may be contacted to supply suggestions and/or product specifications with current solutions.

Policy
• It is the responsibility of REJIS employees, contractors, vendors and agents with remote access privileges to the REJIS network to ensure their remote access connection is given the same consideration as the user's onsite connection to REJIS.
• Secure remote access must be strictly controlled. VPN connections will be enforced via one time password authentication and the use of Token Server software.
• The token device is the responsibility of the party to whom it is assigned and at no time should the token, ID, password or client configuration be shared with anyone.
• REJIS employees and contractors with remote access privileges must ensure their REJIS owned or personal computer or workstation, which is remotely connected to the REJIS network, is not connected to any other network at the same time.
• Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
• All hosts that are connected to REJIS' internal networks via remote access technologies such as dial in or VPN must meet the following requirements:
o Antivirus The device must use up to date antivirus software. The Antivirus software must be able to automatically update its signatures and must provide on access scanning of data in real time. Online antivirus or onetime antivirus scanning is not adequate and therefore not an acceptable solution.
o Security Patches The device must be up to date with the latest operating system and critical application security patches. Security patches are unique to the version of operating system or application installed on a given device. It is the responsibility of the end user to ensure their security patches are kept current. This applies to user-owned and REJIS supplied computers that do not regularly connect to the REJIS network via a local LAN connection.

o Firewall The computer that is utilized to connect to REJIS is required to be protected by a firewall type device at all times. This device must be able to block incoming connections that are not specifically allowed by the user. The use of address translation for Internet connections is also a required capability. Software type firewalls does not provide adequate protection since they can easily be terminated and does not provide for address translation.

• If a wireless access point is utilized in the process of connecting the computer to an Internet connection, it is the end user's responsibility to ensure that the wireless connection is secured to the point that it is not easily accessible by unknown or unauthorized computers. Security methods should, include but are not limited to Encryption, MAC address filtering, Unique SSID, do not broadcast SSID, etc.
• When access to the REJIS Network is successful, the user shall be presented with a banner notifying them of the restricted use of the network.

Monitoring
Authentication is monitored by the authentication mechanism that is the Token Server software in place. REJIS monitors REJIS owned computers by utilizing a centralized management and reporting platform. With current limitations in monitoring technology and posturing of devices, it becomes the VPN user's responsibility to monitor the status of security patches and configurations of user owned equipment.
Connections to the REJIS network that are suspected as being malicious will be immediately disconnected and will remain blocked until further investigation can be completed.

Supporting Documentation
To report lost or stolen mobile computing devices or authentication token, call the REJIS Help Desk at (314) 535-9497 or Computer Operations at (314) 633-0300.

Compliance
All employees, clients, contractors, vendors and visitors are expected to follow the REJIS IT Policies specific to their relationship with REJIS (employee, client, vendor/contractor, or visitor) as identified within each REJIS IT Policy. Compliance issues will be handled as stated in 1.1.4 Compliance Policy.

General Notes:

- Prices for REJIS software and services are valid for 90 days from the proposal date.
- If quotes from vendors for hardware/software requests are part of this proposal, the final price may fluctuate and will be adjusted accordingly during the billing process.
- Labor identified as "Fixed Fee" will be billed at the quoted rate. Work not identified as fixed fee will be billed the actual number of hours.
- All agencies that access REJIS services must meet anti virus and NCIC/CJIS security requirements.
- For custom code developed by REJIS, the following statement applies. "As implied under the REJIS operating charter to support regional government entities, REJIS will retain ownership of the developed software and will make it available to any/all regional government entity(ies) that can utilize this capability. REJIS retains title to all copyrights, trade secrets, and intellectual property rights to the software. The Agency agrees that the software shall not be disclosed, given, sold to, or used by another party without written approval of REJIS".
- Please contact your Client Services Representative with any questions.