

December 5th, 2024

Ms. Deb McIsaac  
City of Baltic  
130 St. Olaf Avenue  
Baltic, SD 57003

Dear Deb:

Per our recent presentation at your location, Workplace IT Management/Direct Technologies is pleased to submit this letter proposing a transition to our *True Flat Rate (TFR)* managed IT platform. We've appreciated our relationship over the years supporting your IT infrastructure and applications. We believe the Workplace IT Management *True Flat Rate* program that has evolved over decades is the ideal solution for your future IT operations. We are confident that the direction and support inherent in the *TFR* program will result in appreciable stability, security, technical and financial advantages for the City of Baltic.

As you evaluate our proposal, we would ask you carefully consider the following:

- ***Our Experience*** – Founded in 1997 in downtown Sioux Falls, Workplace has grown to a local staff of nearly 50 full-time and part-time Staff, Systems Administrators and Engineers. Workplace employs the deepest bench of local skills and is among the larger IT management firms regionally. Our business and technology leadership team has decades of experience in information technology services in virtually every industry including non-profits, manufacturing, financial services, healthcare, and the legal industry. Our fully staffed local “direct to technician” Help Desk operates out of our office location in Sioux Falls, SD and provide assistance during normal business hours as well as on nights and weekends. In late 2022, our company was acquired by Direct Companies but continues to operate as Workplace IT Management name and most critically with our biggest differentiator – our company culture and the certainty of our *True Flat Rate (TFR)* support platform. This acquisition will allow us to continue to grow to new operating levels, and the combined organization allows us to expand our product and service offering.
- ***Our Philosophy*** – Originally founded as a “pure play” IT Services company our mission is helping organizations develop and maintain secure and stable IT operations. Workplace is not a traditional computer dealership or hardware reseller. We view *all client IT infrastructure* – from ISP services to hardware, peripherals, and applications – as an ecosystem that our team is responsible for keeping in balance, available, and secure.

Our local dedicated Account Managers, Lead Architect and Project Management resources ensure projects are executed successfully, and we include unlimited services to advise on future infrastructure or application investments as part of our flat monthly fee. Combined with our True Flat Rate approach, this ensures Workplace's wholistic view of the entire IT ecosystem is not limited and eliminates parochialism where responsibility for different segments varies based on who originally sold the hardware. Objectivity throughout this

process has been a hallmark of our services and has been the basis of our business model for over 20 years.

### **Current Technical Environment Supported by Direct Technologies**

We understand the City of Baltic technical environment consists of the following:

- There are multiple server instances on the network.
- There are 5 workstations on the network. One being the 3cx box.
- There is a Fortinet Firewall in place today.
- The internet connection is provided by the local vendor.

City of Baltic currently has an agreement with Direct Technologies. Direct Technologies is converting existing clients from the T&M model of service to a flat-rate all-inclusive model. The new flat rate agreement will be provided by Direct Companies/Workplace IT Management.

### **Objectives of Upgrading to the *True Flat Rate Platform*:**

The core objectives of the choosing the TFR management arrangement are to:

- Fully confirm and accurately document the current technology environment, scope of services and support delivery mechanisms through a structured cross-boarding process.
- Provide end users with a responsive, reliable, predictable, and professional support experience via the Workplace “direct-to-technician” IT Help Desk.
- Ensure availability and stability of the network backbone by monitoring all infrastructure 24/7/365, addressing all operational and security alerts/exceptions, and performing structured proactive network operations processes.
- Meet a variety of objectives to maintain a secure, stable, and reliable network through a standardized, diligent and layered approach to:

<b>Prevention</b> – Avoiding downtime and fight attempts by malicious parties to create IT security incidents.	<b>Restoral</b> – Return all data and information systems to normal following a downtime, outage, or security incident.
<b>Detection</b> – Identify real or potential IT operational risks and security threats as quickly as possible.	<b>Response</b> – Develop, document, and execute the most appropriate internal and external issue response activities when handling a security or network operations issue.
<b>Containment</b> – Minimize the impact of any IT security incident or network downtime or disruption.	

- Establish IT support as a predictable, known, and fixed business expense with certainty and continuity in resource availability.
- Provide effective direction on future systems evolution, investments, and strategy.

Flat-Rate Transition On-Boarding Process:

- Finalize Contract and Establish Billing & Service Dates – Upon execution of this agreement, we will identify a master schedule with specific milestone dates for cross-boarding, platform installation, employee orientation and ultimately changes to billing processes.
- Secure & Review Existing Documentation – Workplace resources will start by securing and reviewing all existing Technology documentation to build it into the Workplace documentation framework. Direct and Workplace staff will collaborate to ensure the documentation is accurate and complete.
- Confirmation Audit of Workstations & Network Assets – In order to build the support agreement that clearly defines the scope of covered assets and environments, we will complete an accurate and current inventory of all network assets including workstations, network equipment, cloud environments and peripheral devices. During the transition cross-boarding process Workplace will audit all client assets in detail, label and enter each device / configuration into the Workplace management database, including all servers, network equipment configurations and each workstation you intend to have us manage. We will also be auditing and evaluating all services and network connectivity to support future troubleshooting.
- Deploy Workplace Toolset & Management Platform – In this work segment we will fully deploy the current standard set of monitoring and management tools that make up the *TFR* platform. These tools perform include remote access utilities as well as endpoint security applications, and tools that perform regular scans of the client environment to ensure there are not indicators of compromise or unauthorized changes to the environment and alert our team if we see exceptions. This will standardize your environment and locations on the full Workplace toolset that provides everything from remote access to alerts at our Network Operations Center, as well as administrative reporting utilities.
- Establish Administrative Settings & Automated Notifications – During this segment, we will establish access for Workplace to all necessary client applications and devices. We will also activate and update all on-site notifications for backup and virus activities to report back to our Help Desk alert intake processes. During this segment we will test the deployment of our network monitoring probes across devices to ensure they are reporting properly to our NOC and Security Desk.
- Diagram the As-is Network - Using our network diagramming tools, we will generate a set of current network diagrams created with information from our onboarding activities and generate a detailed document that shows the devices on the network, topology, and IP address scheme.
- Establish Operations Center & Help Desk Procedures – After the additional tools installed and documentation. The Technical Concierge and our Customer Experience Lead will conduct an internal training session for our support staff to educate the team on the overall client environment and orient them to the organization. In addition, the team will establish a

custom set of checklists and internal reference documents that will allow us to begin our remote management program for your organization, a process we call the daily Network Validation Process (NVP) and Security Validation Process (SVP).

- Develop End User Orientation –During this segment of on boarding our Customer Experience Lead and Technical Concierge will provide a number of deliverables and information to be distributed across the client organization that will instruct all staff on how to engage our IT support resources. Mousepads with specific numbers to directly contact our support team are provided to each managed system, along with direction on when and how to best engage our team based on the specific need.
- Develop Customer Service Dashboard – A final Must Have on-boarding segment is to develop and roll-out a client dashboard that provides a variety of different data elements for use by client POC or other staff. The Dashboard includes a number of real-time and near-real-time statistics including:
  - Tickets Opened, Closed & Opened/Closed History
  - Recent Tickets Opened History by User
  - Patch Status
  - Customer Satisfaction Totals
  - Customer Satisfaction Feedback Comments Summary

Upon completion of this onboarding scope of work, Workplace will be well-positioned to deliver the transitioned contract into a Flat-Rate service.

IT Management Scope of Services:

The following table provides a detailed list of our scope of services:

<b>Support Segment</b>	<b>Included Items</b>	<b>Excluded Items</b>
Workplace Internal Security and Stability Assurance <b>Processes</b>	<ul style="list-style-type: none"> <li>▪ Daily Active Directory scans to identify known HW/SW vulnerabilities (e.g., default passwords, missing patches, etc.)</li> <li>▪ Daily indicator of potential compromise scan to identify exceptions / changes that may indicate compromise (e.g., abnormal login activity, rogue software installation, account add/delete activity, new device discovery, etc.)</li> <li>▪ Daily report of critical / suspicions changes in O365 environment, user account setup, O/S, DNS activity, etc.</li> <li>▪ Trend XDR Cloud cross-client and cross-platform alerts of suspicious or malicious activity</li> </ul>	

<b>Support Segment</b>	<b>Included Items</b>	<b>Excluded Items</b>
	<ul style="list-style-type: none"> <li>▪ Receive, resolve, and thoroughly document exceptions via Workplace Security Desk</li> </ul>	
<b>Backbone Devices &amp; Connectivity Management</b>	<ul style="list-style-type: none"> <li>▪ 24/7/365 monitoring of critical devices with real-time alerting:               <ul style="list-style-type: none"> <li>○ Internet Connection</li> <li>○ Firewalls</li> <li>○ Switches</li> <li>○ Wireless equipment</li> <li>○ Servers</li> </ul> </li> <li>▪ Installation of service packs and patches on all PCs / laptops / surfaces</li> <li>▪ Add, change, and delete users as necessary – domains &amp; Office 365</li> <li>▪ Implement user permissions &amp; access</li> <li>▪ Reset passwords when needed</li> <li>▪ Installation of compatible software products</li> <li>▪ Replace faulty / failed hardware</li> <li>▪ Monitor / support VoIP applications</li> <li>▪ Monitoring of backup as scheduled</li> <li>▪ Updating virus signatures</li> <li>▪ Managing malware containment software</li> <li>▪ Monitor user licensing</li> <li>▪ Monitor &amp; report on available disk space / storage utilized on any drives</li> <li>▪ Monitor &amp; report on processor utilization</li> <li>▪ Troubleshoot switches as necessary</li> <li>▪ Respond to any new issues</li> <li>▪ Assist with evaluating 3<sup>rd</sup> party products and services</li> <li>▪ Hardware replacement planning</li> </ul>	<ul style="list-style-type: none"> <li>▪ Software license costs</li> <li>▪ Software upgrade costs</li> <li>▪ Hardware replacement costs</li> <li>▪ Hardware upgrade costs</li> <li>▪ Application-specific software support (e.g., Custom Databases, Excel user support)</li> <li>▪ Installation or repair of data cabling</li> <li>▪ Web site maintenance</li> </ul>
<b>End User Support</b>	<ul style="list-style-type: none"> <li>▪ Unlimited end user access to help desk</li> <li>▪ Structured evaluation, release and installation of service packs and patches on all Windows systems – on-site and remote</li> <li>▪ Installation of compatible software products</li> <li>▪ Replace faulty hardware</li> <li>▪ Updating virus signatures</li> <li>▪ Administer malware containment products</li> <li>▪ Installation &amp; configuration of all network equipment &amp; peripherals</li> <li>▪ Respond to any new issues that may arise</li> <li>▪ Troubleshooting / resolve printer issues</li> <li>▪ Troubleshoot / resolve application access issues</li> <li>▪ Troubleshoot / resolve e-mail issues</li> <li>▪ 3<sup>rd</sup> party escalation</li> </ul>	<ul style="list-style-type: none"> <li>▪ Software license costs</li> <li>▪ Software upgrade costs</li> <li>▪ Hardware/printer replacement costs</li> <li>▪ Hardware/printer upgrade costs</li> <li>▪ Application-specific software support (e.g., Industry Applications, Excel user support)</li> <li>▪ Any Windows OS prior to Windows 8</li> <li>▪ Any Unix device</li> </ul>

<b>Support Segment</b>	<b>Included Items</b>	<b>Excluded Items</b>
<b>Product Standardization</b> - <u>Mandatory</u> :	Delivery and persistent administration of: <ul style="list-style-type: none"> <li>▪ Trend XDR Anti-virus</li> <li>▪ Cisco Umbrella Anti-malware</li> <li>▪ Anti-SPAM Solution (varies based on e-mail environment):</li> <li>▪ On-site and off-site data backup (varies based on solution)</li> <li>▪ Firewall management and hardening</li> </ul>	
<b>Product Standardization</b> - <u>Optional</u> :	Delivery and persistent administration of: <ul style="list-style-type: none"> <li>▪ KnowBe4 Security training, testing and employee learning management</li> <li>▪ Perch SIEM/SOC Services</li> <li>▪ Multi-Factor Authentication</li> </ul>	
<b>On-site Staffing Arrangement</b> - <u>Optional</u>	Optional on-site staffing resource to: <ul style="list-style-type: none"> <li>▪ Provide on-site dedicated IT staff.</li> <li>▪ Staff would be on Workplace payroll.</li> <li>▪ Staff would work on City of Baltic issues first/monitor/first line of defense.</li> <li>▪ Resource embedded to live in and understand the client culture.</li> </ul>	

**Management Service Provider Fees & Expenses:**

Pricing for our **true flat-rate**, on-going management services is as follows:

One Time Professional Services Fees:

Item	Quantity	Rate	Total	Comments
One-time On-site Onboarding Fee	1	\$0	\$0	Existing customer – cross-boarding fee waived.
<b>Total One-time Fees:</b>			<b>\$0</b>	

**MAIN OFFICE CORE NETWORK - Monthly Professional Services Fees – REQUIRED Products & Services:**

\*Note an audit will take place at the end of on-boarding for a final number and items will be adjusted if necessary once confirmed.

Item	Quantity	Rate	Total	Comments
Backbone Management				
Server and Network Backbone Management Fee <ul style="list-style-type: none"> <li>• Switches / Wireless equipment</li> <li>• Printers &amp; peripherals</li> <li>• Site fee</li> </ul>	1	\$400	\$400	
Server Identity Management Only	1	\$100	\$100	
Cyber Operations Platform Services (COPS) Fee <ul style="list-style-type: none"> <li>• Tier 1 Client Environment</li> </ul>	1	\$80	\$80	
Cloud Complexity Management Fee <ul style="list-style-type: none"> <li>• Tier 1 Client Environment</li> </ul>	1	\$80	\$80	
End User Support				
Unlimited <b>Dedicated</b> End User Workstation & Peripheral Support – On-site and Remote	4	\$52.75	\$211.00	<ul style="list-style-type: none"> <li>• An onboarding audit will be conducted to confirm exact number</li> </ul>
Workplace Standard Products - Mandatory				

<b>Item</b>	<b>Quantity</b>	<b>Rate</b>	<b>Total</b>	<b>Comments</b>
Endpoint Protection Suite - Trend Micro XDR Anti-Virus & Cisco Umbrella Anti-Malware	7	\$8.80	\$70.40	
Server Backup Software License – Acronis Physical Server	2	\$75	\$150	
Server Backup – Offsite Data	500GB	\$.15 per GB per month	\$75	
Security Awareness Training & Testing	15	\$2.50	\$37.50	Includes council members (optional)
Managed VOIP Services	8	\$5.99	\$47.92	Phone management
3 <sup>rd</sup> party license (Microsoft 365)		\$140.00	\$140.00	This is 3 <sup>rd</sup> party licenses based on last month licenses
<b>Total Projected Monthly Recurring Flat Rate Fees –</b>			<b>\$1,491.82</b>	

### **Liability Limitation Statement**

By signing this agreement, Workplace and Client acknowledge and agree that Workplace’s services outlined in this agreement represent Workplace’s best practices management program. The terms of this agreement do not create an express or implied warranty with respect to the services provided by Workplace. Client understands and agrees that system downtime, virus infection, business interruption, connection to the public Internet, including but not limited to virus authors, unprotected outside systems, hackers, Internet outages and data loss/corruption,

among other risks, are inherent in Client's decision to store and manage its valuable information in electronic form (herein "Inherent Risks"). Client agrees to indemnify and hold Workplace harmless for any damages attributable to such Inherent Risks.

Workplace's obligation is limited to performing proactive system maintenance procedures, which are standard in Workplace's industry, to minimize inherent risks. In no event shall Workplace be liable for any indirect, incidental, special or consequential damages of any kind or nature whatsoever, including without limitation, loss of profits or other economic loss, arising from or relating to this Agreement or any such Inherent Risks. Workplace's total cumulative liability in connection with this Agreement, whether in contract or tort or otherwise, will not exceed the aggregate amount paid by client to Workplace hereunder during the twelve (12) month period immediately preceding any such claim.

### **Assumptions & Important Considerations**

This proposal is submitted based on the following assumptions:

- ✓ Arrangement to begin upon completion of setup scope of work and execution of this document.
- ✓ Optional products and solutions may require further auditing and inventory information of client network. Workplace can provide detailed pricing upon completion of on-boarding activities.
- ✓ Existing staff will work to help secure all access necessary information including administrative ID's and passwords for applications, servers, etc. per our previous outline.
- ✓ On occasion our audit process will reveal existing viruses on workstations or file servers that can be time-consuming to eliminate. While none is anticipated, any up-front existing virus 'cleanup' work that is required will be billed as time and materials at a rate of \$185/hour.
- ✓ City of Baltic will designate a client liaison primarily to help prioritize activities.
- ✓ Service Level Expectations:
  - Workplace Help Desk will be staffed from 8:00 a.m. to 5:00 p.m. Any user can call the Workplace Help Desk, providing they have their unique workstation ID.
  - Helpdesk voicemail box will be provided for extended coverage on nights and weekends. Voicemails will designate emergency vs. next business day calls. Workplace commits to a 2-hour response.
- ✓ Monthly services will be billed in advance, e.g., July Management Fees are billed on June 30th.
- ✓ This arrangement provides no support for development or maintenance of any City of Baltic web sites, application software or other custom-developed software or interfaces. Workplace works with programming businesses locally and can provide recommendations if needed.
- ✓ Acceptance of this agreement should not be assumed to allow termination of any other existing 3<sup>rd</sup> party maintenance agreement, for example virus signature subscriptions or Industry Application maintenance fees.
- ✓ This is to be a 12-month agreement. If not renewed by the end of the 12 months, the contract will proceed on a month-to-month term.
- ✓ 45 day written notice is required for early termination of this agreement.
- ✓ As part of this agreement, Workplace IT Management provides IT support services and administration to support routine daily business activities. Workplace does not provide, have the tools or training to support or provide computer forensics services that may be part of any

litigation activities, digital investigation, or any other computer forensic work. As such, all computer forensic activities are NOT INCLUDED as part of this proposal. We understand that Workplace staff may be required to comment on our normal procedures, activities, and provide information from our documentation systems and will do so as part of this agreement. However, Workplace reserves the right to refuse and/or defer specific requests for assistance with any forensics activity/activities that we are not qualified to perform, or we feel presents risk to our client, unwarranted involvement of our company or in any way potentially jeopardizes the legal proceedings at hand. Client agrees to fully disclose that specific requests are related to current or potential litigation in all cases.

- ✓ From time to time, we are asked to dispose of retired systems on behalf of our clients. As part of this agreement, Workplace will remove systems from your location and contract with SEAM to properly destroy the hard drive to ensure data is destroyed. We do not provide any logging or reporting related to system destruction as part of this standard disposal process. If compliance or other regulatory obligations require your organization to provide reporting on system destruction or you desire to have full serial number level disposition, we recommend you work directly with SEAM. Disposal charges may apply and are the client's responsibility.

We appreciate your careful consideration of our proposal. We believe that by accepting this proposal you are retaining the highest quality network support professionals available, in an innovative and cost-effective arrangement. Please feel free to contact me at 605-251-8696 with any questions or email me at [jhenderson@workplace-it.com](mailto:jhenderson@workplace-it.com).

Regards,

Workplace IT Management

\* \* \* \* \*

Proposal Accepted:

\_\_\_\_\_  
City of Baltic

\_\_\_\_\_  
Date

\_\_\_\_\_  
Workplace IT Management

\_\_\_\_\_  
Date