CITY OF BROADVIEW HEIGHTS
RESOLUTION NO. 2025-36

INTRODUCED BY MAYOR AND ENTIRE COUNCIL

A RESOLUTION AUTHORIZING THE MAYOR TO ENTER INTO AN AGREEMENT BETWEEN THE CITY OF BROADVIEW HEIGHTS AND BPI INFORMATION SERVICE FOR MULTI-FACTOR AUTHENTICATION AND CYBER SECURITY TRAINING IN THE CITY OF BROADVIEW HEIGHTS AND DECLARING AN EMERGENCY

WHEREAS, the City Council has determined that it is in the best interest of the City to enter into an agreement between the City of Broadview Heights and BPI Information Service for Multi-Factor Authentication and Cyber Security Training in the City of Broadview Heights.

NOW, THEREFORE, BE IT RESOLVED BY THE COUNCIL OF THE CITY OF BROADVIEW HEIGHTS, COUNTY OF CUYAHOGA AND STATE OF OHIO:

SECTION 1. The Mayor is hereby and herein authorized to enter into an agreement between the City of Broadview Heights and BPI Information Service for Multi-Factor Authentication and Cyber Security Training in the City of Broadview Heights as delineated in Exhibit "A" attached hereto and made a part hereof as if fully rewritten.

SECTION 2. This Resolution is hereby declared to be an emergency measure necessary for the immediate preservation of the public health, peace, safety and welfare for the reason stated in the Preamble hereof, and provided it receives the affirmative vote of five (5) or more of the members of Council and signature of the Mayor; otherwise it shall take effect and be in force from and after the earliest period allowed by law.

Passed and Adopted by the Council on this 24th day of February, 2025

Robert Boldt, President of Council

February 24, 2025

Samuel J. Alai, Mayor Date

Robin Parsons February 24, 2025

Attest: Robin Parsons, Clerk of Council Date

City of Broadview Heights
Interoffice Memorandum

To: Members of Council
From: David A. Pfaff, Finance Director
Date: February 13, 2025
Re: BPI Information Service (BPI) – Multi-Factor Authentication & Cyber Security Training

Our Cyber Liability Insurance carrier requires us to have Multi-Factor Authentication (MFA) and Cyber Security training as part of us obtaining coverage. These services are provided by BPI Information Systems.

Our current agreement for these services expires in February. I recommend that we enter into the attached two-year renewal agreement for these services at a cost of $755 per month, which represents a $60/month increase over our current rate.

The cost for MFA will remain $400 per month or $4,800 annually based on 100 users. We can add additional users if needed at a cost of $20 per month for each additional 5 users. The cost for Cyber Security Training will increase $60 per month to $355 per month or $4,260 annually. We can add additional users if needed at a cost of $13 per month for each additional 5 users.

This two-year agreement will now run concurrent with our Managed Services Agreement and expire at the same time.

Please let me know if you have any questions.

cc: Sam Alai, Mayor

BPI INFORMATION SYSTEMS
MANAGED SERVICES STANDALONE OPTIONS SCHEDULE

This BPI Managed Services Standalone Options Schedule (this "**Schedule**") is entered into as of the Schedule Effective Date set forth below by and between BPI Information Systems ("**BPI**") and City of Broadview Heights ("**Customer**"). This Schedule is subject to the terms of the Master Services Agreement between BPI and Customer dated 01/30/2023 (the "**Agreement**"). Capitalized terms used in this Schedule and not otherwise defined have the meaning given to them in the Agreement.

1. Customer Information

Site Location(s):	9543 Broadview Road, Building 7, Broadview Heights, OH. 44147		
Primary Customer Contact:	Ted Bruzdzinski	**Secondary Customer Contact:**	Dave Pfaff
Emergency Phone #:	440-584-8548	Emergency Phone #:	330-338-4056

2. Summary

Schedule Effective Date	Commencement Date	P.O. Number	Setup Fee (one time)	Monthly Price
02/13/2025	03/1/2025		N/A - Renewal	$755.00

3. Term of Schedule

Service under this Schedule shall begin on the Commencement Date set forth above, with the first month of Service pro-rated until month end, and continue for □ one (1) year ☒ two (2) years or □ three (3) years after the first partial month of Service.

4. Enterprise Cloud (if checked below). Customer-specific options are set forth in Exhibit B, and additional terms are set forth in Exhibit C as applicable.

□ **Enterprise Cloud**: Enterprise Cloud is a cloud hosting service consisting of hosted and maintained equipment which provides physically dedicated and virtualized compute resources with dedicated storage, including as applicable managed external hosting of servers (colocation), firewall security, SSL VPN security, third-party software licensing, internet access services, and data protection.

5. Security and Other Services. Please check the Services to be provided below:

□ **Email Security Advanced Threat Protection:** A hosted email security service that blocks unwanted email before it reaches the corporate network and identifies sources of spam, along with outbound anti-virus scanning.

□ **Email Archiving**: Services provide complete, searchable email archive accessed any time anywhere on the internet, email continuity during local outages, rapid retrieval of local deleted emails and a searchable knowledgebase of a company's email.

□ **Email Encryption**: Provides email encryption for compliance and the protection of sensitive information.

□ **Cloud Delivered Threat Protection**: This network security and threat intelligence Service blocks malware, botnets and phishing from Customer's network. It detects and contains advanced attacks before they can cause damage, by using big data analytics and machine learning to automate protection against known and emergent threats. It also gives Customer a more complete picture of real-time network usage, so that Customer can have compliance visibility and controls with granular Web filtering and protect against threats that firewalls and antivirus tools miss.

□ **Endpoint Security Protection**: Protection against malware and viruses infiltrating the network through devices connected to the network, including laptops and desktops. Includes up to 2 hours of remote remediation support per incident for incidents that are timely reported to BPI.

□ **Advanced Endpoint Security Protection with XDR**: Premier managed enterprise level cybersecurity offering with real-time 24x7 Security Operations Center (SOC) monitoring using AI detection and prevention for optimized performance and security. Includes up to 2 hours of remote remediation support per incident for incidents that are timely reported to BPI.

☒ **Multi-Factor Authentication**: Protect local logins, on premise, and cloud-based applications with MFA. Common applications include M365, VPNs, VDI, RDP, SSH. Includes up to 2 hours of remote remediation support per incident for incidents that are timely reported to BPI.

□ **Network Security Service**: External vulnerability scans and reports are provided monthly. Dark Web remote monitoring of your organization's domain for stolen email addresses, passwords and includes up to 2 hours of remote remediation support per incident for incidents that are timely reported to BPI. NOTE: Use of this Service by more than 500 users requires the written approval of BPI, and will be subject to additional fees. Monthly internal vulnerability scans are available for an additional fee.

☐ **Security Information and Event Management**: 24/7 BPI SIEM solution delivering high-level threat protection. Includes endpoint detection and response (EDR); 400 days of log archives and compliance reporting for PCI, GDPR, HIPAA and NIST 800-171. Includes up to 2 hours of remote remediation support per incident for incidents that are timely reported to BPI.

☐ **Zero Trust Application Control**: Application whitelisting and fencing protects you, your customers, and your data from exploited files and applications by reducing attack surface area. Only explicitly approved programs, installers, and applications are allowed to run. Storage control sets modifiable standards for uploading / exporting and unambiguously provides audit history. Includes up to 2 hours of remote remediation support per incident for incidents that are timely reported to BPI.

☐ **Cloud to Cloud Backup**: Microsoft 365 and Google Workspace backups that are restorable and protected in the cloud. Includes up to 2 hours of remote remediation support per incident for incidents that are timely reported to BPI.

☒ **Security Awareness Training:** Using tools provided by KnowBe4, this service helps your users understand the mechanisms of spam, phishing, malware and social engineering. BPI will assist in setting up a campaign that provides baseline testing, monthly fake phishing emails with result based training recommendations, quarterly user web-based training, and management reporting.

☐ **Desktop Management:** Provides unlimited remote desktop help desk support, Microsoft patch management as requested and hosted email security (spam, anti-virus) if available. Approved desktop software for helpdesk includes current versions of Microsoft OS, and Microsoft Office. Other desktop solutions may be approved if agreed in writing by an authorized BPI officer. These services are provided using remote control technology/phone.

☐ **Password Management:** Using a solution powered by Password Boss, this service helps simplify and protect a large security threat – poor password security. Includes up to 2 hours of remote remediation support per incident for incidents that are timely reported to BPI.

☐ **Patch Management 3rd Party Applications:** Provides patch management for supported 3rd party applications as requested including (as of the date of this Schedule) Chrome, Firefox, Avast, Malwarebytes, Dropbox, Google Drive, PDFCreator, and OpenOffice. Not all applications are supported; Customer should verify all requests with BPI.

☐ **Firewall Patch Management:** Provides monthly patch management for supported firewalls and HA pair firewalls including Fortinet, SonicWall, and others. Not all firewalls are supported; Customer should verify all requests with BPI. Includes up to 2 hours of remote remediation support per incident for incidents that are timely reported to BPI.

☐ **Microsoft Cloud**: Products such as Microsoft 365 and Azure are available. BPI license management is included. Exhibit D contains additional terms regarding use of Microsoft software and online services.

☐ **Xerox Printer Management**: Support Services for Xerox printers. **Additional terms and fees for Xerox printer management Services are set forth in Exhibit E.**

6. **Price Worksheet and Payment Terms.**

(a) The Price Worksheet, attached hereto as Exhibit A, contains additional detail regarding the calculation of the fees set forth above. Onetime SP Setup fees are fees associated with a third party BPI service partner. SP Setup Fees do not include any time for BPI installation and support services.
(b) At the Schedule Effective Date, BPI will invoice and collect payment for the first monthly fee and all one-time fees associated with this Schedule. This payment must be received before any Service under this Schedule can be scheduled or delivered.
(c) Either party may request from time to time a "true-up" adjustment to the number of units covered by this Schedule. However, in no event will the true-up numbers be less than listed on this Schedule at the time of signing. Applicable units include, depending on the specific Service, number of servers/network devices; number of PC's/notebooks; IP addresses; e-mail user accounts, and locations. Any price changes from the true-up will begin on the start of the next month.

7. **Technical Requirements.** In order for Customer's existing environment to qualify for the Services under this Schedule, the following requirements must be met:

(a) All servers with Microsoft Windows operating systems must be running Windows 2012 Server or later and have all of the latest Microsoft Service Packs and Critical Updates installed.
(b) All desktop PC's and notebooks/laptops must be running Windows 10 or later and have all of the latest Microsoft Service Packs and Critical Updates installed.
(c) All server and desktop software must be genuine, licensed, and vendor-supported
(d) The environment must have a currently licensed, up-to-date and vendor-supported:
    (i) server-based anti-virus solution protecting all servers, desktops, notebooks/laptops, and email;
    (ii) server-based backup solution; and
    (iii) hardware firewall between the internal network and the internet.
(e) Any wireless data traffic in the environment must be secured with a minimum of 128-bit data encryption.

BPI may update and/or supplement the above technical requirements from time to time upon notice to Customer

BPI may identify Customer's failure to meet the above technical requirements and other issues with Customer's technical infrastructure, and recommend changes/fixes. BPI recommendations shall be reviewed by Customer in a timely basis with serious consideration given. If Customer does not comply with BPI's recommendations, the Services may be adversely affected and additional fees may apply. In addition, BPI may terminate this Schedule after a 60 day written non-compliant notification to Customer if Customer does not implement recommendations within such time period.

Services and fees required to bring Customer's environment up to the foregoing minimum standards are not included in this Schedule.

8. **Managed Services Customer Requirements.** Customer will at its own cost:

(a) Maintain sufficient bandwidth and a high-speed Internet connection at the Customer site(s) to support the Services. If this is not maintained, BPI will not be obligated to provide the Services and/or may increase fees for the Services to reflect the higher cost of supporting Customer.
(b) Unless specifically agreed herein, maintain, manage, and keep records of valid licenses, warranties and/or support contracts for hardware, operating software and application software used in its network and systems with respective third-party vendors.
(c) Notify BPI immediately of any issues needing Service.
(d) Notify BPI upon the removal of a managed device from the network so the BPI's remote management and monitoring systems can be updated.
(e) Provide necessary supplies when deemed necessary, including but not limited to printer consumables, backup tape media, and tape drive cleaning supplies.
(f) Maintain Customer site conditions within the environmental range of all Customer system devices and media as specified by the manufacturer.
(g) Include (except to the extent that Customer wishes to discuss certain aspects of BPI services without BPI present) its BPI account representative in Customer's material IT planning and IT decision making meetings in order to facilitate continuity of Services.
(h) Be responsible for designating one or more authorized contacts for screening end-user service requests and to determine level of service needed and assignment of requests to BPI.
(i) Instruct all users to leave workstations, servers and other computer and network equipment on at all times, unless otherwise instructed by BPI. Users shall also leave any remote agents active and running at all times unless otherwise instructed by BPI. Users may log off at the end of their work shift.

9. **Exclusions.** BPI is not required to provide any Services except those Services expressly set forth in this Schedule. Without limiting the foregoing, the following items, fees, and/or services are excluded from the Services under this Schedule; any work performed related to the following will be billed at BPI's standard rates:

(a) Installation of new network infrastructure, hardware and software.
(b) Upgrades to existing network infrastructure software; not to be confused with software updates and patching that are expressly set forth above in this Schedule.
(c) Customer support services, except as specifically provided above.
(d) Any service(s) required due to treatment or attempts to install, repair, maintain, or modify any Supported Devices or related software or peripherals by a non-BPI authorized person or entity, including but not limited to negligent acts. improper configuration changes, new application installations, and upgrade installations.
(e) Supported Devices, which cannot be properly serviced due to end of life conditions, other withdrawal or termination of warranty or support by the manufacturer, unavailability of documentation or parts, or that exhibit excessive damage. BPI will use commercially reasonable efforts to provide thirty (30) days notice to Customer of any issues under this clause.
(f) Any project/integration or programming work that is designed to add or increase functionality or capacity. Projects are outside the scope of this Schedule and will be identified, quoted and agreed separately.
(g) Support for line of business applications such as accounting packages, CRM software, ERP software, etc. not specifically identified in this Schedule are outside the scope of this Schedule. BPI will use reasonable attempts to correct connectivity issues to such applications; however, problems specific to such applications or system and network problems caused by such applications are excluded.
(h) Provision of supplies or accessories for any Supported Devices or electrical work external to Supported Devices.
(i) Maintenance of accessories, alterations, attachments, upgrades or other devices; or services related to any relocation of Supported Devices unless specifically listed in a Schedule.
(j) The cost of any parts, equipment, or shipping charges of any kind.
(k) Third-party software license fees, renewal fees, or upgrade fees of any kind (except in connection with software provided by BPI in support of the Service).
(l) The cost of any third-party vendor or manufacturer support or incident fees of any kind.
(m) Training services of any kind unless otherwise agreed in writing by BPI.
(n) Moving hardware from one physical address to another physical address.
(o) Unless otherwise agreed as part of Xerox Printer Management, BPI supports only the network connection of network enabled and shared printers/copiers, and the printer connection and printer drivers of locally attached printers. Any other printer maintenance is not covered. In addition, copiers are not covered by this Schedule.

(p) Any peripheral attached or connected through a network connection to a workstation/laptop including, but not limited to USB hard drives, scanners, docking devices, cameras, and VoIP phones are not covered unless specifically listed on this Schedule.
(q) Mobile devices, smartphones, and tablets are not covered unless specifically listed on this Schedule.
(r) Home PC's and other home-based computer equipment and software.
(s) Non-Windows devices, including but not limited to Apple devices and Linux devices.

10. Backup and Restore

Customer agrees and understands that, unless BPI is providing Customer with a fully managed backup (MBS) solution under a separate Schedule, BPI is only able to review backup logs and use commercially reasonable efforts to verify that backup systems are reporting proper operation and can make no guarantees as to whether or not actual backups are taking place. If applicable, general disk/tape rotations and offsite transit of disks/tapes are Customer's responsibility. Customer is ultimately responsible for ensuring that data backups have actually been performed and are available in the event of any failure of the backup subsystem which leads to any data loss or the inability of the backup subsystem to restore data at any time. BPI has no liability for any costs associated with data recovery/disaster recovery services.

11. Hardware

BPI offers hardware warranty and extended warranty/maintenance services. Please contact BPI for further details. Under this Schedule, however, BPI does not provide hardware warranty or maintenance services, and does not maintain an inventory of spare parts or replacement hardware. It is Customer's responsibility to enter into appropriate warranty/replacement arrangements with BPI or with hardware vendors. BPI will use reasonable efforts to coordinate with hardware warranty/maintenance providers in the repair and replacement of defective hardware. BPI reserves the right to utilize the services of manufacturer's representatives for repairs guaranteed by those manufacturers under separate service contracts. BPI shall have no obligation with respect to components that are identified by the manufacturer as a consumable or expendable item including, but not limited to, printer cartridges, fuser assemblies, batteries, print heads, magnetic media, paper supplies and similar items; handling all such items are the Customer's responsibility.

12. Disaster Planning

A formal disaster recovery or business continuation plan is NOT within the scope of this Schedule. Although the services to be provided under this Schedule are designed to provide managed IT continuity and will, under certain conditions, help Customer recover from certain disasters, it should in no way be considered a formal disaster recovery or business continuity plan. If Customer requires a disaster recovery or business continuation plan, including testing of the plan, BPI can assist Customer with the development of such a plan. All time spent in the development and testing of this plan would be billable against Block Time or as an agreed additional service.

EACH PARTY REPRESENTS AND WARRANTS THAT IT HAS READ AND AGREES TO BE BOUND BY THIS SCHEDULE, INCLUDING ALL ATTACHED EXHIBITS, AND IS AUTHORIZED TO EXECUTE THIS SCHEDULE.

BPI Information Systems

By: ______________________________

____
Print Name and Title

Date: ______________________________

Customer: City of Broadview Heights

By: ______________________________

Samuel J. Alai, Mayor
Print Name and Title

Date: February 24, 2025

BPI Managed Services Standalone Options Price Worksheet

Client Information

Organization:	**City of Broadview Heights**	Date:	2/13/25
Contact:	Ted Bruzdzinski		
Address:	9543 Broadview Road, Building 7		
City/State/Zip:	Broadview Hts, OH 44147		

Monthly Services Security Management	Mo. Fee	Quantity	Units	Total
Cloud Delivered Threat Protection	$ 13.00		Device 5-Pack	$ -
Advanced Endpoint Security Protection with XDR	$ 75.00		Device 5-Pack	$ -
Multi-Factor Authentication - MFA	$ 20.00	20	User 5-Pack	$ 400.00
Network Security Service - Base IP and Domain	$ 250.00		IP Address/Domain	$ -
Network Security Service - IP Addresses 2-10	$ 35.00		IP Address	$ -
Network Security Service - Additional Domains	$ 75.00		Domain	$ -
Network Security Service - Internal Vulnerability Scans	$ 500.00		Site	$ -
Security Awareness Training	$ 95.00	1	Company	$ 95.00
Security Awareness Training Platinum Subscription	$ 13.00	20	User 5-Pack	$ 260.00
Security Information and Event Management	$ 50.00		Device 5-Pack	$ -
Zero Trust Application Control	$ 45.00		Device 5-Pack	$ -
Email Management				
Email Security Advanced Threat Protection (ATP)	$ 13.00		User 5-Pack	$ -
Email Archiving (ATP and all users required)	$ 14.00		User 5-Pack	$ -
Email Encryption Basic (ATP and all users required)	$ 7.00		User 5-Pack	$ -
Email Encryption Advanced AR (all users required)	$ 30.00		User 5-Pack	$ -
Other Services				
Cloud to Cloud Backup Bundle	$ 25.00		Site	$ -
Cloud to Cloud Backup	$ 17.00		User 5-Pack	$ -
Desktop Management	$ 175.00		User	$ -
Microsoft Cloud Bundle	$ -		Bundle	$ -
Password Management	$ 19.00		User 5-Pack	$ -
Patch Management 3rd Party Applications	$ 45.00		Device 5-Pack	$ -
Firewall Patch Management	$ 185.00		Firewall	$ -
Firewall Patch Management - HA Pair	$ 250.00		HA Pair	$ -
Total Monthly Fee				**$ 755.00**

Initial Agreement Setup and Other Fees		Fee	Quantity	Units	Total
Section	Security Management *	Block	Actual	Hours	
Section	Email Management	Block	Actual	Hours	
Section	Other Services *	Block	Actual	Hours	
Setup Fee	Network Security Service	$ 250.00		One Time	$ -
Setup Fee	Security Awareness Training	$ 350.00		One Time	$ -
Setup Fee	Desktop Management	$ 20.00		User	$ -

Summary	Quantity	
Total BMS Setup Fee		$ -
Total BMS Monthly Fee		$ 755.00
Amount Due at Signing		$ 755.00

* Exceptions: Desktop Management, Network Security Service, Security Awareness Training