RESOLUTION NO. 31-2026

Harrisburg Redevelopment Authority

WHEREAS, the Redevelopment Authority of the City of Harrisburg's Executive Director is hereby authorized to execute a professional services contract with RDCS Corporation, whose corporate headquarters is located at 616 Bartlett Drive, Dallastown, PA 17313, to provide IT and Cybersecurity Managed Services.

WHEREAS, the Authority's current contract with the same above-mentioned agency on file is dated May 03, 2017, and

WHEREAS, the Authority wishes to have an updated written agreement with this service provider.

NOW THEREFORE, BE IT RESOLVED, by the Redevelopment Authority of the City of Harrisburg, that the Executive Director is hereby authorized to enter into a professional service agreement with RDCS Corporation at the price of $690.80 per month for the ongoing services.

10/20/2026
Date

Secretary

MASTER SERVICES AGREEMENT

Managed IT Services & Cybersecurity

Between

RDCS CORP

and

REDEVELOPMENT AUTHORITY OF THE CITY OF HARRISBURG

Effective Date: **October 1, 2026**

CONFIDENTIAL

RECITALS

This Master Services Agreement (this "Agreement"), dated as of **October 1, 2026** (the "Effective Date"), is by and between **RDCS CORP**, a Delaware corporation doing business in Pennsylvania, with a mailing address of 616 Bartlett Drive, Dallastown, PA 17313 ("Service Provider" or "RDCS") and **Redevelopment Authority of the City of Harrisburg, a local government entity and public instrumentality incorporated in 1949 under the Pennsylvania Urban Redevelopment Law of 1945**, with offices located at **10 North Second Street, Suite 405, Harrisburg, PA 17101** ("Company" or "Customer").

WHEREAS, Service Provider is a leading provider of IT Managed Services, specializing in comprehensive computer and network support for businesses of all sizes, with a strong emphasis on cybersecurity;

WHEREAS, Company desires to have Service Provider provide IT and Cybersecurity Managed Services ("Services") as purchased by Company from time to time by way of a service agreement or statement of work, in exchange for the Compensation specified in this Agreement or any applicable Service Schedule, Service Order, or Invoice prepared by Service Provider; and

WHEREAS, Service Provider is willing and qualified to provide such Services to Company as defined in this Agreement;

NOW, THEREFORE, Company agrees to hire Service Provider and the Parties hereby agree as follows:

RDCS and Customer are each sometimes referred to herein as a "Party" and, collectively, as the "Parties." This Agreement may be revised by RDCS from time to time upon advance written notice to the Client due to changes in technology or laws.

ARTICLE 1 — GENERAL

1.1 Term and Termination

This Agreement shall commence on the Effective Date and shall remain in effect for **one (1)** year (the "Initial Term") and shall automatically renew for successive **one (1)**-year periods (each a "Renewal Term"), unless and until terminated by either Party by providing the other Party with sixty (60) days' written notice in accordance with this Agreement.

1.1.1 Termination for Convenience

Either Party may terminate this Agreement or any Statement of Work, in whole or in part, at any time without cause, provided the terminating Party gives the other Party at least sixty (60) days' written notice. If Customer terminates this Agreement or any Statement of Work for a reason not described in Section 1.1.2, or if RDCS terminates for a reason described in Section 1.1.2, Customer shall pay RDCS an amount equal to sixty (60) days or two billing cycles of the then-current monthly charges. Customer shall remain responsible for all license fees and related costs tied to End User License Agreements and/or Third-Party Providers, including any remaining license fees and related charges for Microsoft NCE. If Customer disagrees with any changes RDCS makes to the fees in a Statement of Work, Customer has the right to cancel the contract with sixty (60) days' notice, during which period no fee changes will apply.

1.1.2 Termination for Cause

Either Party may terminate this Agreement or any Statement of Work if the other Party (the "Defaulting Party"): (a) commits a material breach that cannot be cured; (b) commits a material breach that can be cured but fails to cure it within thirty (30) days after receiving written notice; (c) becomes unable to pay its debts as they come due; (d) becomes involved in any bankruptcy or insolvency proceedings; (e) is dissolved or liquidated; (f) assigns its assets to its creditors; or (g) has a receiver, trustee, custodian, or similar agent appointed by a court.

If either Party or anyone working with or for that Party behaves in a manner that makes continuation of this Agreement impractical, unwise, or unreasonable, the other Party may terminate this Agreement and/or any active Statement of Work by giving ten (10) days' written notice.

The Customer may terminate this Agreement if the Service Provider makes any changes to its fees, policies, or services and the Customer notifies the Service Provider that such changes are unacceptable. However, if there is any change in the quantity specified in the Agreement or Statement of Work (such as the number of sites or users), the Service Provider reserves the right to adjust its pricing accordingly.

1.1.3 Effects of Termination or Expiration

Upon expiration or termination of this Agreement for any reason:

(a) Service Provider will promptly deliver to Customer all final and incomplete work product that Customer has paid for, provide the latest backup of Customer's data, return all Customer equipment and materials (if any), remove Service Provider's equipment from Customer's premises (if any), and assist Customer in transitioning to a new service provider upon written request (at Customer's expense). Service Provider will also refund Customer for any services not yet performed or products not yet provided, unless fees or outstanding invoices are due.

(b) Both Parties will return any documents or materials containing the other's Confidential Information, delete all such information from their computer systems, and confirm in writing that they have done so.

(c) If Customer fails to provide access to Service Provider's equipment, or if any such equipment is missing, broken, or damaged (beyond normal wear and tear), or if any Service Provider software is missing, Service Provider may charge Customer the full replacement cost.

(d) If Customer requests transition assistance, Service Provider will provide reasonable assistance once Customer has paid all outstanding fees and agreed to pay Service Provider's current hourly rate. Retrieving and providing passwords, log files, server information, or converting data are considered transition services. Any software configurations created by Service Provider are Service Provider's property and will not be disclosed to Customer. Unless stated otherwise in a Statement of Work, Service Provider will not store or maintain any Customer data more than five (5) days after the end of services. Customer agrees to indemnify Service Provider from any claims related to deleting Customer's data after this period.

1.2 Independent Contractor Status

Service Provider is an independent contractor and is neither an employee nor a partner, joint venturer, or agent of the Company. Neither Party shall bind or attempt to bind the other to any contract. Company will not provide fringe benefits of any kind to Service Provider or its members, employees, agents, or affiliates. Service Provider is solely responsible for all taxes, withholdings, and other statutory or contractual obligations, including workers' compensation insurance. Unless this Agreement specifically states otherwise, the manner

in which Services are performed shall be determined by Service Provider. Service Provider may have other clients and may provide services to any third party during the term of this Agreement.

ARTICLE 2 — SERVICES AND SERVICE ORDERS

2.1 Scope of Services

Beginning on the Effective Date, Service Provider agrees to undertake and provide the Services described in this Agreement and any subsequent Schedules or Service Orders approved by Service Provider (collectively, the "Services"). Services will be delivered as detailed in each Statement of Work ("SOW"). By accepting the services and/or a SOW, Customer agrees to the terms of this Agreement. If there is a significant discrepancy or direct conflict between this Agreement and a SOW, the SOW takes precedence.

Each SOW may include: (a) a description of the services; (b) start date and duration; (c) payment details; (d) project plan and schedule; (e) project milestones and payment schedules; (f) completion criteria; and (g) any other agreed terms.

All services will be provided based on a schedule and priority that Service Provider deems reasonable and necessary. Service Provider is not responsible for delays due to reasonable and necessary transition periods, scheduled downtime, customer-side downtime, vendor-side downtime, security-related suspensions, or force majeure events. Service Provider will offer expert consultation and work diligently to provide solutions in the event of downtime; however, since these issues are beyond Service Provider's control, Service Provider cannot be held accountable for any decisions to work around downtime or related events.

Each Party owns its intellectual property rights. Nothing in this Agreement or any SOW transfers ownership of these rights unless explicitly stated in a SOW. Customer understands and agrees that Service Provider owns any software, codes, algorithms, or other works created while providing the Services. Third-party products are licensed, not sold, to Customer under the terms of this Agreement, the relevant SOW, and any applicable end user license agreement (EULA).

2.2 Cybersecurity Services Risk Assessment (CSRA)

Service Provider recommends, but does not require, that Customer complete a Cybersecurity Services Risk Assessment ("CSRA") prior to or within sixty (60) days of the Effective Date. The CSRA evaluates Customer's security posture and helps inform the Services provided under this Agreement. If Customer declines the CSRA, Customer acknowledges that Service Provider's ability to assess and address certain security risks may be limited, and Service Provider shall not be liable for vulnerabilities that would have been identified through a CSRA.

2.3 Assignment and Outside Contractors

Service Provider may, with the prior consent of the Company, engage such persons, corporations, or other entities as it reasonably deems necessary to perform Services under this Agreement; provided that Service Provider shall remain responsible for performance of all such Services.

The Service Provider shall: (a) assign a competent, experienced staff member as the main contact for this Agreement with decision-making authority; (b) obtain and maintain all required licenses or permissions before starting services; (c) follow all written rules, regulations, and policies provided by Customer regarding system and data security, building access, and health and safety; (d) for time-and-materials engagements, keep

detailed records of time and resources in a format approved by Customer; and (e) be responsible for all staff salaries, tax withholdings, payroll taxes, unemployment insurance, and workers' compensation.

2.4 Exclusions

While Service Provider will always make best efforts to provide support and troubleshoot issues, this Agreement only applies to the systems and services listed in the Service Schedule and applicable Service Orders. This Agreement does not cover: (a) issues caused by using equipment, software, or services in a manner not recommended; (b) issues resulting from unauthorized changes made by Company to configurations or setups; (c) issues caused by Company's actions that have prevented or hindered Service Provider in performing required maintenance or upgrades; or (d) issues resulting directly from work performed by Company or its contractors (other than Service Provider) on covered systems.

ARTICLE 3 — COMPANY RESPONSIBILITIES

3.1 General Obligations

Company will use all software, equipment, and services covered under this Agreement as intended. Additionally, Company will: (a) notify Service Provider of any issues or problems in a timely manner; (b) provide Service Provider with access to software, equipment, and services for maintenance, updates, and fault prevention; (c) keep Service Provider informed about potential changes to its IT systems; and (d) maintain good communication with Service Provider at all times.

Company will assign a staff member as the primary contact ("Customer Contract Manager") with decision-making authority. Service Provider may rely on instructions from this person until notified of a change in writing (not via ticketing system or voicemail).

3.2 Access and Environment

Customer commits to maintaining a dedicated full-time internet connection and granting RDCS access to its network. Customer consents to RDCS employees or subcontractors accessing its facilities solely to execute services outlined in this Agreement. Customer will provide Administrator-level password access for all covered equipment and servers as required. RDCS will not hinder Customer from accessing any Customer-owned equipment.

Customer agrees to allow Service Provider and any third-party providers to monitor, manage, communicate with, retrieve information from, and otherwise access the working environment as necessary. Service Provider may need to install software agents within the environment. Customer is responsible for obtaining all required rights of entry, licenses, permits, or other permissions at Customer's own expense prior to commencement of services. Customer must ensure safe working conditions at all times.

3.3 Minimum Environment Requirements

To ensure compatibility with the Services, Customer's existing environment must meet the following criteria. Service Provider will assess Customer's environment, advise of any non-conformities, and work with Customer to bring the environment into compliance:

(a) All servers must run Windows Server 2016 or later with the latest Service Packs and Critical Updates. (b) All desktops and laptops must run Windows 10 Pro or later with all current updates. (c) All server and desktop software must be genuine, licensed, and vendor-supported. (d) The environment must have a currently

licensed, up-to-date antivirus solution protecting all devices and email. (e) The environment must have a currently licensed, vendor-supported backup solution with monitoring and notification capabilities. (f) The environment must have a currently licensed, vendor-supported hardware firewall between the internal network and the internet. (g) All wireless data traffic must be securely encrypted. (h) Customer must provide a clean operating environment within manufacturer specifications for temperature and humidity.

3.4 Security and Compliance Obligations

Customer is solely responsible for following all applicable laws, including confidentiality and security requirements. The Services are not intended to make Customer fully compliant with any law, rule, regulation, or requirement; however, the Services may help Customer meet regulatory compliance. If Customer must comply with specific regulations (e.g., HIPAA, Gramm-Leach-Bliley Act, USA Patriot Act), Customer must inform Service Provider about any data or information requiring protection under such laws before providing or granting access to such information.

Customer understands that data loss or network failures can occur even when unpredictable. Customer must keep its computer and information systems secure, including complying with update and security policies from Service Provider and following security standards such as those in the NIST Cybersecurity Framework. Service Provider is not expected to provide internet security monitoring, cybersecurity monitoring, or watch for other cyber threats unless clearly stated in the SOW.

Customer agrees that no security solution can protect against every threat. Certain types of malware (such as previously unknown ransomware or rootkits) may bypass security measures. Service Provider does not guarantee detection, avoidance, quarantine, or removal of all malware or malicious activity, or recovery of any affected data ("Impacted Data"). Unless clearly stated in the SOW, recovering Impacted Data is not included in the Services. Customer is strongly advised to obtain cyber liability insurance.

The recovery point objective ("RPO") for restoring data from RDCS Backup is twenty-four (24) hours. Customer acknowledges that data added or changed within the preceding twenty-four hours may not be recoverable.

3.5 Advice and Recommendations

Customer acknowledges that Service Provider may provide specific advice and directions related to the Services ("Advice"), such as recommendations to increase server capacity, replace aging equipment, or cease activities that compromise the environment's stability or security. Customer is strongly advised to follow such Advice promptly. Service Provider is not responsible for any problems (including downtime or security incidents) caused by Customer's failure to follow Advice in a timely manner. If Service Provider determines that Customer's failure to follow Advice makes the Services impractical or unreasonably expensive to provide, Service Provider may terminate those Services upon notice to Customer.

3.6 Additional Customer Obligations

Customer shall: (a) submit all support tickets to support@rdcstech.com or call (717) 202-3587; (b) keep all vendor support agreements active and allow RDCS to contact vendors on Customer's behalf; (c) notify RDCS of data backup selections, preferred backup timing, and applications/data to include; (d) not change or move the working environment or install software without informing Service Provider; (e) ensure all equipment is in good working order, meets applicable standards, and complies with manufacturer warranty terms; (f) promptly inform Service Provider of any hardware or software issues and refrain from attempting repairs independently; (g) follow all copyright and intellectual property rights of third parties; and (h) carry out all patches and updates in a timely manner per manufacturer's instructions.

If Service Provider is unable to fulfill its obligations due to actions or inactions by Customer, its agents, subcontractors, or employees, Service Provider will not be deemed in breach and will not be liable for any resulting costs, charges, or losses, provided Service Provider promptly notifies Customer and consults on how to proceed.

ARTICLE 4 — BILLING AND PAYMENTS

4.1 Charges and Billing

Company shall pay all monthly recurring charges ("MRC") in advance and all other charges monthly in arrears. All charges shall be payable in U.S. Dollars, no later than **fifteen (15)** days from the invoice date ("Due Date") and shall be exclusive of any applicable taxes. Charges for each Service Order shall begin to accrue on the date the Service is provisioned. Charges are subject to change if third-party charges increase, with no less than thirty (30) days' advance written notice.

For time-and-materials engagements: (a) fees will be calculated using daily or hourly rates as specified in the SOW; (b) Customer will reimburse Service Provider for Materials (with prior written approval); and (c) Service Provider will invoice monthly. For fixed-price engagements, fees will be specified and invoiced per the SOW.

Monthly recurring payments are typically made automatically from Customer's bank account or credit card on the first business day of each month. Non-recurring payments are due upon receipt and payable within **fifteen (15)** days by check, wire transfer, ACH, or credit card.

4.2 Late Payments

If Company is more than fifteen (15) days late in making any uncontested payment, a late fee of one and a half percent (1.5%) per month shall apply. If Service Provider uses a collection agency or attorney to collect a late payment, Company agrees to pay all reasonable costs of collection. Service Provider may suspend services until payment is received and continue to charge during suspension. If Customer disputes a fee, Customer must notify Service Provider in writing within thirty (30) days of receiving the service or paying the invoice, whichever is later. A reconnection fee may apply upon resumption of suspended services.

4.3 Taxes

All charges are exclusive of taxes. Company is responsible for all applicable taxes including value added, consumption, sales, use, gross receipts, excise, access, and bypass taxes. **Company is a governmental entity exempt from Pennsylvania sales and use tax. Service Provider will not charge such taxes for so long as Company maintains a valid exemption certificate on file with Service Provider, and Company shall promptly notify Service Provider of any change in its tax-exempt status.**

4.4 Invoice Disputes

Company must notify Service Provider in writing with detailed supporting documentation within thirty (30) days of the invoice date to dispute any portion of an invoice; otherwise, the right to adjustment is waived. During a billing dispute, Company shall timely pay all undisputed amounts. If the dispute is resolved against Company, Company shall pay such amounts plus interest from the original Due Date. Company may not offset disputed amounts against other payments.

4.5 Fee Changes

Service Provider shall not change fees during the first year of this Agreement and may change fees at most once every six (6) months thereafter with no less than thirty (30) days' written notice. Any fee estimates are for informational purposes only and may differ from actual invoiced amounts.

4.6 Annual Service Rate Adjustment

To account for inflation, rising operational costs, and continued investment in service quality, RDCS reserves the right to increase fees for ongoing managed services by up to five percent (5%) annually. This adjustment will occur on the anniversary of the service start date each year, unless otherwise agreed in writing. At each renewal, RDCS may increase the contract amount by 5% to cover the cost of doing business.

4.7 Per-User and Per-Device Adjustments

Any user added to the contract (with access to the service desk) will add $150.00 to the monthly billed amount. Any system added above the contracted amount will add $50.00 to the monthly billed amount. If the user count is reduced, Customer should notify RDCS for a rate adjustment.

4.8 Refunds and Cancellations

Fees charged under this Agreement are non-refundable once Service Provider has commenced work. Partial refunds requested prior to commencement may be given at Service Provider's discretion, subject to an administrative and cancellation fee of fifty percent (50%) of fees already paid, or up to $2,000, whichever is greater.

ARTICLE 5 — LIMITED WARRANTY

5.1 Warranty

Service Provider warrants, for a period of thirty (30) days following delivery of any services (the "Warranty Period"), that all Services will be performed in a professional manner and in accordance with generally applicable industry standards. Service Provider's sole liability (and Customer's exclusive remedy) for any breach of this warranty shall be for Service Provider to re-perform any deficient services, or, if unable to remedy the deficiency within three (3) days, to void the invoice for the deficient services.

Service Provider shall have no warranty obligation if: (1) notified after the Warranty Period; or (2) the claim is solely the result of third-party hardware or software, Customer's actions, or factors outside Service Provider's reasonable control. Service Provider further warrants that its work does not infringe on anyone else's intellectual property rights.

5.2 Disclaimer

THIS SECTION IS A LIMITED WARRANTY AND SETS FORTH THE ONLY WARRANTIES MADE BY SERVICE PROVIDER. SERVICE PROVIDER MAKES 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, OR THOSE ARISING FROM THE COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE. TO THE FULL EXTENT PERMITTED BY LAW, THE DURATION OF STATUTORILY REQUIRED WARRANTIES SHALL BE LIMITED TO THE WARRANTY PERIOD.

Service Provider will pass along to Company any third-party warranties relating to any goods purchased and/or installed by Service Provider on Customer's premises and/or equipment.

ARTICLE 6 — LIMITATION OF LIABILITY

EXCEPT AS OTHERWISE PROVIDED HEREIN, COMPANY UNDERSTANDS AND AGREES THAT SERVICE PROVIDER 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 NEGLIGENCE), OR STRICT LIABILITY, EVEN IF SERVICE PROVIDER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LIABILITIES.

IN NO EVENT SHALL THE AGGREGATE AMOUNT COMPANY MAY RECOVER FROM SERVICE PROVIDER UNDER THIS AGREEMENT FOR ANY AND ALL INJURIES, CLAIMS, LOSSES, EXPENSES, OR DAMAGES, 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 NEGLIGENCE, ERRORS, OMISSIONS, STRICT LIABILITY, BREACH OF CONTRACT, OR BREACH OF WARRANTY, EXCEED THE TOTAL PAYMENTS MADE TO SERVICE PROVIDER BY COMPANY IN THE IMMEDIATELY PRECEDING SIX (6) MONTHS.

THE FOREGOING LIMITATION SHALL NOT APPLY TO THE UNAUTHORIZED DISCLOSURE OF CONFIDENTIAL INFORMATION, GROSS NEGLIGENCE, OR WILLFUL MISCONDUCT BY SERVICE PROVIDER, NOR TO PERSONAL INJURY OR DAMAGE TO TANGIBLE PROPERTY CAUSED BY SERVICE PROVIDER'S WILLFUL MISCONDUCT OR NEGLIGENCE.

ARTICLE 7 — INSURANCE

7.1 General Insurance

Each Party agrees to maintain comprehensive liability insurance, including general liability, contractual liability, property damage, and cyber liability coverage, through a reputable carrier licensed in the State of Pennsylvania, in commercially reasonable amounts calculated to protect itself and the other Party from the consequences of a data security breach and other claims. Proof of insurance shall be provided upon execution of this Agreement, and each Party shall immediately notify the other in writing of any lapse, cancellation, or modification of coverage.

7.2 Customer Cyber-Liability Insurance

Company agrees to purchase and maintain throughout the term of this Agreement a technology/professional liability insurance policy, including network security/data protection liability insurance ("cyber liability") with a minimum limit of $1,000,000 per claim and in the aggregate. Such coverage must include: (a) privacy and security liability, including breach of security/privacy laws; (b) data theft, damage, unauthorized disclosure, destruction, or corruption, including identity theft and transmission of malicious code; (c) loss or denial of service; (d) technology/professional liability, including breach of contract; (e) privacy regulatory defense and payment of civil fines; (f) payment of credit card provider penalties; and (g) breach response costs (including notification, forensics, credit protection, call center, identity theft protection, and crisis management/public relations services).

The policy shall have no cyber terrorism exclusion and must provide coverage for wrongful acts, claims, and lawsuits worldwide. Such insurance must include affirmative contractual liability coverage for the data breach indemnity obligations in this Agreement.

If Customer declines these insurance requirements, a disclaimer must be issued stating that RDCS is not responsible for any damages. RDCS maintains its own general liability, cyber liability, professional errors and omissions, and workers' compensation insurance. However, Customer is responsible for maintaining its own adequate coverage.

ARTICLE 8 — INDEMNITY

8.1 Mutual Indemnification

Each Party agrees to release, indemnify, defend, and hold harmless the other Party, including its directors, officers, employees, agents, successors, and assigns, from all claims, losses, expenses, fees, damages, liabilities, including reasonable attorney fees, arising from any third-party action related to the Indemnifying Party's performance or failure to perform its obligations under this Agreement, except for those arising from the negligence or willful misconduct of the Indemnified Party.

Service Provider is not obligated to indemnify Company for claims by third parties (including Company's clients or customers) related to services provided by Company that incorporate Service Provider's Services, including claims arising from: (a) violation of any law by Company or its clients; (b) property damage or personal injury caused by Company's clients; (c) termination or suspension of services due to a Company default; or (d) use or misuse of any Service. Indemnification will be based on a comparative fault and responsibility basis.

8.2 Indemnification Procedures

The Indemnified Party shall promptly notify the Indemnifying Party in writing of any claim and take necessary action to avoid default. The Indemnifying Party shall have the right to select counsel and control the defense and settlement, provided the Indemnified Party may participate at its own expense. The Indemnifying Party shall not take any action that would negatively impact the Indemnified Party. The Indemnified Party shall provide cooperation at the cost and expense of the Indemnifying Party.

ARTICLE 9 — CONFIDENTIALITY AND DATA PROTECTION

9.1 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. Such information shall not be disclosed to any third party and shall not be used for purposes other than those contemplated by this Agreement.

9.2 Confidential Information

Confidential Information includes but is not limited to: (a) any materials furnished by either Party; (b) information stamped "confidential" or "proprietary"; (c) business plans, strategies, customer lists, operating procedures, design formulas, know-how, processes, software, trade secrets, pricing information, and sales projections; (d) information belonging to employees, agents, customers, suppliers, vendors, contractors, and affiliates; (e) non-public inventions and proprietary technical information; (f) any other proprietary information; and (g) any templates, schematics, processes, or technical documentation provided by Service

Provider (which shall be deemed Confidential Information without any marking). Service Provider shall maintain the confidentiality of protected health information in accordance with applicable law.

9.3 Non-Disclosure

Neither Party will disclose or use, during or after the term of this Agreement, any Confidential Information of the other Party for their own benefit or the benefit of any third party, without prior written consent. Both Parties will treat Confidential Information as strictly confidential unless: (a) it becomes publicly known through no fault of the Receiving Party; (b) it was already in the Receiving Party's possession prior to disclosure; (c) it is subsequently disclosed by a third party not under any obligation of confidentiality; (d) it is approved for disclosure by prior written consent; (e) it is required by court order or law (with prompt notice to the Disclosing Party); (f) it is independently developed by the Receiving Party; or (g) disclosure is required to comply with this Agreement (with prior notice). A violation of this section shall be a material violation of this Agreement.

9.4 Employees and Agents

The Parties agree to disclose Confidential Information to their officers, directors, employees, contractors, and agents solely on a need-to-know basis and represent that such agents have signed appropriate non-disclosure agreements or are otherwise bound to hold Confidential Information in strictest confidence.

9.5 Unauthorized Disclosure

If either Party discloses or threatens to disclose the other Party's Confidential Information in violation of this Agreement, the aggrieved Party shall be entitled to seek a temporary restraining order and/or preliminary injunction without the need to post a bond. The infringing Party further agrees to reimburse the Disclosing Party for any loss or expense incurred, including court costs and reasonable attorney fees.

9.6 Data Protection

Service Provider will comply fully with all applicable laws, regulations, and government orders relating to personally identifiable information ("PII") and data privacy. Service Provider will not store, copy, analyze, monitor, or otherwise use Customer data except for the purposes set forth in this Agreement. Service Provider will protect PII and will not use, disclose, or transfer such PII except as necessary to perform under this Agreement or as authorized by the data subject or applicable law.

9.7 How We Protect Customer Information

RDCS does not store client data on its systems. All backups are stored off-site, encrypted at rest and in transit. Access to client systems is by request only, and RDCS does not access any data without the customer's direct input. Network documentation is stored in an encrypted vault with multifactor authentication. RDCS implements strict security protocols, regular audits, and staff training to ensure the protection of customer information.

9.8 Survival

The confidentiality obligations under this Article 9 shall survive termination or expiration of this Agreement for a period of **four (4) years**.

ARTICLE 10 — DEFAULT

10.1 Default by Company

Company is in default if it: (a) fails to cure any monetary breach within ten (10) days of notice; (b) fails to cure any non-monetary breach within thirty (30) days of notice; or (c) files or has proceedings initiated against it seeking liquidation, reorganization, or similar relief under any bankruptcy or insolvency law. Upon Company Default, Service Provider may suspend Services until cured or may terminate this Agreement. Service Provider may, at its sole option, cure a non-monetary breach at Company's expense and invoice Company accordingly.

10.2 Default by Service Provider

Service Provider is in default if it fails to cure any non-monetary breach of any material term within thirty (30) days of written notice from Company; provided that service-related failure or degradation in performance is not subject to a default claim unless caused by Service Provider's acts or omissions. Company's sole and exclusive remedy for any failure of Service is limited to the Limited Warranty and Limitation of Liability provisions. Upon Service Provider Default, Company may terminate upon written notice but remains obligated to pay all charges incurred prior to termination.

ARTICLE 11 — MISCELLANEOUS PROVISIONS

11.1 Notices

All notices shall be in writing and deemed delivered when personally delivered, sent by email, or forty-eight (48) hours after being deposited in the United States mail as certified or registered mail with postage prepaid, addressed to the address specified in Article 12 or to such other address as a Party may designate in writing.

11.2 Entire Agreement

This Agreement, together with all attachments, schedules, exhibits, and documents incorporated by reference (including all Statements of Work), constitutes the entire agreement between the Parties and supersedes all prior discussions, understandings, agreements, negotiations, and written agreements. Amendments require the written consent of both Parties.

11.3 Severability

If any provision is declared illegal, void, unenforceable, or invalid, the remaining provisions shall remain in full force and effect. If a court finds that an unenforceable provision may be made enforceable by limitation, it shall be deemed written, construed, and enforced as so limited.

11.4 Successors and Assigns

Company shall not transfer or assign its obligations without Service Provider's prior written consent (not unreasonably withheld), other than pursuant to a merger or change of control. Service Provider may assign this Agreement pursuant to a merger, change of control, or to an assignee of substantially all of its assets. Any purported assignment in violation of this section shall be void.

11.5 Survival

All provisions that logically ought to survive termination, including Warranties, Limitation of Liability, Indemnity, Choice of Law, Forum Selection, and Confidentiality provisions, shall survive expiration or termination.

11.6 No Waiver

The failure of any Party to insist upon strict compliance with any term of this Agreement shall not constitute waiver of such term or any breach thereof.

11.7 Force Majeure

Either Party shall be excused from delay or failure in performance caused by a Force Majeure Event (any event not caused by and not within the reasonable control of the Nonperforming Party), including but not limited to: acts of war, insurrections, fire, laws, strikes, riots, explosions, and natural disasters. Obligations shall be extended day-for-day for the duration of the interruption. If the interruption exceeds thirty (30) days, either Party may terminate upon ten (10) days' written notice.

11.8 Mediation and Arbitration

If a dispute arises, the Parties agree to first attempt resolution through mediation in accordance with the rules of the American Arbitration Association, held in the State of Pennsylvania, with costs shared equally (excluding respective attorney fees). If not resolved through mediation, the dispute shall be submitted to binding arbitration under the Commercial Rules of the American Arbitration Association. Judgment on any arbitration award may be entered in any court having jurisdiction.

11.9 Governing Law

This Agreement shall be governed by and construed in accordance with the laws of the Commonwealth of Pennsylvania, excluding its choice-of-law principles. All claims relating to this Agreement shall likewise be governed by Pennsylvania law.

11.10 Choice of Forum

All demands, claims, actions, and proceedings arising under this Agreement shall be filed and conducted in the Commonwealth of Pennsylvania. Each Party consents and submits to the exclusive jurisdiction of state or federal courts located in Pennsylvania, and waives any claims or defenses of lack of jurisdiction or improper venue.

11.11 Attorney Fees

Each Party shall bear its own attorneys' fees, costs, and expenses. The arbitrator or court may, in its discretion, award reasonable attorneys' fees and costs to the prevailing Party if it finds the other Party acted in bad faith or pursued a frivolous claim.

11.12 Electronic Signatures

This Agreement may be executed in counterparts, each deemed an original. The Parties agree that electronic signatures carry the same weight and effect as traditional handwritten signatures, and this Agreement may be electronically signed via any e-signature service compliant with the ESIGN Act and the Uniform Electronic Transactions Act (UETA).

ARTICLE 12 — CONTACT INFORMATION

All official communications related to this Agreement should be sent to the addresses specified below (or to a new address if one Party notifies the other in writing).

Service Provider:	Attention: Giuseppe Rodriguez RDCS Corp 616 Bartlett Drive Dallastown, PA 17313 (717) 844-5406 grodriguez@rdcstech.com
Customer:	Attention: **Bryan K. Davis** **Redevelopment Authority of the City of Harrisburg** **10 North Second Street, Suite 405** **Harrisburg, PA 17101** **(717) 255-6639** **bdavis@hra-harrisburgpa.org**

SUMMARY

Contract Date	**October 1, 2026**
Customer	**Redevelopment Authority of the City of Harrisburg**
Effective Date	**October 1, 2026**
Renewal Date	**October 1, 2027**
Contract Length	1 year
Payment Terms	Check, Credit Card, or ACH, **Net 15 days**
Billing Cycle	Monthly
Monthly Billing Amount	**$690.80** USD (tax-exempt)

The Agreement shall commence on **October 1, 2026**. *To confirm all the details mentioned above, both Parties have signed this Agreement on the date first mentioned.*

AGREED AND ACCEPTED:

Signature

Giuseppe Rodriguez
Printed Name

RDCS Corp
Organization

President & CEO
Title

grodriguez@rdcstech.com
Email

Date

AGREED AND ACCEPTED:

Signature

Bryan K. Davis
Printed Name

Redevelopment Authority of the City of Harrisburg
Organization

Executive Director
Title

bdavis@hra-harrisburgpa.org
Email

Date

EXHIBIT A — STATEMENT OF WORK

This Statement of Work ("SOW") adopts and incorporates by reference the terms and conditions of the Master Services Agreement entered into on **October 1, 2026** *between RDCS Corp ("Service Provider") and* **Redevelopment Authority of the City of Harrisburg** *("Customer"). This SOW is effective beginning on* **October 1, 2026** *and will remain in effect until the term set forth in Article 4 (Billing and Payments), unless earlier terminated in accordance with the Master Services Agreement.*

The onboarding process involves setting up software, security measures, and services outlined below. This setup may take up to thirty (30) days, during which some features may not be fully operational.

Monthly Contract Breakdown	
RDCS Plan	**RDCS Basic**
Plan Cost	**Four Hundred Twenty Dollars ($420.00)**
Workstations in Agreement	**5**
Users Supported	**4**
Servers in Agreement	**1**
Sites in Agreement	**1**
Firewall/Routers/VPN & Network Appliances	**1 managed firewall (SonicWall TZ-270)**
Onsite Support	**4 hours per month included**
Add-Ons	**Microsoft 365 Business Premium (4 x $28.00): $112.00** **Managed Firewall incl. subscription: $250.00** **Non-Profit Discount (Managed Firewall): ($150.00)** **SIEM, 6 devices x $9.80, 1 year log data: $58.80**
Total Monthly Cost	**Six Hundred Ninety Dollars and Eighty Cents ($690.80)**, tax-exempt (governmental entity; see Section 4.3)
Term of Agreement	1 year, 60-day cancellation notice

Monthly Pricing Detail

Description	Qty	Rate	Monthly
RDCS Basic managed services plan	1	$420.00	$420.00
Microsoft 365 Business Premium license	4	$28.00	$112.00
Managed Firewall including subscription (SonicWall TZ-270)	1	$250.00	$250.00
Managed Firewall, Non-Profit Discount	1	($150.00)	($150.00)

Description	Qty	Rate	Monthly
SIEM (Security Information and Event Management), per device, 1 year of log data	6	$9.80	$58.80
Total Monthly (tax-exempt)			**$690.80**

A.1 Support and Services

Unlimited Remote Helpdesk Support (up to **4** users). 24/7 ticket response (response only; support provided during contract hours: Monday–Friday, 9 AM–5 PM ET, closed on federal holidays). After-hours support is available at VIP rates ($195/hour) by client request and approval only (5 PM–9 PM on business days; 9 AM–9 PM on weekends and holidays; one-hour minimum). **Onsite support is included up to four (4) hours per month, as scheduled by the service desk; onsite time beyond four (4) hours in a month is billable at VIP rates.** Technical support covers desktops, printers, servers, and networking issues, **including Microsoft operating systems, Microsoft Office suites and applications, production (line-of-business) software, and security software.** The service desk uses escalation-based severity determination.

Proactive Maintenance for servers, workstations, and network resources, including weekly maintenance and monthly health reporting (up to **5** workstations), critical health and uptime monitoring, alerting for hardware failures, resource exhaustion, and internet outages, and patch management for Microsoft, Apple, and third-party applications. **Maintenance includes software updates, driver updates, performance tune-ups, auditing of logs, and security testing.**

Server Management and Support (1 server): ongoing maintenance, monitoring, and support of Customer's server.

Network Monitoring and Firewall Management: monitoring of Customer's network and management of the SonicWall TZ-270 firewall, including its security subscription, as itemized in the Monthly Pricing Detail.

RDCS IT Support application provided for quick contact, links, and automated resolutions.

Vendor Management: RDCS serves as liaison for all third-party hardware and software vendors (including Microsoft 365, Google Workspace, scanners/copiers/printers, and all line-of-business applications). RDCS will handle all future IT vendor support and ISP management.

A.2 Cybersecurity

Cybersecurity and phishing awareness training **(Security Awareness Portal)** with ongoing training throughout the calendar year and optional monthly phishing tests and attack simulators. Managed Threat Detection and Response (up to **5** workstations) including: advanced endpoint security (EDR & MDR), web content filtering, ongoing security scanning with real-time alerts, real-time threat hunting, continuous 24/7 threat monitoring and alerting 365 days a year, AI-enabled endpoint protection with machine-learning behavioral analysis, and workflow automation for escalation.

Cloud Premium Email Security (**4** accounts) including Microsoft 365 Business Premium, Microsoft 365 Defender for Malware, Spam, Phishing, and BEC protection, and daily email quarantine digest (by request).

Encryption on supported workstations and backups (at rest and in transit), secure email encryption on Microsoft 365 (by request), multifactor authentication on workstations (up to **5**), secure DNS on workstations (up to **5**), and Premier Password Vault (up to **4** accounts, optional).

Security Information and Event Management (SIEM) (6 devices): collection and retention of security event log data for one (1) year.

Incident Response and IT Policies: RDCS will maintain incident response procedures and baseline IT policies for Customer's environment.

A.3 Backups

RDCS Backup (**1** server): Full image backup to the cloud every 4 hours, encrypted at rest and in transit, **together with onsite (local) backup of data**. 1 TB of backup storage included ($50/TB thereafter). 7-year data retention. Cloud Backup for Microsoft 365 (**4** accounts): Offsite backup of mailboxes, OneDrive, SharePoint, and Microsoft Teams, multiple times daily, with unlimited storage and 7-year retention. Periodic testing of the restoration process.

A.4 Cloud Services

M365 Business Premium Licenses (**4** accounts)**, billed as an itemized line in the Monthly Pricing Detail at $28.00 per license per month**. Any migration services required will be specified in a separate addendum or included here as applicable.

A.5 RDCS Customer Experience

Quarterly cybersecurity risk reviews, comprehensive trouble-ticketing system, 9 AM–5 PM service desk support, unlimited remote support during contracted hours, network documentation, ongoing administration and management of all cyber tools/services, and asset inventory.

A.6 Exclusions from Services

The following are expressly excluded: (a) equipment purchases (quoted separately); (b) web design services (referral to trusted vendor available); (c) project work such as migrations, compliance assessments, site relocation, additional site support, or anything outside the scope of this SOW (billable separately; project work may be performed during monthly onsite visits **within the four (4) included onsite hours**, with overages billable); (d) wireless network surveys and installations; (e) employee-owned devices (RDCS may assist with email/security configuration but will not support, secure, maintain, backup, or monitor such devices); and (f) additional software or services not specified in this SOW.

A.7 VIP Rates and Out-of-Scope Work

VIP rates are $195.00 per hour. Services outside the scope of this SOW and services provided after hours (other than Monday–Friday 9 AM–5 PM ET) will be priced at VIP rates unless included in this SOW.

A.8 Guaranteed Response Times

Response times are based on severity as determined by the service desk. All response times may vary depending on complexity and technician availability. Onsite response times marked with (*) are measured from the technician's determination that onsite support is needed. Technical work for non-critical issues will cease at 5:00 PM and resume the following business day. Tickets placed after 5:00 PM carry over to the next business day per standard SLA.

Incident Example	Priority	Remote (Business Hrs)	Remote (After Hrs)	Onsite (Business Hrs)	Onsite (After Hrs)
Server offline, all users unable to work; Network switch failure halting operations; VPN link down causing office outage	**0 – Urgent**	30 min	2 hrs	2 hrs*	4 hrs*
Internet offline (local work possible); Executive workstation down; Critical LOB application failure	**1 – High**	2 hrs	4 hrs	4 hrs*	4 hrs*
Single user workstation issue; Secondary printer failure; Wireless connectivity problem	**2 – Normal**	4 hrs	Next bus. day	1 bus. day*	1 bus. day*
Slow printing; Single user scan issue; Software installation request	**3 – Low**	8 hrs	Next bus. day	Scheduled	Scheduled
Proactive maintenance; Automated tasks; Backup testing	**No Priority**	N/A	N/A	N/A	N/A

SCHEDULE 1 — GLOSSARY OF TERMS

"Advice" means specific recommendations and directions related to the Services, as described in Section 3.5.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a Party.

"Confidential Information" has the meaning set forth in Section 9.2.

"Customer Contract Manager" means the designated primary contact for Customer, as described in Section 3.1.

"Customer Equipment" means any computers, equipment, systems, cabling, or facilities owned by Customer and used in the provision of Services.

"Customer Materials" means any documents, data, know-how, methodologies, software, and other materials provided to or owned by Customer.

"Customer-Side Downtime" means any period of delay caused by Customer actions or omissions, including inability to reach the Customer Contract Manager.

"Defaulting Party" has the meaning set forth in Section 1.1.2.

"Deliverables" means all documents, work product, and materials delivered to Customer or prepared in the course of performing Services.

"Disclosing Party" means a Party that discloses Confidential Information under this Agreement.

"Environment" means any computer network, system, peripheral, or device (virtual or physical) acquired, installed, maintained, monitored, or operated by Service Provider for Customer.

"EULA" means an End User License Agreement for third-party products.

"Force Majeure Event" has the meaning set forth in Section 11.7.

"Impacted Data" means any data affected by malware or malicious activity, as described in Section 3.4.

"Intellectual Property Rights" means all patents, trademarks, copyrights, trade secrets, and all other intellectual property rights, whether registered or unregistered.

"Law" means any statute, law, ordinance, regulation, rule, code, order, constitution, treaty, common law, judgment, or decree of any government or tribunal.

"Losses" means all losses, damages, liabilities, deficiencies, actions, judgments, penalties, fines, costs, or expenses, including reasonable attorneys' fees.

"Materials" means any materials, machinery, equipment, and third-party services required to provide Services, as described in Section 4.1.

"Minimum Requirements" has the meaning set forth in Section 3.3.

"Receiving Party" means a Party that receives Confidential Information under this Agreement.

"Scheduled Downtime" means hours during which Service Provider performs scheduled maintenance (not between 9 AM–5 PM ET Monday–Friday without Customer authorization), with at least twenty-four (24) hours' notice.

"Service Provider Equipment" means any apparatus, systems, wiring, or facilities furnished by or representative of Service Provider used in the delivery of Services.

"Services" means the services described in this Agreement and any Statement of Work, including licenses, services, or products that Service Provider sells or re-sells to Customer.

"Statement of Work" or "SOW" means each Statement of Work entered into by the Parties describing the scope and provision of Services.

"Transition Exception" means the first forty-five (45) days following commencement of any Service, as well as any off-boarding period.

"Vendor-Side Downtime" means any delays or deficiencies caused by third-party service providers, licensors, or upstream vendors.