THE PENNSYLVANIA CYBER CHARTER SCHOOL
(Kindergarten through Twelfth Grade)

REQUEST FOR PROPOSAL FOR MANAGED SERVICES – NETWORK AND SERVER INFRASTUCTURE

NOTICE IS HEREBY GIVEN that The Pennsylvania Cyber Charter School ("PA Cyber" or "the Charter School") is requesting Vendor proposals under the following requirements, terms, and conditions.

PA Cyber is a public charter school authorized by the Pennsylvania Department of Education ("PDE"). The Charter School operates as a nonprofit entity incorporated in the Commonwealth of Pennsylvania, and is located at 652 Midland Avenue, Midland, Pennsylvania 15059, serving Kindergarten through Twelfth Grade.

This document will provide an overview of the proposal information requested by PA Cyber.

TABLE OF CONTENTS

I. PROPOSAL REQUEST INFORMATION

A. PROPOSAL DESTINATION

Dean Phillips
The Pennsylvania Cyber Charter School
652 Midland Avenue Midland,
PA 15059
Email: dean.phillips@pacyber.org

B. PROPOSAL KEY DATES & INFORMATION

Proposal shall be delivered by email to the above address any time prior to, but not later than, 5:00 pm on March 24, 2017. One (1) hard copy and one (1) electronic copy are to be submitted by mail or hand delivered to the above address. Proposals received after this time may be returned to the PSC. At its sole discretion, PA Cyber may extend the deadline for the delivery of proposals.

- RFP Release Date: March 6, 2017
- Intent to Submit Proposal by Vendor: March 15, 2017
- Proposal Due Date: March 24, 2017 before 5:00 p.m. Eastern Standard Time
- In- Person Presentations by Vendor Finalists: April 3-7, 2017
- Award by PA Cyber Board of Trustees : April 18, 2017

C. QUESTIONS ABOUT THIS RFP

All questions concerning this RFP should be directed to Dean Phillips, Senior Director of Technology *via* email to dean.phillips@pacyber.org. All questions and answers will be disseminated to every Vendor via email, so long as the Vendor notifies PA Cyber's representative that it wishes to receive such communications prior to submission of the RFP Response. Those notifications should be sent to dean.phillips@pacyber.org

D. VALID OFFER

All proposals submitted must be held open and remain valid for a minimum period of 90-days after the due date for the proposals.

II. PROPOSALS

The Pennsylvania Cyber Charter School ("PA Cyber" or "the Charter School") requests responses to this RFP for Managed Services – Network and Server Infrastructure. The objective of this RFP is to accomplish a fair, open, and competitive procurement. PA Cyber reserves the right to cancel the RFP or procurement, or accept or reject any and all proposals submitted in response to this request in accordance with applicable law.

Proposals will be received through the period of March 15, 2017 through March 24,2017

III. OVERVIEW AND BACKGROUND

PA Cyber serves the needs of public education throughout every county in the Commonwealth of Pennsylvania. Central administrative offices are located at 652 Midland Avenue, Midland, PA 15059. PA Cyber operates regional offices in Allentown, Erie, Greensburg, Harrisburg, Philadelphia, Pittsburgh, State College, and Wexford. PA Cyber provides services to more than 10,000 students across the Commonwealth of Pennsylvania.

Main Office	652 Midland Avenue, Midland, PA 15059
1200 Midland	1200 Midland Avenue, Midland, PA 15059
617 Midland	617 Midland Avenue, Midland, PA 15059
722 Midland	722 Midland Avenue, Midland, PA 15059
735 Midland	735 Midland Avenue, Midland, PA 15059
900 Midland	900 Midland Avenue, Midland, PA 15059
Hardware/Warehouse	518 Railroad Avenue, Midland, PA 15059
Philadelphia	1553 Chester Pike, Crum Lynne, PA 19022
Erie	2212 W. 15th Street, Erie, PA 16505
Greensburg	351 Harvey Avenue, Greensburg, PA 15601
Harrisburg	479 View Port Drive, Harrisburg, PA 17111
State College	1700 S. Atherton Street, State College, PA 16801
Pittsburgh	2600 E. Carson Street, Pittsburgh, PA 15203
Wexford	155 Lake Drive, Wexford, PA 15090
Allentown	974 Marcon Boulevard, Allentown, PA 18109

PA Cyber desires to establish a professional services relationship with a Vendor based on comprehensive and clear management principles in compliance with all federal, state, and local laws.

Vendors may only submit a proposal to provide all of the services described in this RFP. If the Vendor does not propose to provide all services, the Vendor will be disqualified.

IV. GENERAL CONDITIONS

A. **HOURS OF OPERATION.** Normal hours of operation are expected to be at a 7:30 a.m. to 4:30 p.m., continuous Monday through Friday.

B. **CHARACTER.** It is recognized that, for the protection of the children, all persons affiliated with and/or employed by the Vendor must be of stable personality and of the highest moral character. Any persons working on school grounds shall obtain the following clearances: Federal Criminal History Record, FBI Clearance Check, PA State Criminal Record Check, and PA Child Abuse History Clearance. The cost to obtain these clearances shall be borne by the Vendor who is awarded the contract. Copies of the clearances shall be given to PA Cyber at PA Cyber's request.

C. **COMPLIANCE WITH LAWS.** The proposal shall at all times observe and comply with all laws, ordinances, regulations and codes of the federal, state, county and other local government agencies, which may in any manner affect the performance of the contract. The Vendor, as an employer, shall not discriminate against any worker, employee or applicant, or any member of the public because of race, creed, color, age, sex or national origin, nor otherwise commit an unfair employment practice.

D. **INCURRED COSTS.** PA Cyber is not liable for any cost incurred by the Vendor prior to the signing of a contract by all parties.

E. **CONTRACTOR NOT AN AGENT.** Unless otherwise stated in the final Professional Services Agreement, the Vendor shall not be held or deemed in any way to be an agent, employee, or official office of PA Cyber, but rather an independent contractor furnishing professional services to PA Cyber.

F. **INDEMNIFICATION.** The Vendor shall indemnify, save, and hold PA Cyber and PDE and all of its employees, officers, directors, subcontractors and agents harmless against any and all claims, demands, suits or other forms of liability that may arise out of, or by reason of, any noncompliance by the Vendor with any agreements, warranties or undertakings contained in or made pursuant to this Agreement.

G. **NEGOTIATION OF PROFESSIONAL SERVICES AGREEMENT.** PA Cyber reserves the right to reject any or all proposals or to award a Professional Services Agreement to the next most qualified Vendor if the successful Vendor does not execute a Professional Services Agreement within twenty (20) days after award of proposal. At its sole discretion, PA Cyber may extend the date for award of the Services Agreement. PA Cyber reserves the right to negotiate any or all terms upon award of proposal.

H. **ETHICS IN PUBLIC CONTRACTING.** By submitting its Proposal, Vendor certifies that its Proposal is submitted without collusion or fraud, that it has not offered or received any kickback or inducement from any other Vendor, supplier, manufacturer, subcontractor, customer or other person in connection with its Proposal and that it has not conferred on any public employee or official having official responsibility for this procurement transaction any payment, loan, subscription, advance, deposit of money, employment,

service or anything of more than nominal value, present or promised, unless consideration of substantially equal or greater value was exchanged.

I. **PROHIBITED CONTACT.** Registered and non-registered lobbying of PA Cyber staff members or Board members with respect to a pending projector award is prohibited during the time between the date the RFP is advertised and the date a final contract is awarded. Any contact between PA Cyber staff members or Board members and any representative of a Vendor relating to a pending project or award (whether by writing, telephone, e-mail or otherwise) outside of properly scheduled meetings, other than as intended and initiated by a PA Cyber staff member or a Board member, shall be grounds for disqualification of the Vendor from the RFP response process. By submitting a Proposal, the Vendor represents and warrants that it has not made, and will not make, any contact prohibited by this paragraph.

J. **CONFLICT OF INTEREST**. Vendor certifies that no PA Cyber Board member, staff member or any PA Cyber employee has a financial or beneficial interest in the Vendor. Vendor is required to complete Vendor Conflict of Interest Disclosure Form (Schedule G)

K. **TERMINATION**. Failure by the successful Vendor to comply with the terms and conditions of this RFP or to deliver the Services identified in this RFP or the contract at the prices quoted shall void the contract award. In the case of the successful contractor's failure to deliver the Services in accordance with the contract terms and conditions, PA Cyber, after due oral or written notice, may procure such Services from other sources and hold the successful contractor responsible for any resulting additional purchase and administrative costs.

L. **AUDIT**. Unless the contract is a firm fixed price contract, PA Cyber shall be entitled to audit the books and records of the successful Vendor or any subcontractor thereof to the extent that such books and records relate to the performance of the successful Vendor's contract with PA Cyber. Accordingly, the successful Vendor agrees, and any subcontractor thereof will agree, to retain all books, records and other documents relative to this RFP and the related contract for a period of three (3) years from the date of final payment under the contract for the Vendor and for a period of three (3) years from the date of final payment under the subcontract for the subcontractor, unless a shorter period is otherwise authorized in writing by PA Cyber. By submitting a Proposal, the successful Vendor grants to PA Cyber the right to perform, or have performed by its authorized agents and/or auditors, an audit of the books and records of the successful Vendor. Consequently, PA Cyber will have full access to, and the right to examine, any of said materials following the giving of reasonable notice during said period. VENDORS ARE HEREBY NOTIFIED THAT ALL RECORDS OF ALL PERSONS CONTRACTING WITH PA CYBER MAY BE SUBJECT TO THE PENNSYLVANIA PUBLIC RECORDS ACT.

M. **TAXES**. The successful Vendor shall determine, be responsible for, and pay any applicable taxes related to the Professional Services Agreement. PA Cyber is a tax-exempt organization and shall not be billed for, nor be expected to pay, any taxes applicable to the Services. A COPY OF DOCUMENTATION VERIFYING THE "TAX EXEMPT" STATUS OF PA CYBER IS AVAILABLE AND WILL BE FURNISHED TO THE SUCCESSFUL VENDOR UPON REQUEST.

N. **SUPPORT**. The successful Vendor agrees and affirms that, throughout the Agreement Term, it will utilize its best efforts to assist and support PA Cyber in addressing any problem whatsoever relating to the Professional Services Agreement.

O. **INSURANCE**. By submitting a Proposal in response to this RFP, the Vendor certifies that, if awarded a contract, it will have the insurance coverage required for performance of the Services, if any, at the time the work commences. Additionally, the Vendor certifies that it will maintain this insurance coverage throughout the entire term of the contract and that all insurance coverage shall be provided by insurance companies authorized to sell insurance in Pennsylvania. During the term of the contract, PA Cyber reserves the right to require the successful Vendor to furnish certificates of any required insurance for the coverage required by PA Cyber, if any is required.

P. **CONFIDENTIAL AND PROPRIETARY INFORMATION**. PA Cyber is subject to the Pennsylvania "Public Records Act." Accordingly, no claim of confidentiality or proprietary information in all or any portion of any Proposal submitted in response to this RFP will be honored unless a specific exemption from the Public Records Act exists and such exemption is cited in the Proposal. Any claimed exemption must be specifically cited by page and paragraph number(s). An incorrectly claimed exemption does not disqualify the Vendor.

Q. **ASSIGNMENT OF CONTRACT**. Upon execution, the contract shall not be assigned or subcontracted by the successful Vendor, in whole or in part, without the prior written consent of PA Cyber.

R. **BINDING NATURE OF THIS RFP**. By submitting a Proposal, the Vendor agrees to be bound by all of the provisions of this RFP. The Vendor further agrees that, if it becomes the successful Vendor, the Vendor and its heirs and assigns will continue to be bound by the provisions of the RFP for the duration of the Agreement Term except to the extent any provision hereof is explicitly waived in the Agreement.

S. **APPLICABLE LAWS AND COURTS**. This RFP and any related Proposal and resulting contract shall be governed in all respects by the laws of the Commonwealth of Pennsylvania. Jurisdiction over any matter arising in connection with this RFP or any related Proposal or resulting contract hereunder shall be held by the state and federal courts having jurisdiction in Beaver County, Pennsylvania and the Western Federal District (Pittsburgh).

T. **ADDITIONAL INFORMATION.** PA Cyber reserves the right to request clarification of information submitted and to request additional information of one or more Vendors.

U. **CAPTIONS.** Headings in all sections of this document are provided as a convenience only, and shall not affect the interpretation of this instrument, its attachments, and addenda.

V. SERVICE SPECIFICATIONS

PA Cyber is requesting proposals for Managed Services – Network and Server Infrastructure.

Managed Services are to include:

NETWORK

Network hardware and software support and maintenance; Network security management; LAN Administration (except end user identity management); Network installations and de-installations, upgrades, etc. Network technologies will include LAN, WAN, Wireless/WiFi, unless already managed by another third party (e.g. MPLS, ISP, etc.).

SUPPORT SERVICES. The Managed Service Partner shall provide management, maintenance and support of the current operational LAN environments and associated infrastructure elements at all in-scope locations, including documentation by following ITIL Service Management processes and as per guidelines and policies as defined or agreed to by PA Cyber. The sub-services include, but are not limited to:

- Network Support and Maintenance
- Wireless Networks
- LAN and WAN Administration
- Network Security
- Installation / De-installation
- Reporting

For additional information about the network, please contact Dean Phillips

NETWORK SUPPORT AND MAINTENANCE. The Managed Service Partner shall perform the on-going support and delivery of all local networks, and ensure end-user and server connectivity in order to meet business objectives and performance criteria.

The Managed Service Partner shall perform maintenance on all local network

infrastructure components in line with the equipment manufacturers and/or PA Cyber guidelines and ensure that firmware is kept current and security patches are applied.

Network equipment components include but are not limited to routers, firewalls, load balancers, switches, patch panels, circuits, and network appliances and cloud-based services (i.e. email security, email archiving, and content filtering).

Other LAN components comprise the Traffic prioritization, Network Client Services, Network Monitoring servers, software and Scripts, networking protocols, IP address Management (DHCP), name resolution services (DNS).

The Managed Service Partner shall configure and maintain Web Content Filtering services with PA Cyber guidance and in accordance with PA Cyber policies.

The Managed Service Partner shall configure and maintain Remote Access (user) VPN services and Site to Site VPN services with PA Cyber guidance and in accordance with PA Cyber policies.

The Managed Service Partner shall administer the cable and patch panel management and perform patching to resolve problems or reconfigure the LAN.

The Managed Service Partner shall ensure that any maintenance action leading to a Scheduled Outage or a noticeable degradation of service is planned via the appropriate Change and Release Process in order to minimize disruption to the service.

The Managed Service Partner shall maintain a detailed inventory of all network equipment including but not limited to routers, switches, firewalls, storage devices/SAN's.

WIRELESS NETWORKS. The Managed Service Partner shall manage and support a wireless LAN for visitors and PA Cyber staff at all designated PA Cyber premises including but not limited to the Midland and remote office locations listed in this document.

* For additional information about the network, please contact Dean Phillips

LAN ADMINISTRATION. The Managed Service Partner shall maintain the PA Cyber IP addressing scheme and continuously support the implementation of optimal policy-based routing policies and architecture.

The Managed Service Partner shall allocate IP addresses when necessary and maintain the register of used and available IP addresses at PA Cyber.

The Managed Service Partner shall provide simple rule-based and/or intelligent filtering of traffic between different network segments along the following principles:

- Create an IP-enabled network infrastructure supporting the injection of all traffic over IP, IP encapsulation and IP tunneling.
- Maintain clear physical and logical boundaries.
- Limit complexity in top level routing.
- Allow peering architecture and addressing hierarchy between locations.
- Include, where appropriate, traffic shaping and prioritization of IP based traffic.
- Include, where appropriate, segmentation and implementation of networks using variable/fixed length subnet masks.
- Maintenance and creation of V-LAN IDs.
- Maintenance and creation of Multi Link Trunks.
- To create, where appropriate, multicast address and support for one to many network broadcasts.

The Managed Service Partner shall implement and maintain access and authentication controls relating to the management and configuration of all intelligent components of the network.

The Managed Service Partner shall support the creation of an IP-centric organization enabling the convergence of all traffic, including IP voice and video.

Where appropriate maintenance and creation of Internet Protocol version 4 and 6 address spaces.

NETWORK SECURITY. The Managed Service Partner shall ensure that wherever the PA Cyber network connects to other networks, the Managed Service Partner shall co-operate with the relevant parties to ensure that appropriate security is put in place with a view to protecting the Network and its components from malicious attack and unauthorized access.

The Managed Service Partner shall also ensure that users on the Network are prevented from making malicious attacks on other networks.

The Managed Service Partner shall monitor the Network for any attempted or actual security breaches.

INSTALLATION / DE-INSTALLATION. Where installation / de-installation has been required and confirmed by PA Cyber, the Managed Service Partner shall be responsible for the complete set

of associated works in line with Health and Safety requirements, and shall communicate with appropriate teams within PA Cyber to this effect.

The Managed Service Partner shall manage the installation / de-installation and testing as needed of all LAN changes in accordance with standard procedures, updating the relevant documentations to reflect the changes, and informing the PA Cyber Technology Director of the impact of the change.

Where work may be carried out by Third Parties appointed by the Managed Service Partner, the end-delivery of the project remains the responsibility of the Managed Service Partner. The Managed Service Partner shall be responsible for the resolution of faults during installation and commissioning, and provide all necessary warranty and documentation.

Where work may be carried out by Third Parties appointed by PA Cyber, the Managed Service Partner shall have the responsibility to provide an efficient service interface for the successful end delivery of the works. The Managed Service Partner shall remain responsible for the Service Support functions post-installation and the Service Management aspects, e.g. Configuration and Capacity Management.

All LAN (including both fixed wired and wireless networks) design, installation and testing works supplied by the Managed Service Partner will have to comply with international standards (IEEE and ISO) including but not limited to:

- ISO 8802.3 1000 Mbps Gigabit Ethernet
- ISO 8802.3 100BASET operating at 100Mb/s
- ISO 8802.3 10BaseT operating at 10Mb/s
- Structured cabling utilizing TIA/EIA-568-B or Category 5 e standards
- Fiber connectivity including single mode and multimode including FC and SC Termination.

Provision of secure wireless networking operating 802.11 (B/G/N), 802.11 (A/C) – utilizing WPA-2 and other approved security authentication.

REPORTING. The Managed Service Provider shall provide regular performance monitoring reports (frequency to be agreed) on network and LAN uptime, incidents, and other performance metrics agreed. Managed Service Provider shall agree to provide PA Cyber with application access to view all monitoring, incidents including all incident details.

The Managed Service Provider shall provide input into the Capacity Planning exercise to ensure that the networks are sized at the level required for the services to be provided.

The Managed Service Provider shall provide high-level and detailed network diagrams for the WAN/Organization and each PA Cyber location/LAN as changes are made.

On request by PA Cyber, the Managed Service Provider shall produce ad-hoc reports related to network and LAN service management aspects.

MINIMUM AND OPTIMUM OPERATING HOURS

The minimum on-site support in all Data Center locations and Network and LAN services will be based on a "lights-on" approach covering the extended working day (i.e. 9 hours from 7:30 to 4:30 Monday through Friday) at each location with on-call support outside these hours.

Optimum on-site support would be for a full 24x7 service.

Remote support and maintenance may be possible outside of core hours or in locations where there is insufficient equipment to warrant a full on-site support service. This will need to be agreed and established in advance based on the service level agreements.

IMPLEMENTATION OF NEW NETWORK AND LAN SERVICES. The Managed Service Partner is expected to be actively involved in the development of new network and LAN services.

The Managed Service Partner would be expected to be involved in all aspects of the service development and to provide work and cost estimates as part of the approval process.

SERVERS

This component will cover: Support and administration services for all physical and virtual servers, operating systems and any other server-related software; systems monitoring and housekeeping; storage management and capacity planning; backup and recovery; business continuity and disaster recovery planning and execution.

SUPPORT SERVICES. The Managed Service Provider shall provide support and administration services for all server hardware, virtual server environment, server operating systems and other software related to server support in scope at all Midland, PA offices as well as PA Cyber regional offices, including documentation by following ITIL Service Management processes and as per guidelines and policies defined or agreed by PA Cyber. The sub-services include, but are not limited to:

Server support and maintenance;
Systems monitoring;
System hardware management and support;
System software management and support;
System housekeeping services;
Storage management and capacity planning;

Database administration;
Email Administration (Exchange/Office 365) and Email Security (i.e. MimeCast)
Active Directory Administration (On-premise/Azure)
Internet Information Services (IIS) - Administration/Configuration.
Anti-Virus – Administration/Configuration. (i.e. AVG)
Single Sign On Support for Systems – Configuration/Maintenance (i.e. LDAP, SAML, etc)
Backup and restore services;
Server Inventory – Maintain (physical and virtual)
Reporting.

*For additional information about the Servers please contact Dean Phillips

SERVER SUPPORT AND MAINTENANCE. The Managed Service Provider shall maintain a stable live data center environment in order to achieve applicable service levels.

Items in-scope shall include all infrastructure elements and systems contained within all data center related to the servers in-scope defined above.

The Managed Service Provider shall perform routine administration and maintenance of PA Cyber's data centers, and to this effect shall:

- Undertake corrective maintenance ensuring that all problems are raised and logged centrally.
- Ensure that all products and tools that support live operations comply with the defined technical standards, policies and procedures, and with government regulations.

- Pro-actively inform PA Cyber if the operational environment in any data center is unsuitable and action is required.
- Provide interface with relevant PA Cyber teams to help ensure the fitness of the Data Center accommodation and operational environment conditions.
- Assist PA Cyber in maintaining a log for data center access.
- Maintain an inventory of on-site spares for critical equipment.
- Prepare and update Standard Operating Procedures (SOPs).

SYSTEMS MONITORING. The Managed Service Partner shall ensure that all System monitoring functions are periodically performed like:

· Performance / uptime monitoring.
· Log monitoring.

SYSTEM HARDWARE MANAGEMENT AND SUPPORT. The Managed Service Provider shall provide support and administration services for all server hardware including installation, maintenance and monitoring of the products including but not limited to:

- Patches for server hardware firmware and BIOS.
- Updates to server hardware firmware and BIOS.
- Be responsible for all upgrades to server hardware.
- Manage and coordinate with third party suppliers (i.e. Expedient, HP, Microsoft)
- Produce and maintain a Capacity Plan covering all systems and proactively inform PA Cyber of the need for any changes.
- Perform a periodic health check on all hardware.
- Maintain a list of all users with system level privileges.

SYSTEM SOFTWARE MANAGEMENT AND SUPPORT. The Managed Service Provider shall provide support and administration services for all operating systems including installation, maintenance and monitoring of the products.

- Perform routine upgrades to the Operating Systems.
- Perform proactive maintenance of Servers.
- Maintain Operating Systems to minimize impact of any potential shortcomings.
- Ensure that appropriate approval is obtained from PA Cyber prior to application of any vendor patches and/or upgrades.
- Manage and coordinate with 3rd party suppliers for provision of OS software.
- Deploy, configure and secure operating systems in use by PA Cyber to vendor recommended best practices or other agreed standards.
- Ensure that any software security related patches for Operating Systems or ancillary software is deployed in an agreed timely manner.
- Implement monitoring of all Operating Systems.
- Maintain a list of all users with system level privileges.
- Ensure all application certificates are renewed and installed.

SYSTEM HOUSEKEEPING SERVICES. The Managed Service Partner shall ensure that all System administration functions are periodically performed like:

- System / file cleanup.
- Server reboot as needed.
- Maintain local firewall rules and policies.
- Perform periodic intrusion detection testing and remediation.
- Monitor supplier websites for critical security alerts and patches.

STORAGE MANAGEMENT AND CAPACITY PLANNING. The Managed Service Provider shall provide managed storage area network and related storage services to include but not limited to:

- The creation and assignment of storage space to servers and services.
- Provision of storage connectivity including the installation of HBA, Switches, and fiber connections.
- Replication, where necessary, of SAN storage to a remote location(s).
- Reallocation of Storage.
- Storage capacity monitoring including alerting when utilization exceeds at prescribed levels.

DATABASE ADMINISTRATION. For databases within the scope of the Infrastructure Managed Services, the Managed Service Provider shall provide database management, support and administration services including installation, maintenance, rebuilding indexes, tuning and monitoring of the database.

The Managed Service Provider shall pro-actively inform PA Cyber of the need for changes in the size of the databases or the need to perform re-organization, due to indicative business growth, new developments, application enhancements or if opportunities for performance optimization are available.

BACKUP AND RESTORE SERVICES. The Managed Service Provider shall operate a data backup and recovery service for PA Cyber Data Centers in accordance with backup and recovery policy and Performance Targets.

Align with PA Cyber Disaster Recovery and Business Continuity Policy and Procedures – agree and maintain the backup policy and procedures in line with PA Cyber standards and Performance Targets.

Back-up system according to agreed Backup Schedule – once authorized by PA Cyber, set up, schedule and carry out relevant back-ups of all User and system data that is held on the servers according to agreed Backup Schedules with PA Cyber.

In the event of a backup failure, load and unload back-up media at the Data Centers and in the backup storage devices in accordance with the backup policy and procedure, restore lost or damaged files and retain back-ups of standard PC system build data.

Carry out replacements of backup media in line with the manufacturers' guidelines and/or diagnostic information produced as a result of backup and restore processes.

Recycle media at end of agreed retention period and replace where operationally desirable (e.g. wear and tear) according to policy agreed with PA Cyber.

Where possible, ensure that data restore is tested on a regular basis to verify integrity of backups and back-up media according to an agreed schedule with PA Cyber.

REPORTING. The Managed Service Provider shall provide regular performance monitoring reports (frequency to be agreed) on server uptime, SAN usage, incidents, and other performance metrics agreed.

The Managed Service Provider shall provide input into the Capacity Planning exercise to ensure that the Data Center is sized at the level required for the services to be provided.

On request by PA Cyber, the Managed Service Provider shall produce ad-hoc reports related to server and data center service management aspects

IMPLEMENTATION OF NEW DATA CENTER SERVICES. The Managed Service Partner is expected to be actively involved in the development of new Data Center services.

The Managed Service Partner would be expected to be involved in all aspects of the service development and to provide work and cost estimates as part of the approval process.

SERVICE WINDOW

The Managed Service Provider is expected to perform data center maintenance (hardware and software) minimizing the impact on operations. This shall require scheduling outages at lower usage periods, outside of normal operating hours, e.g. nights or weekends. This should be part of the base service and not incur any additional (e.g. overtime) costs.

All changes to the systems (hardware and software) should be based on an approved Change Request (or Emergency CR). The Managed Service Provider is expected to follow the established CAB and ITIL procedures when implementing a Change Request.

MINIMUM AND OPTIMUM OPERATING HOURS

The minimum on-site support in all Data Center locations will be based on a "lights-on" approach covering the extended working day (i.e. 9 hours from 7:30 to 4:30 Monday through Friday) at each location with on-call support outside these hours.

Optimum on-site support would be for a full 24x7 service.

Remote support and maintenance may be possible outside of core hours or in locations where there is insufficient equipment to warrant a full on-site support service. This will need to be agreed and established in advance based on the service level agreements.

VI. VENDOR SUBMISSIONS

Vendors are to provide:

General Company Information:

- Include a summary by narrative, brochure, chart, or other means showing the Vendor's qualifications and philosophy that give the Vendor the ability to satisfy all proposal requirements.

Client Relationship Management:

- Include a summary of how staff will be structured, trained, retrained, and professionally developed.
- Detailed plan demonstrating how Vendor plans to provide all services contained within this RFP

- Provide resumes summarizing the experience and qualifications of possible on-site managers and employees.
- Include an organizational chart showing the staffing and lines of authority of key personnel anticipated to be used in performing the contract.
- Describe how you would propose changes in technicians assigned to the contract and seek approval for such changes from PA Cyber.
- Describe in detail how all support staff would be expected to serve PA Cyber including executives, technicians, project, and account staff.
- Include hours of operation for staff and support. Describe how after hours support would be available.

Security:

- Include strategy for securing PA Cyber data.
- Include Company's policies as well as any security certificates that you possess.
- Describe your Company's security certification and expertise.

Service Levels:

- Provide Standard Support Service Level Agreement
- Provide standard response time metrics over the past year
- Provide issue and maintenance communication methods, escalation procedures,
- Description and sample of ticketing/incident tracking system
- Describe customer access to incident ticketing/tracking system, customer access to monitoring systems, and customer access to reporting features
- Provide sample standard vendor reports that are supplied to customer and frequency of each report
- Describe the ability for client to provide feedback regarding services provided and how customer feedback is used and shared to improve services and support.
- Provide your guaranteed response time for issues dependent upon severity and time of day.

- Provide how scheduled down times would be determined and communicated.
- Provide how you propose that SLAs are enforced
- Provide standard key performance indicator samples

VII. PREPARATION OF PROPOSALS

In order to ease comparability and enhance the review process, it is required that proposals be organized in the manner specified below with tabs. Failure to provide the required organized information will affect the evaluation of the proposal and may be grounds for disqualification. It is required that any attached schedule forms be completed and returned with your Proposal in the proper organized manner as specified below. If any form is not applicable, form should be returned stating non-applicable. An original manual signature is required.

Table of Contents: Include a table of contents for clear identification of the material by section and by page number.

Tab 1 Letter of Transmittal: Write a letter of Transmittal, introducing your firm's proposal that summarizes your understanding of the project and highlights your firm's unique qualifications for delivering this solution.

Tab 2 Proposal: The proposal should address the provider's ability to meet the Service Specifications outlined in the RFP. The proposal should be concise and should address the specification requirements as outlined above.

Tab 3 Experience of Firm and Dedicated Staff: Provide a summary of your firm's experience in delivering similar solutions. Make every attempt to match experiences to specific requirements listed in this RFP in order to illustrate specific experiences that qualify your firm to deliver this solution. Also include in this section, your firm's capacity for delivering this proposed solution --specifically, available product inventory and necessary expertise.

Tab 4 References: List at least five (5) other clients for whom the Vendor has provided services similar to the Services (with preference given to clients comparable to PA Cyber) and, for each such reference, the business name, the identification of a contact person, the title of the contact person, a telephone number and email address.

Schedule A

CERTIFICATION OF PROPOSAL

I (We) have read The Pennsylvania Cyber Charter School ("PA Cyber") Request for Proposal ("RFP") and fully understand its intent. I (We) certify that I (we) have adequate personnel and resources to fulfill the proposal requirements. I (We) further understand that our ability to meet the criteria and provide the required services shall be judged solely by PA Cyber.

I (We) further certify that, since the receipt of this RFP, no contact, discussion, or negotiation has been made nor will be made regarding this proposal, with any PA Cyber employee or Board Member other than the listed contact people in the RFP. I (We) understand that any such contact could disqualify this proposal.

I (We) certify that all schedules and addenda contained herein shall be considered part of the entire RFP and that the complete documents submitted shall be considered a legally binding document.

Submitted by:

_____
Proposer's Name

_____
Authorized Signature

_____
Name and Title

_____
Telephone

_____
Date

THIS PAGE MUST BE SIGNED AND INCLUDED IN YOUR RESPONSE.
Unsigned responses will not be considered

Schedule B

ORGANIZATION

Entity Name_____

Principal Name/Title_____

Address_____

Phone_____

Fax_____

HISTORY/PROFILE OF PROPOSER OR PROPOSER'S FIRM.

DESCRIPTION OF ORGANIZATION (IF APPLICABLE). DESCRIBE IN DETAIL YOUR FIRM'S QUALIFICATIONS AND CAPABILITIES LISTED IN SCOPE OF SERVICES.

ATTACH RESUMES OR ANY ADDITIONAL INFORMATION ABOUT THE PROPOSER OR HIS OR HER COLLEAGUES THAT MAY BE CALLED UPON TO CONSULT WITH PA CYBER.

*If additional space is needed, please attach to this document.

Schedule C

REFERENCES, EXPERIENCE AND EXPERTISE

Provide a list of organizations for whom you have performed Technology Support Services for in the last five (5) years. Provide a short summary of the services provided, and the dates of service. Please include a name and telephone number of a contact person who supervised your work where possible.

*If additional space is needed, please attach to this document.

Schedule D

COST

A. I (We) the undersigned, hereby propose to furnish all supervision, labor, materials, tools, equipment, supplies, services, insurance, transportation, and other incidental requirements necessary to perform the work in accordance with the foregoing RFP. I (We) offer the following price schedule that will be held firm for the duration of the contract period. Vendor must provide a detailed cost breakdown by managed service. Vendor must also provide a price list for services or expenses that are optional or are project based that fall outside managed contractual services.

*If additional space is needed, please attach to this document.

COST

B. I (We) acknowledge receipt of the following RFP addenda and have included their provisions in our proposal: (only necessary if additional RFP addenda have been issued)

Addendum No. _____ Dated _____

C. I (We) agree to hold the RFP amount firm for ninety (90) calendar days after the receipt of the proposal by PA Cyber. The contract period will be for two (2) years with the option for PA Cyber to renew under the same terms and conditions for an additional one (1) year period.

D. I (We) have read and understand the RFP documents. Furthermore, I (We) are prepared to comply with all the requirements contained therein. Submitted by:

_____
Proposer's Name

_____
Authorized Signature

_____
Name and Title

_____
Telephone

_____
Date

THIS PAGE MUST BE SIGNED AND INCLUDED IN YOUR RESPONSE.
Unsigned responses will not be considered

Schedule E

NON-COLLUSION AFFIDAVIT

State of _____:

County of _____:

I state that I am _____ of _____
(Title) (Name of Firm)
and that I am authorized to make this affidavit on behalf of my firm, and its owners, shareholders, principals, directors, and officers. I am the person responsible in my firm for the price(s) and the amount of this RFP response.

I hereby certify that:

(1) The price(s) and amount(s) of this RFP response have been arrived at independently and without consultation, communication or agreement with any other Vendor.

(2) Neither the price(s) nor the amount(s) of this RFP response, and neither the approximate price(s) nor approximate amount(s) of this RFP response, have been disclosed to any other firm or person who is a Vendor or potential Vendor, and the price(s) and/or amount(s) will not be disclosed before RFP response opening.

(3) No attempt has been made or will be made to induce any other firm or person to refrain from RFP response ding on this contract, or to refrain from submitting a RFP response higher than this RFP response, or to submit any intentionally high or noncompetitive RFP response or other form of complementary or bogus RFP response.

(4) The RFP response of my firm is made in good faith and not pursuant to any agreement or discussion with, or inducement from, any other firm or persons to submit an intentionally high or noncompetitive RFP response or other form of complementary or bogus RFP response.

(5) _____, its affiliates,
(Name of my firm)
subsidiaries, shareholders, principals, officers, directors and employees are not currently under investigation by any governmental agency and have not in the last four years been convicted or found liable for any act prohibited by State or Federal law in any jurisdiction involving conspiracy or collusion with respect to RFP response ding on any public contract, except as follows:

Schedule E (Continued)

I further certify that _____understands,
(Name of my firm)
acknowledges, and agrees that the above representations are material and important, and will be materially relied upon by PA Cyber in awarding the contract(s) for which this RFP response is submitted. I understand and agree, and my firm understands and agrees, that any misstatement in this affidavit is and shall be treated as fraudulent concealment from PA Cyber of the true facts relating to the submission of RFP response s for this contract.

_____
(Name and Company Position)

SWORN TO AND SUBSCRIBED
BEFORE ME THIS _____ DAY OF _____, 2017

_____ My Commission Expires:
Notary Public

THIS PAGE MUST BE SIGNED AND INCLUDED IN YOUR RESPONSE.

UNSIGNED RESPONSES WILL NOT BE CONSIDERED

Schedule F

VENDOR STATEMENT OF QUALIFICATIONS

Please provide written responses to the following questions. If the answer to any of the questions is "Yes", Vendor shall describe fully the circumstances, reasons therefore, the current status, and ultimate disposition of each matter that is the subject of this inquiry.

1. Has Vendor been declared in default of any contract? ____ Yes _____No

2. Has Vendor forfeited any payment of performance bond issued by a surety company on any contract? _____Yes _____No

3. Has an uncompleted contract been assigned by Vendor's surety company on any payment of performance bond issued to Vendor arising from its failure to fully discharge all contractual obligations there under? _____Yes _____No

4. Within the past three (3) years, has Vendor filed for reorganization, protection from creditors, or dissolution under the bankruptcy statutes? _____Yes _____No

5. Is Vendor now the subject of any litigation in which an adverse decision might result in a material change in the firm's financial position or future viability? _____Yes _____No

6. Is Vendor currently involved in any state of a fact-finding, negotiations, or resistance to a merger, friendly acquisition, or hostile take-over, either as a target or as a pursuer? _____Yes _____No

7. License Sanctions: List any regulatory or license agency sanctions. PA Cyber may perform a background check on respondent with all state and regulatory agencies.

_____

Authorized Representative's Signature

_____

Company Name

Schedule G

Vendor Conflict of Interest Disclosure Form

All vendors interested in conducting business with The Pennsylvania Cyber Charter School must complete and return the Vendor Conflict of Interest Disclosure Form in order to be eligible to be awarded a contract. Please note that all vendors are subject to comply with The Pennsylvania Cyber Charter School's conflict of interest policies as stated within the certification section below.

If a vendor has a relationship with a Pennsylvania Cyber Charter School official or employee or an immediate family member of a Pennsylvania Cyber Charter School official or employee, the vendor shall disclose the information required below.

Certification: I hereby certify that to my knowledge, there is no conflict of interest involving the vendor named below:

- No Pennsylvania Cyber Charter school official or employee, or an immediate family member has an ownership interest in vendor's company or is deriving personal financial gain from this contract.
- No retired or separated Pennsylvania Cyber Charter School official or employee who has been retired or separated from the school for less than one (1) year has an ownership interest in vendor's company.
- No Pennsylvania Cyber Charter School employee is contemporaneously employed or prospectively to be employed with the vendor.
- Vendor hereby declares it has not and will not provide gifts or hospitality of any dollar value or any other gratuities to any Pennsylvania Cyber Charter School official or employee to obtain or maintain a contract.
- Please note any exceptions below:

Vendor Name	**Vendor Phone Number**
Conflict of Interest Disclosure*	
Name of Pennsylvania Cyber Charter School official, employees or immediate family members with whom there may be a potential conflict of interest. Other_____ List name(s) below: _____ _____	( ) Relationship to employee_____ ( ) Interest in vendor's company_____ ( )

*Disclosing a potential conflict of interest does not disqualify vendors. In the event vendors do not disclose potential conflicts of interest and they are detected by the school, then the vendor will be exempted from doing business with the school.

I certify that the information provided is true and correct by my signature below:

_____ _____ _____

Signature of Vendor Authorized Representative | Date | Printed Name of Vendor Authorized Representative

Procurement Use Only

____ Yes, named employee or official was involved in the procurement process or decision
____ No, name employee or official was not involved in the procurement process or decision