The Pennsylvania Cyber Charter School
Managed Services – Network and Server Infrastructure

SECOND SET OF RESPONSES TO RFP QUESTIONS
March 13, 2017

1. As Service Desk and PC support functions are not included in this RFP, are we correct in assuming that another vendor/team would be performing end user support? If so, we assume that network and server issues would be triaged by that Service Desk/PC support team and then escalated to the Managed Service Provider by a select number of designated contacts. Is this a correct assumption or how would issues be submitted to the Managed Service Provider?

Answer: **Yes, Service Desk and End User/PC Support functions will be performed internally. The MSP will not be responsible for supporting PA Cyber in this capacity.**

Yes, network and server issues will be triaged by the internal Service Desk and then escalated to the MSP by a select number of designated contacts.

Yes, your assumption is accurate.

2. Will the Managed Service Provider be responsible for AD user administration (account provisioning and de-provisioning, Group Policy Objects (GPOs), Organizational Units (OUs), etc.) Similarly is the Managed Service Provider responsible for email account management? If the answer is 'yes', how is the information (i.e. new user setup information, distribution list changes, etc.) transmitted to and from the Managed Service Provider?

Answer: **No, the MSP will not be responsible for AD user administration (account provision and de-provisioning, Group Policy, OU's, etc.)**

No, the MSP will not be responsible for email account management.

3. Please clarify what you mean by 'except end user identify management'? (Network section, 1st Paragraph, Page 8)

Answer: **The MSP will not be responsible for AD user administration, email account management, nor assigning privileges to end-users. PA Cyber will internally address the need to ensure appropriate access to resources and applications.**

4. Please clarify what you mean by 'The Managed Service Partner shall support the creation of an IP-centric organization enabling the convergence of all traffic, including IP voice and video'? (LAN Administration section, 5th paragraph, Page 10)

Answer: **PA Cyber is committed to utilizing IP networks for voice (VoIP), messaging, video conferencing, collaboration, and traditional applications. We believe that the convergence and delivery of those services provides advantages including economies of scope and scale but it also makes the performance, reliability, and security of our network extremely important. The MSP will be required to configure, monitor, and manage the networks (i.e. prioritize traffic, QoS) as to provide a high quality of service to our staff and students.**

5. Please confirm our assumption that you mean manage LAN-based IP addresses scheme in reference to 'Where appropriate maintenance and creation of Internet Protocol version 4 and 6 address spaces'? (LAN Administration section, 6th paragraph, Page 10)

Answer: **Yes, LAN-based IP addresses scheme as indicated by the section title "LAN Administration".**

6. Please clarify what you mean by 'the Managed Service Partner shall be responsible for the complete set of associated works in line with Health and Safety requirements'? (Installation/De-Installation section, 1st paragraph, Page 11)

Answer: **The MSP shall comply with the Federal Occupational Safety and Health Act (OSH Act), Pennsylvania state laws/regulations, local laws/regulations, and all areas of workplace health and safety requirements while working onsite at any and all PA Cyber facilities in any working capacity.**

7. Based on the two paragraphs below, will all of your 3rd party carriers (Expedient, carriers, ISPs, etc) be wholly identified and managed by the Managed Service Partner? i.e All PA Cyber 3rd party technology providers will report to the Managed Service Provider and not PA Cyber?

> "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."

Answer: **Work carried out by Third Parties to complete a project or fulfill the obligations and requirements stated in the RFP can be wholly identified and managed by the MSP. For example, the MSP may already have a business relationship, agreement, or alliance with another MSP in the Philadelphia area. In that case, the MSP may independently use that Third Party to carry out a LAN refresh in Philadelphia without consulting or seeking approval from PA Cyber.**

However, long-term service providers and carriers such as (Expedient, AT&T, etc) will be identified by PA Cyber in consultation with the MSP. The MSP will then work directly on behalf of PA Cyber with the service providers and carriers when necessary.

8. Expedient is currently responsible for backup and restore services, as well as you are in the process of moving servers to Expedient for all hosting, will backup and restore services, and hosting, continue to be Expedient's responsibility? If so, what specifically will be the Managed Service Partner's role with respect to these services? (Servers section, 2nd indented paragraph, Page 13)

Answer: **Yes, Expedient currently provides backup and restore services as well as hosting. The MSP will be required to monitor those services daily and work with Expedient to ensure a high level of quality of service and system uptime. The MSP will be required to work with Expedient to address issues, restore data, and move projects forward such as server migrations regularly and as needed.**

9. We assume, excluded from the maintenance requirement 'maintain operating systems to minimize impact of any potential shortcomings' are those servers and applications not currently supported and/or running aged operating systems (i.e. CRM, Great Plains, and BackPack running Windows Server 2003)? (System Hardware Management and Support & System Software Management and Support, Page 14)

Answer: **PA Cyber will aggressively work with the MSP to upgrade, replace, or decommission any system or application with an aged operating system such as Windows Server 2003. Long-term, PA Cyber intends to only maintain operating systems that are current, secure, and supported by Microsoft and other developers. For any operating system that is EOL/EOS such as Windows 2003, the MSP should do what it can (within their control) to minimize the impact of any potential shortcomings.**