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

**FOURTH SET OF RESPONSES TO RFP QUESTIONS**
**March 20, 2017**

1. Reference management following the ITIL process – this is not a discipline we follow internally. Is this a standard you're committed to or can we provide you with options?

**Answer:** **Options can be provided.**

2. The Managed Service Partner shall also ensure that users on the Network are prevented from making malicious attacks on other networks. Can you clarify what you're looking for? I.e. training, software, anti-virus?

**Answer**: **PA Cyber will be responsible for all employee training (e.g. security awareness training) and developing IT policies and procedures. A response may include (but not limited to) the use of software, IT forensics, periodic risk assessments, audit/log reviews, outbound firewall rules-blocking specific ports, packet inspection, IDS, insider threat detection system, and/or malware/phishing detection on inside networks.**

3. The Managed Service Provider shall monitor the Network for any attempted or actual security breaches. Are you requesting ACTIVE monitoring & remediation of firewall intrusions?

**Answer**: **Yes.**

4. After reviewing the RFP, there are two initiatives that would require to be outsourced to a third party, installing network cabling and DBA. Would you be open to utilizing a third party, where they would be fully vetted OR selecting you own service provider and we will manage through our Vendor Liaison Program?

**Answer**: **The MSP is not required to install cabling. The RFP only calls for the MSP to "administer the cable and patch panel management and perform patching to resolve problems or reconfigure the LAN." PA Cyber will use internal staffing resources or a third party to install cabling, patch panels, data jacks, etc.**

**Regarding the DBA and any other service or function that needs to be outsourced, a third party that is fully vetted by the MSP is preferred.**

5. Under the Network Security heading on pg. 10, can additional clarification and/or elaboration be provided re: with whom the MSP will need to co-operate (i.e. relevant parties) as stated in the opening paragraph?

**Answer:** **Relevant parties could include the Beaver Valley Intermediate Unit, Sunesys, AT&T, Mimecast, Dunbar Security, Incapsula, and other software/hardware vendors or service providers.**

6. Can additional detail be provided re: the content next to bullet #7 under System Software Management and Support on pg. 14? Really looking for a more detailed description of PA Cyber's expectation where this service is concerned.

**Answer**: **PA Cyber requires the MSP to apply security patches to server operating systems and ancillary server software including but not limited to MS-Exchange, MS-SQL, anti-virus agents, and backup/Commvault agents regularly, if applicable. Critical security patches should be applied within 24 hrs and other non-critical patches can be applied according to a schedule after approval, testing, or consultation with PA Cyber.**

7. Can additional detail be provided re: the content next to bullets #3 & #4 under System Housekeeping Services on pg. 15? Really looking for a more detailed description of PA Cyber's expectation where these services are concerned.

**Answer**: **The MSP should clearly define a firewall change management plan, test the impact of firewall policy changes, clean up and optimize the firewall rule base, schedule regular firewall security audits, monitor user access to firewalls and control who can modify firewall configurations, update firewall software regularly, and centralize firewall management.**

**The MSP should periodically scan the Network and Servers for vulnerabilities and identify, rank, and report vulnerabilities at least once per quarter or after significant changes are made. Penetration tests should be performed at least once per year and upon significant changes. A manual process the use of automated tools may be proposed. Remediation should be performed immediately or within a reasonable time period.**