Addendum 2 – RFP – 25-003

Required inquiries

1. Please confirm your annual Preliminary Pre-Discount funding Commitment ($)?

   Our preliminary pre-discount commitment amount is $82742.00. This is the full amount that we have to spend over the 3 years of the pilot program. This will be $27580 annually for 3 years.

2. What is the total device count for leadership staff that have PC Workstations, Windows, or MACs (staff with elevated privileges or access to confidential data - e.g. IT, HR, Health, Finance/Payroll departments)?

   Approx. 50

3. What is your total device count for all other Staff?

   Approx. 460

4. What is your total Student device Count?

   Approx. 3240

5. What is the number of computer-based accessories or devices such as interactive smart panels, etc?

   Approx. 150 Interactive boards (Newline and Viewsonic)

6. How many File Servers do you have onsite?

   1

7. How many File Servers do you have hosted offsite?

   0

If you have the ability to provide answers to the above questions, then the following inquiries will help us better tailor our response…

Optional inquiries

1. Are you looking for solutions that you will manage with in-house staff, or would you like a Client-Managed or Fully Managed solution? Would you like quotes for both?

   Prefer Fully-Managed, but will take quotes broken out too.

2. Given that available funds will likely not provide maximum protection for all devices; are you looking to provide some level of security for all devices or are you looking for a solution that provides maximum security for your key devices that would be likely targets for an attack? (Servers, Cloud, Key employees, etc.) – Would you be interested in a quote for both?

Prefer all devices but understand this might cost too much. Willing to take quotes for both options.

3. Should we include the following in our quote to meet your requested services? (yes/no)
    a. Endpoint Detection & Response (EDR) yes
    b. Managed Detection & Response/Managed Security Operations Center (SOC) maybe?
    c. Security Information & Event Monitoring (SIEM) yes
    d. Multi-factor authentication (MFA) no
    e. Network Assessment (Vulnerability Scans) no
    f. Security Awareness Training no
    g. Network Authentication/Network Access Control (Clearpass) no

In addition to what you have requested, we may wish to propose an additional alternative security solution for your consideration. To help us customize that solution, please provide us answers to the following Questions:

1. Do you have Anti-Virus with Endpoint Detection and Response (EDR) capabilities? If you, what solution are you using? Yes – MS Endpoint protection
2. Do you have a Security Information and Event Management (SIEM) solution in place? If you, what solution are you using? no
3. Do you have a Secure Access Service Edge (SASE) solution in place? If you, what solution are you using? no
4. Do you have a 24/7 Managed SOC solution in place? If you, what solution are you using? no
5. Do you have a Data Loss Prevention (DLP) solution in place? If you, what solution are you using? no
6. Do you have a Zero Trust Networking (ZTN) solution in place? If you, what solution are you using? no
7. Do you have an Application Allowlisting/Whitelisting solution in place? If you, what solution are you using? Group policy
8. 8.Do you have an ongoing Vulnerability Assessment solution in place? If you, what solution are you using? CISA and AL Supercomputer
9. Do you have a SASE solution in place? If you, what solution are you using? Repeat of #3
10. Do you have a Password Management solution in place? If you, what solution are you using? no

11. Do you have a Patch Management solution in place? If you, what solution are you using? SCCM for Windows devices

12. Do you have a Disaster Recovery solution in place? If you, what solution are you using?

    DRUVA offsite backup and Quest Rapid Recovery for onsite backups