

Northeast Indiana Works

IT Request for Proposal released on June 23, 2022

Q: Proactive Server Management and Monitoring (service provider) - Installation, configuration, and management of server software. Can you please confirm that that this does not encompass new software applications? What software is currently in place and that the RFP is referring to be installed and configured?

A: Service provider might be required to install/remove applications as the environment changes. This includes, but not limited to installing/uninstalling virus protection, monitoring application and helpdesk software.

Q: Automated weekly and monthly stems status and performance reporting. Reports can be sent to the director of technology - Can you please explain what "Stems" status means?

A: Automated weekly and monthly strategy reporting that should include a summary of current health status, recent asset analysis, and drive utilization.

Q: What backup system/software is currently in place for the NEINW? Will NEINW be open to recommendations to improve backup solution as needed?

A: We have two onsite physical servers and two remote physical servers. We are unable to openly reveal software information due to security concerns. We are always open to learn about new backup tools recommended in the industry.

Q: Does NEINW have a current testing cycle in place and if so, what is that schedule?

A: Data backup reports should be generated from the backup software application and checked regularly. Testing will be required every 3 months.

Q: Can you confirm that any new or replacement firewalls would be considered a project and billed out of scope of service contract.

A: New Firewall configuration will be billable time outside of this contract.

Q: Can you confirm that any new remote users needing VPN access could be considered a project and billable?

A: Current VPN installation and configuration is a 5-minute process. New VPN wide implementation would be a separate project.

Q: Please provide a count of all wireless access points.

A: A total of 12 wireless access points.

Q: Can you confirm the counts and model/descriptions of all network switches in the current infrastructure?

A: 13 Cisco Switches. We are unable to openly reveal all hardware and software components due to security concerns.

Q: Please supply a list of all current software applications, licensing.

A: We are unable to openly reveal software/licensing information due to security concerns.

Q: Can you confirm that the new service provider would maintain the current disaster recovery plan and not the creation of a new recovery plan?

A: Yes. Maintaining current Disaster Recovery Plan.

Q: Can you confirm that NEINW understands that response times for after-hours/off-hours would be considered billable and not covered under contract.

A: Yes. Billable Time.

Q: What general information can you provide about the currently deployed backup solution in terms of the amount of content archived on a nightly basis and what is the desired retention time for that content?

A:

- Local backups every 5 minutes and nightly backup to a data center
- Nightly backup is approximately 1-3 GB
- Amount of content archived is approximately 2TB
- Retention – 2 Years

Q: What is the current backup solution in place today including software vendor and, does this include cloud backup?

A: We have two onsite physical servers and two remote physical servers. We are unable to openly reveal all hardware and software components due to security concerns. No cloud backup.

Q: What Windows server operating system version is deployed on your hosts currently?

A: We are unable to openly share operating system information due to security concerns.

Q: Can you please provide the quantity and type of Microsoft O365 subscriptions in use?

A: 100 accounts. Microsoft 365 Business Standard.

Q: Do you currently have a shared storage or SAN in place today? If so, are you able to provide the manufacturer and model?

A: Only a Dell File Server

Q: How many switches are deployed currently and who is the manufacturer?

A: 13 Cisco Switches

Q: Do you utilize wireless access points at any of your facilities? If so manufacturer/model?

A: Yes, at every facility. A total of 12 wireless access points.

Q: Under the availability section it is being asked for a 2 Hour minimum response time during hours and a 4-hour response time for off hours. With all of our clients we have a 4-hour SLA during working hours, but I will say we generally are responding to tickets within an hour. This does not mean we are fixing or working on the ticket within hour it means that someone from your team will hear from someone from our team within the 4 hours. For critical tickets we have an SLA of 1 hour.

A: Our help desk system receives all of our tickets. Most of them are addressed by us, and we only forward urgent. Every ticket needs to be accepted and assigned within the allotted two to four hours, but that doesn't necessarily mean work has started within that time frame. We are aware that each issue is unique and may call for a different level of expertise handle it. We choose a provider based on a

variety of criteria in addition to this one. To reach a decision, we consider additional characteristics. I believe your requirements and ours on this particular issue are in sync.

Q: Are there any other Cyber Security measures in place other than Proofpoint and Firewalls, like mandatory Security Awareness Training, SIEM or Zero Trust that we need to be aware of?

A:

- Content filtering, machine behavior, and application management are all part of our current virus defense.
- We are unable to openly reveal all our security solutions utilized on our servers/local devices due to security reasons.
- We provide employee training on social engineering and cybersecurity challenges/topics.

Q: Do you currently mandate MFA for every user?

A: MFA implementation is currently underway.

Q: Do you currently have Cyber Security Insurance?

A: We don't have a policy in place.

If yes, can we see the requirements of the policy? n/a

If yes, are you currently in compliance with the policy requirements? n/a

If yes, have you ever had to use it? n/a

Q: Have you ever had a security breach and been ransomed?

A: No

Q: Is there any assessment opportunity of how the systems are setup currently, like Firewalls, Active Directory or VM's? If support, setup, configuration, and troubleshooting are requested to be included in the overall price we would need to know what it looks like before being able to quote pricing to manage these.

A: Due to the nature of our system configuration, evaluation will not be permitted until a provider is chosen.

Q: How often are you expecting data restoration tests to be run? Monthly? With the monthly reports of the backup reports?

A: Data backup reports should be generated from the backup software application and checked regularly. Data restoration testing will need to be conducted on a monthly basis. Testing will be required every 3 months.

Q: Is the bid winner expected to create the Comprehensive Disaster Recovery Plan as part of the monthly flat rate or is this expected to be a separate project cost? In order to create these plans properly takes significant time and input from key stakeholders of your organization as well as our team.

A: No, we have a disaster recovery strategy in place, it must be updated if the environment changes or a new provider is selected to update contact information. Once the service provider is chosen, updates will be carried out by the director of technology.

- **Q:** Follow-up to the above, are there currently any Security Policies in place and if so are they up to date with current Contact Information?
- **A:** We have a policy and it's kept up to date.

Q: Are there any Compliance regulations required? i.e.: HIPPA/PCI

A: No

If yes, are you currently working towards compliance and is this being documented? n/a

If yes, what expectations do you have of your IT Service provider to maintain required Compliance? n/a