Seeking Proposals:

Information Technology (IT) – Cybersecurity and Managed Services

The Denver Preschool Program (DPP) helps Denver fulfill its commitment to its youngest learners. We champion, fund, and increase access to quality preschool across our community. The core of our mission is to make high quality preschool accessible to every Denver preschooler.

To help successfully accomplish this, DPP is seeking proposals from qualified contractors to support DPP in continuing to build its Information Technology (IT) in the form of Cybersecurity and Managed Services.

A. Overview:

Denver Preschool Program Inc. (DPP) seeks proposals from qualified firms, contractors, and agencies to provide Cybersecurity and Managed IT Services support for the organization.

DPP invites individuals, firms or partnership to submit a proposal to DPP for consideration.

B. Submission Period: Thursday, July 11, 2024, through Thursday, August 8, 2024.

No proposals will be accepted after the deadline. Proposals should be emailed to Matt Jordan, CFO/COO, at matt@dpp.org.

C. Background of DPP:

The Denver Preschool Program (DPP), initially approved by voters in November 2006, then renewed and expanded by voters in November 2014 and November 2023, is an independent 501(c)3 created for the purpose of managing the City and County of Denver's dedicated preschool tax. The organization is governed by a Board of Directors appointed by the Mayor of Denver and Denver City Council and comprised of citizens with experience managing businesses, non-profits, and public programs.

More information regarding DPP and the services provided can be found on DPP's website at www.dpp.org.

.

305 Park Ave. West, Ste. B Denver, CO 80205 720.287.5055 303.496.1114 info@dpp.org dpp.org

D. Services Required

As part of the 2023-2025 strategic plan, DPP has a goal to ensure the organization has the infrastructure, staffing and governance to thrive. It is through this goal that DPP is seeking contract services to support the infrastructure of the organization. The Denver Preschool Program is currently a nine (9) member staff working on a hybrid (in-person/remote) schedule with the likelihood to increase in the coming year. All employees primarily use laptops to access Google Workspace and Microsoft Office. Employees use a VPN to gain access to DPP's shared drive while working remotely. Additional information about the organization's current technology is outlined below. Prospective contractors should have extensive experience with implementing cybersecurity & IT managed services and working with hybrid teams.

Notable Current Tech (Not all inclusive):

- Core Hardware
  - Physical Servers: 1
  - Switches/Firewall/Router
  - Laptops: 13 currently, additional devices anticipated
  - WIFI extenders
  - Additional computer monitors
  - TV's in conference rooms
  - Canon Printer
  - Audio & Video Equipment
- Systems & Main Applications
  - Google Workspace and Gmail
  - Microsoft Office
  - QuickBooks Desktop Pro Plus
  - Adobe Creative Cloud
  - Zoom
  - Data backup process happens regularly and is encrypted and stored offsite. Current IT vendor uses a Cloud Backup platform in connection to Synology NAS devices, running automatic backups weekly and running regular manual checks to ensure the process is running correctly. IT vendor utilizes a tool designed by the device vendor to verify backups.
  - Remote support
  - Antivirus

Managed IT Services & Cybersecurity

The Denver Preschool Program needs a prospective Managed Services Provider (MSP) to Manage, maintain, and improve upon its' IT services and cybersecurity practices. Key elements include, but are not limited to:

- **Help Desk Support** – The MSP should offer superior Help Desk support services utilizing industry best practice processes and procedures.

- **Server & Network System Monitoring** – The MSP must provide 24x7 monitoring of DPP's server and network system with proactive communication and escalation protocols based on the severity of any unscheduled outages.
- **Patch Management Services & Preventative Maintenance** – The MSP must provide management of critical security and system patches to all servers and systems on the network to ensure DPP's IT systems and resources are properly managed and maintained.
- **Business Continuity and Disaster Recovery** – The MSP must be able to support DPP's ability to recover based a mutually agreed upon Recovery Time Objective (RTO) and Recovery Point Objective (RPO). In addition, backup and redundancy should be used to support this need.
- **Remote Backup** – The MSP must execute a nightly backup plan for designated servers, including a regularly-tested recovery process.
- **Email System Management** – DPP requires the management and administration of DPP's email system for all users.
- **Antivirus, Antispam, and Antispyware Protection** – DPP is looking for solutions to defend against security threats including phishing, malware, spam, viruses, and ransomware.
- **Onsite Support** – When needed, the MSP should have the ability to deploy onsite resources to assist in issues which cannot be resolved through remote access to in-house systems, having a regular scheduled in-house visit might be needed for regular maintenance and support.
- **Networking Support** – DPP requires proactive management and monitoring of our switches, firewalls, routers, phone, Wi-Fi systems, and other networking equipment.
- **Security Systems Monitoring** – MSP must provide proactive monitoring and management of DPP's security systems, including firewalls, intrusion prevention, secure remote access, and any advanced security solutions MSP utilizes or suggests.
- **Vendor Management** – The MSP should be able to manage other vendors which may be contracted by DPP and serve as the key point of contact unless escalated.
- **Warranty and Asset Inventory Management** – DPP expects the MSP to maintain a hardware and asset inventory that includes Desktops, Laptops, Servers, Printers/Scanners, Fax Machines, and to notify DPP of any potential service or warranty issues. The MSP must also assist with managing the lifecycle of DPP's devices and maintain an equipment inventory to ensure our systems are always functional and current.
- **Software Licensing Control** – The MSP must provide oversight of automatic renewal of software applications and maintenance of appropriate documentation.
- **Procurement Management** – The MSP must assist with the selection of commercially-rated equipment, order placement, order tracking, shipping, equipment returns, sourcing, and ordering of replacement parts.
- **PC Deployment** – The MSP must provide delivery and setup of machines onsite or to staff working remotely.
- **Desktop and Laptop Support** – The MSP must include their ability to support existing and future desktop and laptop hardware. This includes maintenance and repair, replacement for failed equipment, and the acquisition and provisioning for new equipment as needed.

- **Printers, Copiers, and Scanners** – The MSP must be able to support existing printers, copiers, and scanner-related network-printing issues.
- **Desktop Software Standardization and Software Licensing and Upgrades** – The MSP must have a process for identifying standardization and management of desktop images and ensuring that staff are using current products as well as current OS and browser versions.
- **Lifecycle Management of Hardware Units** – The MSP should have processes for end-of-life notification, replacement, and asset decommissioning/disposal.
- **Break Fixes and Installation** – The MSP should offer planned and on-call break/fix services, including emergency response to server issues.
- **Move, Add, Change (MAC)** – DPP is looking for the MSP to help with any changes to the location, configuration of existing equipment or software, and installation of additional equipment or software as needed.
- **Reporting** – The MSP should provide relevant reporting not only based on their performance from a help desk perspective but also regarding system health, uptime, and assist in keeping an accurate hardware inventory to inform ongoing planning of maintenance, warranties, and refresh schedules.
- **Technology Strategy Planning** – The MSP will work with designated DPP staff to develop a strategic technology plan. The plan will take advantage of new and existing technologies to produce a pragmatic and effective roadmap that enables the organization to fulfill its overall mandate, utilizing best-in-class software and tools.
- **Account Management** – The MSP must offer an internal escalation process in tandem with DPP to ensure the ability to have multiple points of contact available if needed depending on the items or issue encountered.
- **Project Management** – The MSP should be able to offer project management and technical engineering resources to assist with technical projects as identified by the MSP or DPP.
- **Solution Design** – The MSP must provide solution packages (e.g., hardware, software, licensing) and associated consolidation of data.
- **Service Levels** – The MSP should identify service-level agreements or objectives and report back on a regular basis to DPP on their ability to meet these agreements or objectives.
- **IT Policy Review and Development** – The MSP should be able to assist in the development of customized policies related to the use of technology.
- **Hosting** – The MSP should offer services relative to hosting or co-location of equipment, either directly or through partners.
- **Onboarding and Offboarding Staff** – The MSP must have process and procedure in place to onboard or offboard team members in a timely and efficient manner.
- **Compliance** – The MSP must use systems that comply with published Payment Card Industry (PCI) Security Standards. In addition, the MSP should support rules and regulations as provided by relevant governing organizations as identified by regulatory or grant-based requirements.
- **Scalability** – The MSP must be able to offer a model where scaling up or down from a system and cost perspective is simple and nimble.

- **Multi-Factor Authentication (MFA)** – The MSP must be able to provide and manage a Multi-Factor Authentication (MFA) solution to provide an easy-to-use method to verify user identities at login, and to protect logins with multi-factor authentication.
- **End-User Security Awareness Training** – The MSP should offer Security Awareness Training to teach DPP's staff and employees about current threats, terms, standards, and compliance to help them avoid a security incident.
- **Vulnerability Testing** – The MSP should offer vulnerability tests, both internally and externally, to determine what flaws and potential threats exist from the outside, or perimeter, of DPP's business network.
- **Managed SOC-as-a-Service** – The MSP should offer a Security Operations Center, Managed SOC-as-a-Service, to monitor DPP's environment and ensure proactive detection and response to threats, intrusions, and attacks.

E. Information to include in Proposal

- Statement of your understanding of the services to be provided to DPP.
- Your experience and qualifications in working with organizations similar to DPP.
- Evidence of your qualifications to provide the above services.
- The size and organizational structure of the firm.
- Proposed fee structure, including guarantees can be given regarding increases in future years, and the maximum fee that would be charged.
- Names of the project lead and any applicable staff who will be assigned to the work and provide biographies.
- Provide references (names and contact information) for similarly sized clients.
- Describe how and why you think you are the best fit for DPP's needs.
- Comment on your firm's efforts towards diversity, equity and inclusion.

Please direct any proposal inquiries to: Matt Jordan, CFO/COO, at matt@dpp.org

F. Evaluation of Proposals

DPP will evaluate proposals on a qualitative basis. This includes our review of the proposal materials, results of discussions with other clients, the completeness and timeliness of responses to us and vendor interviews as necessary.