REQUEST FOR PROPOSAL (RFP)

Managed IT Services Provider (MSP)
City of Powder Springs



Issue Date: Friday, October 16, 2026

BIDS DUE NO LATER THAN: 12:00 noon EST, Wednesday, November 11, 2026

Attn: Candyce James City Clerk

4483 Pineview Drive

Powder Springs GA, 30127

1. Introduction and Project Information

The City of Powder Springs is soliciting sealed proposals from qualified professional IT firms to provide recurring monthly managed IT services for the city. The selected vendor must demonstrate the ability to provide a full suite of network and IT services with an

emphasis on robust cybersecurity solutions aligned with the City's operational requirements and security objectives.

The City requires a comprehensive managed IT and security services solution, including network infrastructure and hardware updates, to ensure optimal performance, protection against evolving cybersecurity threats, and ongoing testing to maintain Cybersecurity Liability Insurance compliance.

The deadline for submission of questions shall be **12:00 noon EST on Friday, October 30, 2026**. All questions shall be submitted to the attention of **Candyce James, City Clerk, at, cjames@powderspringsga.gov**.

Sealed proposals shall be submitted to **The City of Powder Springs, 4483 Pineview Drive, Powder Springs, Georgia 30127**, to the attention of **Candyce James, City Clerk, by no later than 12:00 noon EST on Wednesday, November 11, 2026**. **No proposals will be accepted after the 12:00 noon deadline.**

Vendors shall submit an **original and three (3) copies** of the **proposal along with an electronic copy**.

2. Background

The City of Powder Springs is located in southwest Cobb County and is a member of the ten-county Atlanta Regional Commission. The City is approximately twenty-two miles west of Atlanta and twelve miles southwest of Marietta. Powder Springs encompasses approximately 4,580 acres (7 square miles) with an estimated population of 15,758.

The City emphasizes transparency in local government and easy access to public records. Accordingly, IT systems must support secure operations, data retention, and Open Records Act compliance.

3. Scope of Services

The selected provider will oversee and manage the City's IT network and functions. The following services represent the minimum required support services:

- Comprehensive trouble ticketing (average ~1,200 tickets annually) system with business-hours help desk and after-hours support.
- Unlimited remote and onsite (when needed) support, including emergency response
- Data encryption across systems and endpoints
- Document management and automatic offsite data transfer with backup monitoring
- Business Continuity and Disaster Recovery (BCDR) capabilities
- 24x7 Security Information and Event Management (SIEM) monitoring with expert response team

- Security incident response including isolation, remediation, recovery, and Cyber Incident Response Plan (CIRP) maintenance
- Remote monitoring and management suite licensing and hosting
- Anti-malware and anti-ransomware protection with dark web monitoring
- Managed endpoint prevention, detection, response, and remediation (EDR)
- Managed endpoint domain name security
- Support and maintenance of network drives
- Hardware drive space management
- Microsoft workstation and server security patch management
- Support for third-party software programs
- Secure remote access agent or VPN capabilities
- Security awareness training tools and phishing simulation campaigns
- Microsoft 365 licensing with password management and multi-factor authentication (MFA)
- Managed backup and archiving of Microsoft 365 emails/data with retrieval capabilities for Open Records Act requests
- Firewall management and monitoring
- Switch management and monitoring
- Server management and monitoring
- Wireless LAN controller management and monitoring
- Managed wireless access point services
- Workstation IT management agent deployment and monitoring
- CJIS compliant and capable to handle CJIS environments.

AI:

- Provide AI advisory, planning, implementation, and governance services to help the organization adopt AI securely, responsibly, and effectively.
- Establish AI governance policies, acceptable-use guidelines, and approval processes.
- Implement approved AI solutions, including generative AI, AI assistants, and workflow automation.
    - Ensure human oversight, transparency, accountability, and appropriate use of AI-generated outputs.
- Maintain an inventory of approved AI applications, models, and use cases.

Security:

- 24 x 7 Security Information and Event Monitoring
- 24 x 7 US-based Security Operations Center
- 24 x 7 Security Expert Team on Standby
- AI- based Cybersecurity - Implement and manage security controls to protect AI systems, organizational data, users, and infrastructure against emerging AI-related threats.
- Ongoing administration and management of all cyber tools / services

Provide Active Tools for:

- AI Platform
- Anti-Phishing
- Anti-Malware and Ransomware
- Endpoint Prevention, Detection, Response, and Remediation
- Extended Detection and Response (XDR)
- Click-Time Protection
- Account Takeover Prevention
- Mock-Phishing campaigns to test/educate.
- Dark-web Monitoring & Scanning
- Advanced Cyber Threat Hunting
- Advanced Endpoint Security for desktops and laptops
- AI-enabled End User Endpoint & Mobile Protection

4. Vendor Qualifications

Vendors must demonstrate experience supporting municipal or government entities, strong cybersecurity expertise, relevant industry certifications, and the ability to meet Cybersecurity Liability Insurance requirements.

If Awarded f awarded vender must provide on request proof of: Insurance & Liability,

Insurance minimums:

Worker's Compensation Liability min: $1,000,000

Commercial General Liability min's:

- Each occ: $ 1,000,000
- To rented prem: $ 300,000
- Med exp: $ 10,000
- Personal & adv injury: $ 1,000,000
- General aggregate: $ 2,000,000

Umbrella Liability min's:

- Each occurrence: $ 5,000,000
- Aggregate: $ 5,000,000

If awarded vender must provide on request proof of: FAR and Positive Eligibility, EIN, FEI, STI, Sales Tx & Withholding Numbers, W9,

Include (3) references of current clients including an overview of services provided, contact including full name, phone, and e-mail address.

5. Proposal Requirements

To standardize responses and simplify the comparison and evaluation of responses, all proposals must be organized and submitted in the format listed below. Straightforward, precise, and clear language is preferred over many pages of details and specifications. The City of Powder Springs reserves the right to request further information, contact client references, and require interviews/demonstrations with any responding firm.

Proposals should include the following:

1. Company overview and relevant experience with government entities.
    a. Contact name, address, e-mail address, and phone number
    b. Number of years in business, size of firm (number of employees), and number of technicians available to provide services to the city.
    c. Address of local office from which services will be provided.
2. Detailed description of proposed services and service levels (SLAs)
    a. Cybersecurity framework alignment (e.g., NIST, CIS Controls, CJIS)
    b. Staffing model and escalation procedures, including onsite if needed
3. Transition plan and onboarding timeline
    a. Include discovery timelines and transitional timelines
4. Pricing structure (monthly recurring costs and any one-time fees)
    a. All costs shall remain firm for a minimum of one (1 year) from the date of contract award
    b. Cost will be an objective factor with points assigned using a formula that measures each cost proposal against the lowest compliant cost. (lowest cost receives the maximum available points)
5. References from similar municipal clients
    a. Provide a minimum of three (3) municipal references of similar size and scope where your firm has provided services during the past five (5) years.

    b. Provide a contact person with each reference and their phone number and e-mail address.

6. Evaluation Criteria

Proposals will be evaluated based on:

#	Evaluation Criteria	Points	Weight
1	**Company overview/background and relevant experience with government entities.**	**15**	**15%**
2	**Technical capability and completeness of solution; Responsiveness and support model**	**30**	**30%**

3	**Cybersecurity strength and compliance alignment**	**25**	**25%**
4	**Cost-effectiveness and value**	**20**	**20%**
5	**References and past performance**	**15**	**15%**
	Total	**100**	**100%**

7. Timeline

Event	**Date**
RFP Released	**10/16/2026**
Questions Due from Vendors	**12:00 Noon EST on 10/30/2026**
Proposal Submission Deadline	**12:00 Noon EST on 11/11/2026**
Vendor Interviews	**TBD**
Vendor Selection	**TBD**
Service Start Date	**TBD**

The deadline for submission of questions shall be **12:00 noon EST on Friday, October 30, 2026**. All questions shall be submitted to the attention of **Candyce James, City Clerk, at, cjames@powderspringsga.gov**.

Sealed proposals shall be submitted to **The City of Powder Springs, 4483 Pineview Drive, Powder Springs, Georgia 30127, to the attention of Candyce James, City Clerk, by no later than 12:00 noon EST on Wednesday, November 11, 2026**. **No proposals will be accepted after the 12:00 noon deadline.**

Vendors shall submit **an original and three (3) copies** of the proposal **along with an electronic copy**.

8. Terms and Conditions

- The City reserves the right to reject any or all proposals.
- All responses become public record under Georgia Open Records laws.
- The selected vendor must enter into a service agreement including confidentiality, data security, and insurance provisions.
- The City is not responsible for proposal preparation or submission costs
- The City, at its discretion, may extend the agreement for up to four (4) additional periods of one (1) year each if agreeable to both parties.