Town of Atlantic Beach
717 30th Avenue South
Atlantic Beach, SC 29582
Mailing Address: PO Box 5285
North Myrtle Beach, SC 29597
Phone: 843 663-2284 Fax: 843-663-0601

MANAGED IT SERVICES FOR TOWN HALL & CJIS-CONNECTED POLICE DEPARTMENT

Issue Date: January 30, 2026
Proposal Due Date & Time: February 27, 2026 (12:00PM Eastern Time)
Issuing Agency: Town of Atlantic Beach, SC
Procurement / RFP Contact: Carnisha Hennigan
Email: chennigan@townofatlanticbeachsc.com
Phone: 843-663-2284
Submission Method: Electronic submission (PDF) via email: chennigan@townofatlanticbeachsc.com or in-person to the Town Hall.
Anticipated Contract Term: One (1) year with up to two (2) one-year renewal options (at the Town's discretion)

---

1. PURPOSE

The Town of Atlantic Beach, South Carolina is soliciting proposals from qualified firms to provide Managed IT Services for Town Hall and the Atlantic Beach Police Department, including support for a CJIS-connected environment.

The Town intends to award a contract to the Offeror whose proposal is determined to be the **best value** and most advantageous to the Town, considering technical approach, CJIS capability, experience, service quality, and cost. Competitive sealed proposals are an accepted procurement method under South Carolina procurement law where sealed bidding is not practicable or advantageous.

---

2. BACKGROUND & CURRENT ENVIRONMENT (SUMMARY)

2.1 Overview

Town operations include municipal administration and public safety. The Town requires stable, secure technology operations and timely vendor response to support essential services.

2.2 Size of Environment (for proposal assumptions)

The Town estimates **12–15 total users/devices** combined across Town Hall and the Police Department.

The Town environment includes (or may include):

- Windows-based workstations and laptops
- Business-class network infrastructure (firewall, switches, Wi-Fi)
- Email and productivity suite (e.g., Microsoft 365)
- Police Department systems and vendors (CAD/RMS, evidence systems, etc.)
- Backup and recovery systems
- Security tools (endpoint protection, filtering, etc.)

Important: The Police Department is **CJIS connected**, and the selected Offeror must be capable of supporting CJIS-related security and operational requirements. (Law Enforcement)

---

3. SCOPE OF WORK

The selected Offeror shall provide all labor, tools, and expertise needed to deliver the services described below.

3.1 Core Managed IT Services

A. Help Desk & End-User Support

- Provide support **Monday–Friday, [8:00 AM–5:00 PM]**, excluding Town holidays
- Remote support plus onsite support as required
- Resolve issues involving workstations/laptops, printers, email, file access, software
- Support onboarding/offboarding, password resets, device setup, and account management
- Maintain a ticketing system with measurable SLA reporting

B. Infrastructure & Network Management

- Monitor and manage firewall, switching, wireless, VPN, and ISP connectivity
- Patch management and updates for endpoints and servers (if applicable)
- Manage backup systems and conduct scheduled restore tests
- Maintain documentation: network diagrams, inventories, configurations, credentials vault approach
- Vendor coordination and escalation (ISP, copier vendor, software vendors)

C. Cybersecurity Services (Minimum Requirements)

- Endpoint protection/EDR management (recommended)
- Security patching and vulnerability management
- MFA implementation and maintenance for admin accounts and remote access
- Secure configuration baselines (workstations, servers, network devices)
- Email security protections (filtering, phishing controls)
- Security incident response assistance and reporting (see Section 6)

D. Police Department & CJIS Environment Support

Offeror must provide support for a CJIS-connected Police Department, including:

- Network segmentation and access controls appropriate for CJIS systems
- Administration support for CJIS-related workstations and secure access methods
- Evidence and CJ systems support as allowed by vendor contracts
- Coordination with CJIS Systems Officer (CSO) / Agency IT contact and applicable state CJIS authority
- Support for CJIS compliance practices (training, auditing readiness, documentation)

(Note: The Town/PD will define which systems are vendor-managed by the OEM and which are managed by the IT service provider.)

E. Strategic IT & Governance Support

- Quarterly technology planning meeting with Town leadership
- Annual lifecycle recommendations for devices and network equipment
- Budget planning support for IT improvements
- Change management recommendations for CJIS-related changes

---

4. DELIVERABLES & REPORTING

4.1 Transition / Onboarding Deliverables (First 30–60 Days)

Offeror shall provide:

1. **Transition plan and kickoff meeting** within five (5) business days of Notice to Proceed
2. **Comprehensive inventory** of devices, software, licenses, and warranties
3. **Baseline documentation package**, including:
    - Network diagram(s)
    - Key configuration summaries
    - Admin access matrix
    - Backup summary
4. **Cybersecurity baseline assessment** and prioritized remediation plan
5. **CJIS support approach** (access controls, segmentation, incident response coordination)

4.2 Ongoing Deliverables

- Monthly report (Town Hall + PD) including:
    - Ticket volumes, trends, and root causes
    - SLA performance results
    - Patch compliance and vulnerability status
    - Security alerts and incident summary
    - Recommendations and risks
- Quarterly review meeting minutes and action plan

---

5. SERVICE LEVEL REQUIREMENTS (SLAs)

Offerors must meet or exceed the following minimum SLAs:

Priority	Definition	Response Time	Target Time to Restore/Resolve
P1	PD outage, CJIS-impacting incident, ransomware suspected, major network outage	15 minutes	4 hours (restore or workaround)
P2	Significant disruption to Town Hall or PD operations	1 hour	1 business day
P3	Standard single-user issue	4 business hours	3 business days
P4	Service request, minor issue, planned work	1 business day	Scheduled

After-Hours Coverage: Offeror must provide on-call support for Police Department P1 incidents outside normal business hours, including weekends/holidays.

---

6. SECURITY, CONFIDENTIALITY & CJIS COMPLIANCE

6.1 Confidentiality

The Offeror shall maintain confidentiality of all Town and Police Department information, including criminal justice information (CJI), and shall not disclose any protected information without written authorization, except as required by law.

6.2 CJIS Compliance Requirements (Mandatory)

Because the Police Department is CJIS connected, Offeror must demonstrate the ability to comply with the **FBI CJIS Security Policy**, including but not limited to:

- Access control and least privilege
- Secure authentication and MFA for privileged access
- Encryption for CJI where applicable
- System and activity logging
- Incident response coordination
- Secure remote access methods (Law Enforcement)

6.3 Personnel Security / Background Screening

Offeror must describe how it meets CJIS personnel security requirements for any employee/contractor who will access CJIS systems, CJI, or secure Police Department areas. This may include fingerprint-based background checks and CJIS security awareness training as required by CJIS policy and CJIS Systems Agency requirements. (Law Enforcement)

6.4 Security Incident Reporting

Offeror must notify the Town and Police Department within **one (1) hour** of discovering any suspected or confirmed security incident involving Town or Police Department systems,

including any incident impacting CJI, and support incident response actions and evidence preservation consistent with CJIS standards. (Law Enforcement)

---

7. PRICING REQUIREMENTS

Offerors shall provide clear and transparent pricing using one of the following:

- **Flat monthly managed services fee** (preferred) plus hourly rates for projects, or
- A hybrid approach with included hours and defined overage rates

Pricing must include:

- One-time onboarding/transition costs
- Monthly recurring costs
- Included services and exclusions
- Hourly project rates by role
- After-hours and emergency rates (if not included)
- Travel / onsite visit assumptions

---

8. OFFEROR QUALIFICATIONS

Offerors must demonstrate:

- Experience supporting small municipalities or comparable public-sector entities
- Experience supporting police departments and CJIS-connected environments
- Ability to provide onsite support within 24 hours as needed
- Strong cybersecurity practices and tools
- Documented approach to patching, backups, and vulnerability remediation
- Ability to maintain and protect administrative credentials and sensitive documentation

Offerors must provide **three (3) references**, including at least **one (1) law enforcement or CJIS-related** reference if available.

---

9. PROPOSAL SUBMISSION REQUIREMENTS

9.1 Proposal Format

Proposals must be organized as follows:

1. Cover Letter (signed)
2. Executive Summary
3. Company Profile & Qualifications
4. Relevant Experience & References
5. Technical Approach & Work Plan
6. Staffing Plan (roles, resumes, key personnel)

7. Security & CJIS Compliance Approach
8. Transition Plan (first 30–60 days)
9. SLA Commitment and Support Model
10. Cost Proposal
11. Exceptions (if any)

9.2 Submission Instructions

Submit proposals electronically as a single PDF file to:
chennigan@townofatlanticbeachsc.com

Subject line: **RFP Managed IT Services – [Offeror Name]**

Late proposals may be rejected.

---

10. SOUTH CAROLINA PUBLIC RECORDS / FOIA NOTICE

Offerors are advised that proposal submissions may be subject to disclosure under the **South Carolina Freedom of Information Act (FOIA)**. Offerors should clearly mark any portion of the proposal they contend is exempt from disclosure and provide justification; however, the Town makes no guarantee of confidentiality and will respond to records requests as required by law.

---

11. Award Method

The Town intends to award to the Offeror whose proposal is determined to provide the best value. The Town may conduct interviews, request additional information, and negotiate final terms consistent with South Carolina procurement practices.

---

12. TERMS, CONDITIONS & RESERVATION OF RIGHTS

The Town reserves the right to:

- Reject any or all proposals
- Waive informalities and minor irregularities
- Request clarification or additional information
- Conduct negotiations with one or more Offerors
- Cancel or reissue the RFP
- Award in whole or in part

APPENDIX A — REQUIRED OFFEROR RESPONSES (QUESTIONNAIRE)

Offerors must answer the following:

1. Describe your experience supporting municipalities and small government agencies.
2. Describe your experience supporting CJIS-connected police departments.
3. Describe your help desk process, tools, ticketing system, and escalation model.
4. Describe your cybersecurity toolset (RMM, EDR/MDR, logging/monitoring, backup).
5. Describe how you meet CJIS personnel screening and training requirements for staff. (Law Enforcement)
6. Describe your incident response approach and your one-hour notification process. (Law Enforcement)
7. Provide a 30–60 day transition plan and onboarding timeline.
8. Explain how you handle patching, vulnerability remediation, and reporting.
9. Confirm ability to provide after-hours emergency PD support and specify your on-call process.
10. Provide at least three references (including at least one law enforcement or CJIS-related reference if available).

APPENDIX B — COST PROPOSAL TEMPLATE

1) One-Time Fees

- Transition & onboarding: $_____
- Documentation & baseline assessment: $_____
- Security hardening (initial): $_____

2) Monthly Managed Services (12–15 users/devices total)

- Total monthly fee: $_____
  Includes (check all included):
- ☐ Unlimited remote support
- ☐ Onsite support (define frequency): _____
- ☐ Patch management
- ☐ Backup monitoring
- ☐ Security monitoring / MDR
- ☐ Vulnerability scanning
- ☐ M365 administration (if applicable)

3) Hourly Rates (Non-Included / Project Work)

- Project Manager: $____/hr
- Senior Engineer: $____/hr
- Engineer: $____/hr
- Technician: $____/hr

4) After-Hours Emergency Support (PD P1)

- Included? ☐ Yes ☐ No
- After-hours rate: $____/hr
- Minimum charge (if any): $____

5) Optional Services

- MDR (Managed Detection & Response): $____/month
- Security awareness training/phishing: $____/month
- Annual IR tabletop exercise: $____
- Penetration testing coordination: $____

APPENDIX C — MINIMUM REQUIRED INSURANCE (SAMPLE)

Offeror shall maintain:

- General Liability: $1,000,000 per occurrence / $2,000,000 aggregate
- Professional Liability (E&O): $1,000,000
- Cyber Liability: $1,000,000
- Workers' Compensation: Statutory