

COMPUTER SUPPORT TECHNICIAN

Reports To: Computer Support Administrator

Supervises Directly: N/A

Pay Grade: 57

FLSA Status: Non-Exempt

Salary Range: \$29.54 to \$48.48 hourly, depending on qualifications and experience

Closing Date: August 7, 2026



Position Summary

Responsible for installing, configuring, maintaining, securing, and troubleshooting the Authority's desktop computers, laptops, mobile devices, printers, peripherals, operating systems, and business applications. Provides advanced end-user support, performs preventive maintenance, manages endpoint deployments, and helps ensure reliable and secure access to technology resources. Requires independent judgment and a high degree of coordination with administrators, managers, operations personnel, vendors, and customers.

Essential Duties and Responsibilities

The following duties are normal for this position. The omission of specific statements of duties does not exclude them from the classification if the work is similar, related, or a logical assignment. Other duties may be required and assigned.

Endpoint Support

- Provide advanced support for desktop computers, laptops, tablets, smartphones, printers, scanners, docking stations, monitors, peripherals, operating systems, and business applications.
- Diagnose, troubleshoot, and resolve complex hardware, software, performance, printing, connectivity, authentication, and user-profile issues; escalate and coordinate vendor support when necessary.
- Install, image, configure, deploy, upgrade, patch, repair, and replace computers, peripherals, internal components, operating systems, drivers, and approved software.
- Perform hands-on hardware diagnostics and repair, including component replacement, BIOS/firmware updates, warranty coordination, and post-repair testing.
- Manage endpoint configuration and software distribution using approved deployment, patch-management, remote-support, and endpoint-management tools.
- Administer mobile device management (MDM) platforms, including enrollment, configuration profiles, application deployment, security policies, compliance monitoring, remote support, and device retirement or wipe procedures.
- Support mobile email, multifactor authentication, VPN client software, and secure access to organizational applications and data.
- Respond to service requests and incidents through telephone, remote, and email communication; prioritize work, communicate status and resolution clearly, and provide user training as needed.
- Identify recurring endpoint problems, determine root causes, and recommend standardized fixes, replacement strategies, or procedural improvements.
- Evaluate and recommend hardware, software, and support solutions that improve reliability, security, and user productivity.

Documentation & Inventory

- Record incidents, service requests, troubleshooting steps, resolutions, system changes, and recurring problems in the designated tracking system.
- Create and maintain workstation standards, equipment configurations, installation procedures, knowledge-base articles, operational manuals, and user instructions.
- Maintain accurate inventories and lifecycle records for computers, software, licenses, warranties, peripherals, mobile devices, and assigned assets.
- Manage printers, print services, and printer supplies, and coordinate repair or replacement as needed.
- Assist with technology procurement, equipment standards, license compliance, asset disposal, and replacement planning.

Endpoint Systems & Connectivity

- Troubleshoot endpoint network connectivity, including wired and wireless connections, IP configuration, DNS resolution, VPN client access, and access to shared resources; escalate infrastructure issues to the appropriate administrator or service provider.
- Support Microsoft 365, directory services, file and print services, cloud applications, endpoint-management tools, and other user-facing systems within assigned permissions.
- Apply endpoint security controls, including operating-system and application patching, endpoint protection, encryption, multifactor authentication, screen-lock policies, and approved access controls.
- Monitor endpoint health and compliance, investigate alerts, remediate workstation and mobile-device vulnerabilities, and report suspected security incidents promptly.
- Test new hardware, software, updates, and configuration changes before deployment; document results and minimize disruption to users.
- Coordinate with software vendors, hardware manufacturers, managed service providers, and contractors to resolve endpoint issues and complete support projects; assist users with file recovery and approved backup or synchronization tools in accordance with established data-protection procedures.
- Maintain approved content on the Authority's website and support IT department projects, endpoint deployments, office moves, and continuous-improvement initiatives.
- Provide scheduled after-hours support for endpoint deployments, maintenance, urgent user-impacting incidents, or special projects when required.

Safety

- Use safety equipment provided by the Authority; follow all safety rules.
- Notify supervisor of unsafe equipment, missing safety equipment, or unsafe conditions.

Knowledge, Skills, and Abilities

- Advanced knowledge of desktop and laptop hardware, internal components, peripherals, Windows operating systems, drivers, user profiles, and common enterprise applications.
- Strong hands-on ability to diagnose, repair, configure, image, deploy, upgrade, and maintain computers and related equipment.
- Advanced troubleshooting skills for Microsoft 365 applications, browsers, printing, file access, authentication, performance, software installation, operating-system errors, and hardware failures.
- Working knowledge of Active Directory or similar directory services, Microsoft 365, cloud applications, user-account administration, endpoint-management platforms, and remote-support tools.
- Working knowledge of network concepts, including TCP/IP configuration, DNS, DHCP, wired and wireless access, VPN, RDP, SSH, SD-WAN, NAT, and other network protocols and standards.
- Knowledge of mobile device management concepts and platforms, including enrollment, configuration, iOS, application distribution, compliance, security, and remote support.
- Knowledge of endpoint security principles and controls, including least privilege, multifactor authentication, patch management, endpoint protection, encryption, secure configuration, and incident reporting.
- Ability to use remote-support, ticketing, inventory, software-deployment, scripting, and command-line tools to support endpoints and resolve technical problems.
- Strong analytical and troubleshooting skills, including the ability to isolate faults, determine root causes, document findings, and restore service efficiently.

- Ability to plan and implement changes, manage multiple priorities, meet deadlines, and work independently with minimal supervision while contributing effectively to a team.
- Ability to communicate technical information clearly to both technical and nontechnical audiences and to provide effective instruction and customer service.
- Ability to prepare clear technical reports, procedures, knowledge-base articles, recommendations, correspondence, and operational documentation.
- Ability to handle confidential information and maintain reliable, secure, and accurate systems and records.

Physical and Work Requirements

- Inside work environment (approximately 75% or more of the time inside).
- Lifting up to 50 lbs.; occasional walking, standing, reaching, handling, fingering, and feeling.
- Requires seeing and hearing.

Core Competencies

- Mathematical ability sufficient to add, subtract, multiply, and divide.
- Developed language/literacy skills: read and comprehend English instructions, policy manuals, memos, letters, rules, and regulations.
- Ability to understand and carry out complex written and oral instructions; work with speed and accuracy.

Minimum Qualifications

- Associate's degree in information technology, computer science, information systems, or a related field.
- Current or recent endpoint-support certifications such as CompTIA A+, Network +, CCST Networking.
- A minimum of four (4) years of current hands-on, progressively responsible experience providing computer and end-user technical support in a business environment.
- Demonstrated hands-on experience diagnosing, repairing, configuring, imaging, deploying, upgrading, and supporting desktop computers, laptops, operating systems, applications, user profiles, printers, and peripheral equipment.
- Demonstrated experience troubleshooting Windows, Microsoft 365 applications, hardware failures, software installation, printing, authentication, performance, wired and wireless connectivity, and VPN client issues.
- Experience administering or supporting a mobile device management platform and applying device security and compliance policies.
- Experience using ticketing, remote-support, endpoint-management, patching, software-deployment, and inventory tools.
- Ability to perform scheduled after-hours endpoint maintenance or deployments and respond to urgent user-impacting incidents when required.
- Basic understanding of networking and network terminology
- Valid Florida Driver's License and the ability to travel between Authority locations as needed.
- Ability to make decisions in accordance with departmental rules, regulations, security requirements, and policies.
- Ability to establish and maintain effective working relationships with employees, vendors, contractors, and the public.
- An equivalent combination of education, relevant certifications, training, and experience may be considered, provided the candidate demonstrates the required hands-on technical competencies.

Preferred Qualifications

- Bachelor's degree in information technology, computer science, information systems, or a related field.
- Over six (6) years of current hands-on, progressively responsible experience providing computer and network support in a business environment.
- Associate-level skills to support the network.
- Current or recent endpoint-support certifications such as CompTIA A+, Network+, CCST Networking, CCNA, Microsoft 365 Certified: Endpoint Administrator Associate, or equivalent.
- Experience with Microsoft 365, Entra ID, Active Directory, Windows 11, endpoint management, application packaging or deployment, and cloud-based services.

- Experience supporting Microsoft Intune or another enterprise mobile device and endpoint management platform.
- Experience providing PC support in a multi-site government, utilities, critical-infrastructure, or similarly regulated environment.
- Experience in network troubleshooting. Solid understanding of DHCP, VPN, VLANs, SD-WAN, and other essential network services.

Additional Qualifying Factors:

As a condition of employment, must pass a pre-employment drug screening, physical, as well as have acceptable reference and background check results.

Seacoast Utility Authority is an Equal Opportunity Employer. In compliance with the Americans with Disabilities Act, the Authority will provide reasonable accommodations to qualified individuals with disabilities and encourages both prospective and current employees to discuss potential accommodations with the employer.