

Job Description

Provides technical support and troubleshooting to network; desktop; and/or systems hardware and software.

1. Screens; refers and diagnoses internal inquiries and work requests as they relate to maintenance of personal computers and related systems.
2. Installs; configures; and upgrades computer hardware and software.
3. Provides end-user software troubleshooting and support.
4. Applies diagnostic techniques to identify problems; investigate causes; and recommend solutions.
5. Provides troubleshooting and support.
6. Assists in the administration of e-mail systems.
7. Provides phone and help-desk support for local and off-site users.
8. Maintains current knowledge of relevant technologies as assigned.
9. Participates in special projects as required.

Contract requires:

Provide onsite 24x7 coverage of basic help desk support tasks using the customer enclave referred to as the IIS. Perform intermediate skill level tasks in coordination with and supporting customer personnel performing advanced skill level network security tasks.

Perform Client Support Technician (CST) tasks on basic level functions such as answering user calls and logging user/system problems in the provided ticketing system; resetting passwords; basic system trouble shooting; and updating user online information.

Intermediate level tasks will provide support for Vulnerability Management Systems (VMS); Assured Compliance Assessment Solution (ACAS); Host Based Security System (HBSS); and server backups. All tasks will be entered into the provided ticketing system.

Provide basic and intermediate level CST support for users with accounts on NIPRNet; SIPRNet; and JWICS domains.

TECHNICAL HELP DESK & ENCLAVE SECURITY SUPPORT SENIOR

Provide basic and intermediate level CST support for users for SIPRNet Web portal accounts and deployable secure IIS equipment connectivity accounts; such as Global Rapid Response Intelligence Package (GRRIP) user accounts.

Support SIPRNet and JWICS domain VTC suites in customer workspaces to include VTC system operations check; initial system troubleshooting; and basic VTC operation assistance for customer personnel. Coordinate with VTC schedulers and distant end users as required.

Install and maintain IIS computers and enclave infrastructure equipment. Tasks include physical movements; preventative maintenance; and network fiber installation.

Provide support for the Secure Entry Point (SEP) which provides secure reach back for GRRIP systems. Monitor SEP server operation 24x7; perform initial troubleshooting and apply corrective actions in the event of a SEP outage; assist remote users attempting to connect to the SEP; assist users in connecting to backup SEP as required; assist users with GRRIP operations. Notify customer personnel if advanced skills are required to correct the problem.

Perform weekly retina vulnerability scans; importing scan results into VMS and acknowledging identified vulnerabilities in VMS. Identify corrective actions for the identified vulnerabilities. Complete required DISA online training prior to performing these tasks.

Perform weekly ACAS scans and identify vulnerabilities; research corrective actions and provide feedback to customer personnel. Complete DISA required online training prior to performing these tasks.

Check DISA website weekly for Secure Configuration Compliance Validation Initiative (SCCVI) and Fragmentary Orders (FRAGO) updates and load the newest version on network servers.

Load updated versions of HBSS as required; monitor the Host Intrusions Prevention System (HIPS) and create exceptions to allow the system to function properly. Administer policy auditor to ensure compliance with mandates; load McAfee client software to servers and workstations and download new version of client software to install on stand-alone systems. Complete DISA required online training prior to performing these tasks.

Perform routine server backups as scheduled by customer personnel.

Document shift activity in the provided tracking system by the end of their duty shift to include customer calls; trouble tickets (with #s) initiated during the shift and trouble tickets closed during the shift; and assigned tasks performed or completed. Enter user/system problems into the provided tracking system within one hour of problem identification and process tickets per provided guidance within two hours of problem resolution or by the end of each duty shift.

-Perform basic CST tasks.

- Answer user calls; log user information in provided ticketing system.

TECHNICAL HELP DESK & ENCLAVE SECURITY SUPPORT SENIOR

- Determine user system issue by analyzing symptoms & identifying underlying problem.
 - Reset user passwords.
 - Update user online information.
 - Build/update/unlock/delete user SIPRNet accounts.
 - Build/update/ unlock/delete user GRRIP accounts.
 - Build/update/ unlock/delete user Service Manager accounts.
 - Build/update/ unlock/delete Organization box/Distro List accounts.
 - Build/update/ unlock/delete user SIPRNet Web Portal accounts.
 - Coordinate with ESD to build/update/repair/delete user SIPRNet accounts.
- Coordinate with ESD to build/update/repair/delete organizational SIPRNet accounts.
 - Coordinate with users on process to repair/replace SIPRNet Token cards.
 - Update user Information Assurance training dates.
- Image and install workstations; update printer configuration; map network drives.
 - Install/update software on user workstations.
 - Inventory COMSEC materials (each shift).
 - Explain to Senior Leaders their mobile handheld device functions.
- Diagnosing CAC/Token issues; provide POC information for resolution.
- Train users in diagnosing Outlook Web Access (OWA); Virtual Private Network (VPN) Wireless access accounts & issues.
- Support users with Microsoft Office; Defense Connect Online program questions/issues.
 - Support users with replacement of laser printer toner cartridges.
- Initiate Classified Message Incident (CMI) checklist and notify Security Manager.
 - Facilitate operation of SIPRNet and JWICS VTC suites for online meetings.
 - Troubleshooting and fixing software; hardware or network issues.

TECHNICAL HELP DESK & ENCLAVE SECURITY SUPPORT SENIOR

- Configuring workstations; servers and other hardware.
 - Perform diagnostic testing.
- Maintain remote control tools used to assist users remotely.
 - Install or replace various hardware components.
 - Install/update Antivirus files for HBSS.
- Load updated versions of HBSS as required; monitor the Host Intrusions Prevention System (HIPS) and create exceptions to allow the system to function properly.
- Monitor and update VMX and respond to Information Assurance Vulnerability Alert (IAVA) messages.
 - Setup user work areas during contingency operations .
 - Maintain correct EMSEC procedures and equipment layout.
 - Monitor and apply DISA STIGs.
 - Perform and monitor system backups.
 - Perform weekly SnapShot backups of virtual servers.
- Coordinate with vendors to determine cause/develop resolution of software/hardware malfunctions.
- Manually check servers once a shift (24x7) to ensure they are functioning correctly and have the latest security patches.
 - Monitor SEP server to ensure it is fully functioning; assist remote users to facilitate connectivity; perform troubleshooting checklist; notify Government personnel if advanced skills are required.
- Perform weekly retina scans; import into VMS; and acknowledge identified vulnerabilities in VMS. Perform this task in ACAS when network transitions from VMS to ACAS.
- Perform weekly ACAS scans and acknowledge vulnerabilities; research fix action and provide feedback to customer personnel.
- Check the DISA website weekly for Secure Configuration Compliance Validation Initiative (SCCVI) and Fragmentary Orders (FRAGO) updates and load the newest version on our network servers.

TECHNICAL HELP DESK & ENCLAVE SECURITY SUPPORT SENIOR

Education

Associates Degree in a related technical discipline; or the equivalent combination of education; technical certifications or training; or work experience.

Qualifications

3-5 years of directly related experience supporting help desk operations. Experience supporting equipment and systems specified in the Job Responsibilities section is highly desired.

Shall have a minimum of Information Assurance Technical (IAT) II level Department of Defense (DoD) 8570 certification.