ADDENDUM 4.0 – SERVICE EXTENSION

This is an addendum to the Service Level Agreement dated April 7, 2014 to reflect the recent request for adjusted services. Quest will provide the services (as defined below) to Davis Joint Unified School District (Client). The new term of service(s) will commence at the new monthly rate, per Addendum 4.0, for all services noted below. Addendum 4.0 will supersede all previous listed services prior to this Addendum. In the event the terms and conditions expressly set forth in this Addendum conflicts with the original SLA, including previous Addenda, this Addendum's terms and conditions shall supersede the conflicting terms and conditions.

SERVICE TERM: November 1, 2020 through October 31, 2023

1. **Service Summary**

   Quest will provide the following services to Client. The scope of service relating to the items are as follows:

   1.1 IaaS - Provided Virtual Compute and Storage

   1.1.1 Quest will provide the following virtual resources to support Client's virtual servers.

   1.1.1.1 72 vCPU, 432 GB vRAM, 14 TB SATA storage, 1 TB SSD storage

   1.1.2 Client, at their own expense and separate from this Agreement, will procure and maintain any Operating System (OS) and Application licensing. Quest is not providing nor maintaining any licensing on the dedicated servers to Client. Client shall be liable and responsible to follow all vendor licensing terms and conditions where applicable.

   1.1.2.1 Furthermore, Client assumes full responsibility for Microsoft licensing along with the responsibility for licensing any other products not noted as provided by Quest in this Agreement.

   1.1.3 Quest will provide 24 x 7 real-time monitoring and notification of backend hardware for performance, errors, stability, and utilization.

   1.1.3.1 Troubleshooting and/or remediation of hardware platform is included. Troubleshooting or remediation of all other issues will be performed per the technical support rates.

1.1.4 Upon Client request, configuration changes to the platform requested on behalf of the Client will facilitate through the Quest Network Operations Center for processing.

1.1.4.1 Requested changes are billable per the technical support rates.

1.1.5 Upon Client notice and no more than once per quarter, Quest will be available for review of hypervisor updates on provided platform. Quest will review and provide a recommendation on the necessity/urgency of the update.

1.1.5.1 Release of update is determined by the manufacturer.

1.1.5.2 Client and Quest will document the firmware update process and maintenance window upon commencement of the services or shortly thereafter. Both parties must agree on the patching process prior to implementation of service.

1.1.5.3 Installation of minor point releases (5.1.X to 5.1.XX) are included as part of service. Major revision updates or updates for new/additional functionality are not included but can be done under a separate billable project.

1.1.6 Quest will retain and reclaim provided services upon service termination.

1.1.7 Quest is responsible for maintaining an active support contract on the provided software during the term of the agreement, unless vendor releases End of Life of product life cycle at which time Quest may present options to Client for service adjustment. If Client declines options or does not respond back in an appropriate amount of time, Quest's support of end of life environment will be best effort and per the technical support rates thereafter, which shall supersede any previous or then documented understanding.

1.1.8 If Client fails to respond or provide direction, Quest reserves the right to adjust/filter alert/thresholds notifications to Client so long as Quest notifies Client of its intention to do so due to misconfiguration or ongoing event the Client is experiencing which may cause an interruption to Quest's notification service.

1.2 Backup as a Service – Primary Target

1.2.1 Quest will provide one (1) local backup target and backup software with 20 TBs of usable storage space.

1.2.2 Quest will maintain backend platform, including platform updates, patches, hot fixes for the duration of the Agreement.

1.2.3 Quest will perform troubleshooting and remediation of backup infrastructure (hardware and platform software) issues as part of service.

1.2.3.1 If the failure or issue is outside of backup infrastructure, engagement of Quest resources will be billable per the technical support rates.

1.2.3.2 Client may troubleshoot failed backup/replication jobs or Quest resources can assist, billable per the technical support rates.

1.2.4 Quest will monitor and alert 24 x 7 on up to twenty (20) named backup/replication jobs with the following understanding:

1.2.4.1 Quest will notify Client of any failed job

1.2.4.2 Quest will perform initial triage of failed job, to include restarting the failed job as part of the service.

1.2.4.3 If restart of job fails, Quest will investigate and provide Client with recommendations on how to remediate. Engagement of remediation may be billable depending on the nature of the effort and will be discussed with Client prior to proceeding forward.

1.2.4.4 During service onboarding/implementation, Client will provide Quest with documented named list of jobs for this service. Any adjustments (add, removals) to this list must be accompanied by an executed Addendum between both parties.

1.2.5 Storage overages will be based on peak monthly usage.

1.2.6 Upon Client request, configuration changes to the platform requested on behalf of the Client will facilitate through the Quest Network Operations Center for processing.

1.2.6.1 Requested changes are billable per the technical support rates.

1.2.6.2 Quest will retain direct access to backup infrastructure for duration of service. Client will retain access to backup and Client data. If Client requests access to backend platform, a separate service clarification addendum will need to be executed to document roles and responsibilities.

1.2.7 Client is responsible for verifying, communicating, and notifying Quest of all data (drives, servers, VMs, etc.) that require to be backed up.

1.2.8 Client is responsible for providing a list of assets to backup and to notify the Quest Network Operations Center for moves, adds, or changes to backup jobs or additions.

1.2.9 Client is responsible for backup policies and retention policies of backups.

1.2.10 DR Testing is outside of scope of this SLA, but is available via optional services offered by Quest.

1.2.11 Data restoration or disaster recovery services will be billable per the technical support rates at time of request.

1.2.12 Upon expiration or termination of this Agreement, Quest retains all hardware/software.

1.3 Backup as a Service – Secondary Target

1.3.1 Quest will provide a single 25 TB off-site for Clients Veeam Cloud Connect BaaS Target to Client.

1.3.2 Target will be hosted out of the Quest data center located in U.S. Western region.

1.3.3 Quest will provide Client with up to 100 Mbps of ingress bandwidth as part of service. Service also includes two (2) data streams as part of service.

1.3.3.1 Greater speeds are available with Premium WAN option (pricing based on desired speed)

1.3.3.2 Additional data streams are available for additional fees

1.3.3.3 WAN accelerator licensing are available for additional fees

1.3.4 Storage overages will be made available up to 2 TB and billed at the rate of $25.00 per TB. Storage overages will be based on peak monthly usage.

1.3.5 Quest on behalf of Client is responsible for keeping and maintaining Veeam encryption keys, which encode and decode initial data blocks or underlying keys in the key hierarchy. Failure to maintain these keys may result in the inability to restore data. Except as provided by Client, Quest will not have access to any encryption key. These encryption keys include:

1.3.5.1 Session key, meta key, storage key, user key, enterprise manager keys, backup server keys

1.3.5.2 More information on encryption keys can be found on Veeam's support portal.

1.3.6 Client understands that engagement of Quest for restoring the environment from cloud backup files is a best-effort service and acknowledges that Quest is not responsible for any performance degradation, multiple data copies, loss of data, bandwidth limitations or errors on the restored environment as the success of the restoration or the data at rest depends on the reliability of the backup.

1.4 Backup as a Service - Recycle Bin

1.4.1 As included with the BaaS offering, Quest will provide the Veeam Recycle Bin service, configured for 5 days max retention, to Client.

1.4.2 Quest is not liable for data moved to recycle bin nor responsible for restoration if data is moved to the recycle bin.

1.5 Backup as a Service – Protected Storage Target

1.5.1 Quest will provide a single off-site protected storage target to Client with capacity up to 25 TB.

1.5.2 The object lock period is 30 days plus 10 days. This offering does not apply to the Office 365 Cloud Backup service

1.5.3 Upon expiration of the object lock period, data may be altered/deleted.

1.5.4 Client must have, buy or rent a Veeam license compatible with immutable storage.

1.5.5 The Veeam repository must be setup as a Scale Out Repository to support immutable storage.

1.5.6 Quest will utilize the Veeam Cloud Connect secondary copies to create the immutable storage copy of the backups. This will be a one-to-one replica of the Veeam Cloud Connect Secondary copies.

1.5.7 Client understands that engagement of Quest for restoring the environment from cloud backup files is a best-effort service and acknowledges that Quest is not responsible for any performance degradation, multiple data copies, loss of data, bandwidth limitations or errors on the restored environment as the success of the restoration or the data at rest depends on the reliability of the backup.

1.6 Disaster Recovery as a Service – Provided Virtual Firewall w-VPN

1.6.1 Quest will provision one (1) virtual firewall context to Client.

1.6.1.1 Service includes up to five (5) site-to-site VPN licenses. Additional fees apply if Client exceeds licensing. VPN overages above the noted quantity will be assessed at the end of each month and will be invoiced as actuals at a rate of $10.00 per VPN.

1.6.2 Client is responsible for all monitoring, management, configuration, and troubleshooting on provisioned virtual firewall.

1.6.3 Upon Client request, configuration changes to the platform requested on behalf of the Client will facilitate through the Quest Network Operations Center for processing.

1.6.3.1 Requested changes will be billed at the technical support rates.

1.6.4 Troubleshooting and/or remediation of issues will be billable per the technical support rates.

1.6.5 Client is responsible for patching virtual firewall.

1.6.6 Quest will retain hardware/software at the end of the agreement term.

1.7 Cloud Connect DRaaS Reserved Instance

1.7.1 Quest will provide a single 25 TB off-site for Clients Veeam Cloud Connect DRaaS Target to Client.

1.7.2 Quest will provide Client with the following services upon activation or declaration of an event:

1.7.2.1 Quantity 18 virtual machines

1.7.2.2 Quantity 72 vCPU

1.7.2.3 Quantity 432 vRAM GB

1.7.3 Quest will provide Reserved Instances at the Quest data center located in the U.S. Western region.

1.7.4 Quest will provide Client with up to 100 Mbps of ingress bandwidth as part of service.

1.7.5 Storage overages will be made available up to 2 TB and billed at the rate of $125.00 per TB. Storage overages will be based on peak monthly usage.

1.7.6 In the event of a declaration or usage of the environment, Client will be assessed a daily fee based upon contracted amount of Reserved Instances services.

1.7.6.1 Client will be charged usage fees per calendar day if services are activated.

1.7.6.2 The current daily burst rate, per provisioned compute above, is $348.40 per day. Additional fees will apply for additional compute, storage, or connectivity if requested/required.

1.7.7 Reserved Instances provides compute reservations so that you can have assurance in your ability to run the instances you have reserved when you need them. In a declared disaster or Client requested usage of environment, Reserved Instances will be provided on request and if available.

1.7.8 Client will be provided one (1) scheduled Disaster Recovery Test annually. DR test must be coordinated and scheduled with a minimum of five (5) business days' notice by Client to Quest.

1.7.8.1 Troubleshooting, remediation, DR runbook, or other policy creation is not included but available per the technical support rates.

1.7.8.2 Per day usage fees will apply if Client goes beyond one day during DR test.

1.7.8.3 Quest reserves the right to postpone scheduled DR test for up to thirty (30) days, if necessary.

1.7.9 Client is responsible for configuration management, service monitoring, and alert remediation once services are turned-up or activated.

1.7.10 Client is responsible for defining DR processes and maintaining and creating a runbook for initiating and managing a DR event and/or testing.

1.7.11 Client is responsible for software/application configuration and troubleshooting. Upon request, Quest can engage at a billable time and materials rate.

1.7.12 Version upgrades and changes to platform are available per the technical support rates.

1.7.13 Customization of service is available per Client request per the technical support rates. Additional fees may apply.

1.7.14 Client understands that engagement of Quest for restoring the environment from cloud backup files is a best-effort service and acknowledges that Quest is not responsible for any performance degradation, multiple data copies, loss of data, bandwidth limitations or errors on the restored environment as the success of the restoration or the data at rest depends on the reliability of the backup.

1.8 Infrastructure Monitoring – Provided HA Firewalls w-IDS-IPS

1.8.1 Quest will provision two (2) virtual firewalls with IPSEC VPN capability at the Quest BRC, McClellan, CA.

1.8.2 Quest will provide 24/7 real-time monitoring and notification of assets via SNMP statistics for performance, errors, stability, and utilization.

1.8.3 Quest will provision IDS/IPS event monitoring and alerting.

1.8.3.1 SEIM/log correlation and retention services are not provisioned at this time. Upon Client request, Quest can provide these services.

1.8.3.2 Client is responsible for defining security policies and firewall rule sets. Quest has requested the security policies necessary to ensure configuration

tasks are carried out in a way that are acceptable to Client and within their established policy. At this time, Quest does not possess a copy of Client's firewall security policy. If provided by Client, Quest would like to review it against the current firewall configurations to ensure compliance. Quest can also engage with Client to draft such a policy. Until Client provides security policy requirements to Quest, Client authorizes and is responsible for the following support handling approach.

1.8.3.3 For non-immediate IDS/IPS threats, Quest will continue to notify Client when an event occurs and await Client direction before taking action.

1.8.3.4 For immediate IDS/IPS threats, Quest is authorized to take action without Client direction if Client is not immediately available. In such a case, Quest may implement ACLs and filters as needed, short of actually shutting down Internet or services. Those would require Client approval. As such, there could be unforeseen impacts to production or connectivity.

1.8.3.5 Quest will inform and update Client regarding changes being made.

1.8.4 Client will follow Quest Change Management Procedure for services defined in this addendum. Changes requested or on behalf of Client will be billable per the technical support rates. Quest will retain direct access to asset(s) in line with Quest Change Management Procedure.

1.8.5 Troubleshooting and/or remediation of provided hardware/iOS (non-configuration) is included. Troubleshooting and/or remediation of all other issues will be billable per the technical support rates.

1.8.6 Quest will maintain a recent configuration backup remotely from the device with notification from the Client that the configuration has changed. Client is responsible for configuration policy.

1.8.7 Quest conducts logical/physical access reviews of the underlying hosting platform periodically, as well as annually, as part of its SSAE16 audit. Upon Client request, Quest can add service to perform similar access reviews of the systems and applications under Client control. Upon Client notice, Quest will be available for

review of Firmware/iOS updates on contracted asset(s). Quest will review and provide recommendation on the necessity/urgency of the update. Implementation of update(s) may be billable based on the nature of the update.

1.8.8 Threat monitoring services are not included, but can be added to service upon Client request.

1.8.9 Quest retains ownership of hardware and support contracts related to the technology provided within the services listed.

1.9 Infrastructure Monitoring – Provided Load Balancer

1.9.1 Quest will provision one (1) load balancer on a shared platform for Client's public-facing websites per the following specific list.

1.9.1.1 208.67.177.123

1.9.1.1.1 parentportal.djusd.net

1.9.1.1.2 preenroll.djusd.net

1.9.1.1.3 q.djusd.net

1.9.1.1.4 qconnect.djusd.net

1.9.1.1.5 qloader.djusd.net

1.9.1.1.6 qsummer.djusd.net

1.9.1.1.7 qtraining.djusd.net

1.9.1.1.8 studentportal.djusd.net

1.9.1.2 208.67.177.106

1.9.1.2.1 qwebapi.djusd.net

1.9.2 Quest will provide 24/7 monitoring and alerts on the back-end infrastructure and hardware failure. Quest will remediate hardware or component failure(s) for provided infrastructure

1.9.3 Quest retains ownership of the hardware and support contracts related to the technology provided within the services listed.

1.9.4 Changes requested or on behalf of Client will be billable per the technical support rates.

1.9.5 Troubleshooting and/or remediation of issues will be billable per the technical support rates.

1.9.6 Quest will maintain a recent configuration backup.

1.10 Infrastructure Monitoring – Client Virtual Servers

1.10.1 Quest will provide 24/7 alerting of asset(s) for performance, errors, stability, and utilization for up to 20 virtual servers.

1.10.2 Troubleshooting and/or remediation will be billable per the technical support rates.

1.10.3 Client is responsible for SQL/application monitoring.

1.10.4 Client will provide Windows Server OS and application licensing.

1.11 Infrastructure Patching Services - Servers

1.11.1 Quest will apply Windows Operating System and basic third-party application patch updates on up to 17 Client servers.

1.11.1.1 During service onboarding, Quest and Client will define patching protocol for service. Both parties will agree to patching process prior to initiation of service.

1.11.1.2 Application patch list is subject to prior approval by Quest for service inclusion.

1.11.1.3 Client and Quest will define and document process for adding/removing devices from patching service during onboarding.

1.11.2 Client is responsible to validate services/applications on workstations post deployment of automated patch. Upon Client request, Quest is available for review or troubleshooting. Engagement of Quest may be billable per the technical support rates depending on the nature of the issue or resolution.

1.11.3 Quest will notify Client of failed or issued patch/update

1.11.3.1 For third-party, non-Microsoft applications, if necessary and requested by Client, Quest can investigate failed patches billable per the technical support rates.

1.11.4 Quest will utilize its Change Management policy for this service offering.

1.11.5 Client is responsible for patching policy and schedule. Schedule of patching, number of workstations per patch window, is subject to approval by Quest. Quest reserves the right to adjust or change requested patching maintenance at any time.

1.11.6 Additional patches, outside of the once per month schedule, can be applied throughout the month and would be done under a ticket/project, per the following understanding.

1.11.6.1 Automated push of Zero day or Microsoft critical security patches are applied as needed and per the above understanding at no incremental cost.

1.11.6.2 Manual push or intervention, including package manipulation, onsite hands, screen share sessions, is outside of scope and billable per the technical support rates.

1.11.7 Any manual push of or installation of updates is considered outside of scope and billable per the technical support rates.

1.11.8 Client is responsible for maintaining current maintenance/license and support contracts on the provided hardware/software.

1.11.9 If Client fails to respond or provide direction, Quest reserves the right to adjust/filter alert/thresholds notifications to Client so long as Quest notifies Client of its intention to do so due to misconfiguration or ongoing event the Client is experiencing which may cause an interruption to Quest's notification service.

1.11.10 Items not included in this service include but are not limited to

1.11.10.1 Software, hardware, support contracts

1.11.10.2 Regulatory compliance

1.12 Infrastructure Patching – Client Network

1.12.1 Quest will provide the following services up to twice per year for up to 225 Client switches and up to three (3) Client wireless LAN controllers.

1.12.2 Review current patch level for Client contract switches (2k, 3k, and 4k) and wireless controllers.

1.12.3 Review current published patch available from Cisco.

1.12.4 Provide feedback to Client on necessity of deploying patch to Client's environment.

1.12.5 If Client wants to push patch:

1.12.5.1 Quest/Client coordinate patch windows to push patch.

1.12.5.2 Quest confirms patch applies successfully and switch is available to ping.

1.12.5.3 Client confirms service functionality.

1.12.6 If Client declines patch, close out ticket and no patchwork and wait until next review.

1.12.7 Upon Client request, monitoring services can be added via addendum.

1.13 Scanning Service – Quarterly Vulnerability

1.13.1 Quest will provide quarterly vulnerability scans for up to nine (9) IP addresses as pre-defined by the Client.

1.13.2 The Client will receive comprehensive vulnerability report details of all known system vulnerabilities and quarterly review session with Quest representative.

1.13.3 Includes scanning appliance installed on inside of Client's network.

1.13.4 Troubleshooting and/or remediation of related issues is available upon Client request, billable per the technical support rates.

1.13.5 Ad hoc scanning service can be provided at $35/IP address per event.

1.14 Co-location Service – Internet Bandwidth

1.14.1 Quest will provide 100 Mbps of fixed internet bandwidth at the Quest BRC, McClellan, CA.

1.14.2 Quest will provision up to eight (8) public IPs for Client use.

1.14.3 Quest will provide two (2) cross connects for Client's private circuit connectivity at the Quest BRC, McClellan, CA. Client is responsible for telecommunications contracts on private circuit.

1.15 Distributed Denial-of-Service (DDoS) Protection Service

1.15.1 Quest will provide 24/7 real-time internet threat intelligence for mitigation and service protection from volumetric and application-layer DDoS attacks.

1.15.2 DDoS Mitigation Service provides real-time scanning of the Client's Quest provided IP address space and returns clean traffic to the Client.

1.15.3 Automatic analysis of internet traffic with re-routing of attacks through a cleansing center to remove threats.

1.15.4 Protection Service has a minimum of 10 Mbps (Base) billing fee.

1.15.4.1 Overages/usage beyond the base rate will be billed and paid by the Client at a rate of $20.00 per Mbps based on the 95th percentile billed monthly.

1.15.5 Client acknowledges that the DDoS Protection Service may not successfully mitigate all attacks and may also result in some legitimate traffic being filtered from Client's website(s). Quest may discontinue the DDoS Protection Service at any time by giving reasonable advance notice if Quest determines, in its sole discretion, that the website(s), domains, or IP addresses for which Client has requested the DDoS Protection Service pose an undue risk to the Quest Network or other Clients.

1.15.6 Client will provide via existing contract with Quest or their own Internet Services. Additional cross connections, including additional fees, may be necessary or required depending on the chosen migration/configuration path Client moves forward with during implementation.

1.16 Application Monitoring Service – O365

1.16.1 Quest will provide 24/7 application monitoring and alerting for services, faults, mail queue, and performance.

1.16.2 Changes requested or on behalf of Client will be billable per the technical support rates.

1.16.3 Troubleshooting and/or remediation will be billable per the technical support rates.

1.16.4 Client is responsible for application and Active Directory management.

1.16.5 Client will provide application licensing.

1.16.6 Client is responsible for roll-ups, minor updates, and all non-OS patching.

1.16.7 Client is responsible for Architecture and Active Directory Policy.

1.16.8 Client is responsible for licensing of Microsoft O365 services.

1.17 Service Provisioning

1.17.1 Quest will perform the following service provisioning adjustments as noted herein on a time and material basis as noted in Section 2.

1.17.2 BaaS – Primary Target

1.17.2.1 Quest will increase existing primary vault capacity to 20 TB.

1.17.3 BaaS – Secondary Target

1.17.3.1 Quest will increase existing sencodary valut capacity up to 25 TB.

1.17.4 BaaS - Protected Storage

1.17.4.1 Quest will provision new capacity up to 25 TB.

1.17.4.2 Client to specify which VMs to configure.

1.17.5 BaaS - Recycle Bin

1.17.5.1 Quest will provision new capacity up to 25 TB.

1.17.5.2 Client to specify which VMs to configure.

1.17.6 Monitoring Client Virtual Servers

1.17.6.1 Quest will increase existing quantity up to 20.

1.17.6.2 Client to specify which VMs to configure.

1.17.7 OS Patching Client Virtual Servers

1.17.7.1 Quest will increase quantity up to 17.

1.17.7.2 Client to specify which VMs to configure.

1.17.8 DDoS Mitigation

1.17.8.1 Quest will provision service protection.

2. Investment and Terms:

The following table identifies Client's investment for the service package.

Quest Select Service Package	Term	New Monthly Charges
Selected Service Package (Services listed in Section 1)	36 Months	$9,349.00/Month
DRaaS Burst/Activate Fee - Daily Per services provisioned in Section 1.5	As-Needed	$348.40/Day
Provisioning Service Per items noted in Section 1.17	NRC	Time and Material

2.1 All fees are in US Dollars.

2.2 The fees noted herein will replace the previous servie fee and will commence under its own thirty-six (36) month term.

2.3 Incident Response, data and/or application migration services are available upon request for an additional fee/cost.

2.4 In addition to the amounts set forth above, any technical support provided by Quest in connection with the services shall be billed by Quest on a time and materials basis pursuant to the rate schedule. (See Appendix A)

Accepted and Agreed to By:

CLIENT	**QUEST**
Signature: Amari Watkins	**Signature:** _____
Name: Amari Watkins	**Name:** _____
Title: Associate Superintendent of Business Services	**Title:** _____
Date: 10/26/2020	**Date:** _____

Quest Representative:

Name: Andrew Samms

Email: andrew_samms@questsys.com

Mail: 9000 Foothills Blvd., Suite 100
Roseville, CA 95747

Phone: 916-338-7070

Quest Representative:

Name: Dave Montano

Email: dave_montano@questsys.com

Mail: 9000 Foothills Blvd., Suite 100
Roseville, CA 95747

Phone: 916-338-7070

Quest Representative:

Name: Chris Freitag

Email: chris_freitag@questsys.com

Mail: 9000 Foothills Blvd., Suite 100
Roseville, CA 95747

Phone: 916-338-7070

Once signed, please fax or email the signed document to Managed Service Contracts at 916-344-5924 or QMSinstall@questsys.com. Upon receipt, Quest's authorized representative shall execute the Addendum and return a fully executed Addendum, including all exhibits, to Client for their files.

APPENDIX A – TECHNICAL SUPPORT RATE SCHEDULE

Remote (Quest NOC) Support (billed in 15-minute increments)	
Cable Plant at Quest Data Center	$85 per hr.
Desktop/Printer	$85 per hr.
Project Coordinator	$95 per hr.
Video Surveillance, Access Control	$110 per hr.
Audio/Video, Video Conferencing	$110 per hr.
Router, Switch, Server, or Storage	$185 per hr.
Program or Project Manager	$155 per hr.
SQL, .NET, SharePoint	$210 per hr.
VoIP, Firewall, Security, Mobility, VMware, or Citrix	$210 per hr.
DevOps/SSO/Orchestration Engineer	$225 per hr.
Security Incident Emergency Response Resource	$275 per hr.
On-Site Scheduled Support (4 hr. min, scheduled 24 hrs. in advance)	
Data Cabling	$95 per hr.
Desktop/Printer	$90 per hr.
Project Coordinator	$100 per hr.
Video Surveillance, Access Control	$125 per hr.
Audio/Video, Video Conferencing	$125 per hr.
Router, Switch, Server, or Storage	$195 per hr.
Program or Project Manager	$160 per hr.
SQL, .NET, SharePoint	$225 per hr.
VoIP, Firewall, Security, Mobility, VMware, or Citrix	$225 per hr.
DevOps/SSO/Orchestration Engineer	$250 per hr.
Security Incident Emergency Response Resource	$275 per hr.
After Hours Technical Support (4 hr. min, less than 24 hr. notice and/or after hrs./weekends)	
Data Cabling	$110 per hr.
Desktop/Printer	$130 per hr.
Video Surveillance, Access Control	$150 per hr.
Audio/Video, Video Conferencing	$175 per hr.
Router, Switch, Server, or Storage	$230 per hr.
SQL, .NET, SharePoint	$275 per hr.
VoIP, Firewall, Security, Mobility, VMware, or Citrix	$275 per hr.
DevOps/SSO/Orchestration Engineer	$295 per hr.

- Emergency Incident Response Services - billed per hour with minimum amounts determined at time of incident:
    - Immediate response to threat
    - Assess your security posture against the threat
    - Determine the level of effort required to protect Client assets
    - Work to prevent, detect, and respond to incidents
    - Identify and mitigate complex security vulnerability
    - Provide risk analyses and recommendations for threat eradication
    - Provide forensic analysis to determine extract threat vector
- Rates listed above exclude Professional Service engagement(s) and/or project(s) and are subject to rates listed in any separate engagement documents. Please contact the Quest account manager, technical consultant, or service manager for engineering rates that may fall outside of listed engineering services.
- Quest reserves the right to adjust technical support rates.