CONTRACT NAME: AGREEMENT BETWEEN QUEST TECHNOLOGY MANAGEMENT AND DAVIS JOINT UNIFIED SCHOOL DISTRICT

BRIEF DESCRIPTION OF PLAN: This agreement is an addendum to the Service Level Agreement dated April 7, 2014, to reflect DJUSD's request to extend existing, additional and adjusted services. The term of this extension is July 1, 2018 through June 30, 2021.

FISCAL IMPACT: This extension includes a one-time cost of $12,000, and monthly ongoing charges of $10,665, representing a reduction of $3,100 per month. These costs are included in the Instructional Technology budget.

ADDENDUM 3.0 – Service **EXTENSION**

This is an addendum to the Service Level Agreement dated April 7, 2014 to reflect the recent request to extend existing, additional or adjusted services. As such, Quest will provide the services (as defined below) to Davis Joint Unified School District (Client).

SERVICE TERM: July 1, 2018 through June 30, 2021

1. Addendum Service Summary

Quest will provide the following existing, additional or adjusted services to Client. The scope of service relating to the existing, additional and adjusted 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

1.2 BaaS – Primary Veeam Target

1.2.1 Quest will provide 15 TB of raw local backup storage at the Quest BRC, McClellan, CA. Overages will be billed at $25/month per TB.

1.2.2 Quest will retain ownership of all software and licensing for provided solution.

1.2.3 Quest will maintain the back end infrastructure and validate solution connectivity.

1.2.4 Quest will monitor backup jobs and remediate job failure(s) if they occur.

1.2.4.1 Troubleshooting/remediation of backup job failures within the scheduled backup window are included as part of the service.

1.2.4.2 Troubleshooting/remediation of failure events caused by misconfigureation or Client platform issues, will be billable per the technical support rates.

1.2.5 Troubleshooting/remediation outside of job failure(s) will be billable per the technical support rates.

1.2.6 Client is responsible for providing current lists of assets to backup and local retention policies.

1.2.7 Client is responsible to notify Quest of a new server/data to backup or monitor for job failure(s).

1.2.8 Client is responsible for determining backup policies and retentions.

1.2.9 Restoration of data will be billable per the technical support rates.

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

1.3 BaaS - Veeam Cloud Connect Target

1.3.1 Quest will provide a single 15 TB off-site for Clients Veeam Cloud Connect BaaS Target to Client. Storage overages above the noted storage quantity, per TB, will be assessed at the end of each month and will be invoiced as actuals at a rate of $9.00/TB per month.

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 is available for additional fees.

1.3.4 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. Quest does not have access to any encryption key. These encryption keys include:

1.3.4.1 Session key, meta key, storage key, user key, enterprise manager keys, backup server keys.

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

1.3.5 Engagement of Quest resulting from upgrades to the Veeam Cloud Connect software will be billed per the technical support rates.

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, multipule 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.

1.3.7 Recommended minimal requirements:

1.3.7.1 Veeam Enterprise Suite (latest published edition).

1.3.7.2 Recommended bandwidth: 1 Mbps for each 300 GB of data.

1.3.7.3 One useable public IP for outbound communication.

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

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

1.4.1.1 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.

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

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

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

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

1.4.5 Client is responsible for patching virtual firewall.

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

1.5 Disaster Recovery as a Service - Provided Veeam Cloud Connect Reserved Instance

1.5.1 Quest will provide a single 20 TB off-site for Clients Veeam Cloud Connect DRaaS Target to Client. Storage overages above the noted storage quantity, per TB, will be assessed at the end of each month and will be invoiced as actuals at a rate of $91.00/TB per month.

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

1.5.2.1 Quantity 18 virtual machines

1.5.2.2 Quantity 72 vCPU

1.5.2.3 Quantity 432 vRAM GB

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

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

1.5.5 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.

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

1.5.5.2 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.

1.5.5.3 In the event of a declaration, Client can utilize any unused balance of the included seven (7) burst days a year.

1.5.6 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.

1.5.7 Client will be provided seven (7) burst days per year included for the purposes of Disaster Recovery (DR) and scheduled DR tests. DR test must be coordinated and scheduled with a 72-hour notice.

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

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

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

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

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

1.5.13 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, multipule 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.

1.5.13.1 Configuration, troubleshooting, or remediation of firewall/VPN routing, communication, traffic classification, QoS, throughput

1.5.13.2 Disaster Recovery runbook

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

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

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

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

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

1.6.3.2 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.

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

1.6.3.4 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.

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

1.6.4 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.

1.6.5 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.

1.6.6 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.

1.6.7 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.

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

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

1.7 Infrastructure Monitoring – Provided Load Balancer

1.7.1 Quest will provision one (1) load balancer on a shared platform for Client's public-facing website.

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

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

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

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

1.7.6 Quest will maintain a recent configuration backup.

1.8 Infrastructure Monitoring and OS Patching – Client Virtual Servers

1.8.1 Quest will provide 24 x 7 alerting of asset(s) for performance, errors, stability, and utilization for up to (16) virtual servers.

1.8.2 Quest will implement OS Patches for up to 15 Windows Server OS (monthly basis on critical patches as defined by vendor). Manufacturer will determine the release of updates. Quest and Client will define a patch maintenance window and process during installation of services.

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

1.8.4 Client is responsible for SQL/application monitoring and management.

1.8.5 Client will provide Windows Server OS and application licensing.

1.9 Infrastructure Patching – Client Network

1.9.1 Quest will provide the following services up to twice per year for up to 220 Client switches and up to three Client wireless LAN conrollers.

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

1.9.3 Review current published patch available from Cisco.

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

1.9.5 If Client wants to push patch:

1.9.5.1 Quest/Client coordinate patch windows to push patch.

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

1.9.5.3 Client confirms service functionality.

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

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

1.10 Scanning Service – Quarterly Vulnerability

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

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

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

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

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

1.11 Co-location Service – Internet Bandwidth

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

1.11.2 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.

1.12 Co-location Service – Rack Space and Power

1.12.1 Quest will provision rack space for two (2) 1U Barracuda 300 Spam Firewalls at the Quest BRC, McClellan, CA.

1.12.2 Quest will provision 120V-20A (A+B) redundant power circuits at the Quest BRC, McClellan, CA.

1.12.3 Quest will provision two (2) cross connections at the Quest BRC, McClellan, CA.

1.12.4 Client will utilize existing internet connectivity for access to Client equipment.

1.12.5 Client will not have direct access to non-dedicated rack space environment. Remote hands support will be billable per the technical support rates.

1.13 Load Balancing Service – Barracuda Spam Filter

1.13.1 Quest will provision load balancing for two (2) Client provided Barracuda 300 Spam Firewalls at the Quest BRC, McClellan, CA.

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

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

1.13.4 Implementation and/or requested changes on behalf of Client will be billable per the technical support rates.

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

1.13.6 Quest will maintain recent configuration backup(s).

1.14 Application Monitoring Service – O365

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

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

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

1.14.4 Client is responsible for application and Active Directory management.

1.14.5 Client will provide application licensing.

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

1.14.7 Client is responsible for Architecture and Active Directory Policy.

1.15 Provisioning Services

1.15.1 Virtual compute and storage.

1.15.1.1 Quest will provision cloud target.

1.15.1.2 Quest will email Client with credentials for access.

1.15.2 BaaS Cloud Target.

1.15.2.1 Quest will provision cloud target.

1.15.2.2 Quest will email Client with credentials for access.

1.15.3 DRaaS Virtual Firewall Context.

1.15.3.1 Quest will provision firewall context with Client provided information.

1.15.3.2 Quest will email Client with credentials for access and management.

1.15.4 DRaaS Cloud Target Reserved Instance.

1.15.4.1 Quest will provision cloud reserved instance target.

1.15.4.2 Quest will email Client with credentials for access.

1.15.5 Co-location Service

1.15.5.1 Provision 100M bps of fixed internet bandwidth

1.15.6 Items that fall outside the included setup service, that may be performed by Quest if requested, on a time and material basis per the technical support rates, include but are not limited to the following:

1.15.6.1 Veeam enterprise console configuration.

1.15.6.2 Veeam backup and replication configuration or troubleshooting.

1.15.6.3 Data seed configuration, troubleshooting, and remediation.

1.15.6.4 Data speed transfer troubleshooting or remediation.

1.15.6.5 Configuration of Virtual Machines, migration to newly provision IaaS environment.

1.15.6.6 Firewall policy review.

1.15.6.7 Configuration of DRaaS environment.

2. Investment and Terms:

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

Quest Select Service Package	Term	Charges
Selected Service Package (Services listed in Section 1)	36 Months	$10,665/ Month
DRaaS Burst/Activate Fee - Daily Per services provisioned in Section 1.5	As-Needed	$348.40/Day
Target Provisioning Service Per services noted in Section 1.15	NRC	Included
Setup Services – Separate SOW to be provided for Migration Scope	-	$12,000.00/ Onetime

2.1 All fees are in US Dollars.

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

2.3 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: _____	**Signature:** _____
Name: _____	**Name:** _____
Title: _____	**Title:** _____
Date: _____	**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	$75 per hr.
Desktop/Printer	$78 per hr.
Video Surveillance, Access Control	$95 per hr.
Audio/Video, Video Conferencing	$95 per hr.
Network, IaaS, Server, or Storage	$150 per hr.
Program or Project Manager	$140 per hr.
SQL, .NET, SharePoint	$180 per hr.
VoIP, Security, Mobility, VMware, or Citrix	$180 per hr.
DevOps/SSO/Orchestration Engineer	$210 per hr.
Incident Response Resource	$350 per hr.
On-Site Scheduled Support (4 hr. min, scheduled 24 hrs. in advance)	
Data Cabling	$90 per hr.
Desktop/Printer	$85 per hr.
Video Surveillance, Access Control	$98 per hr.
Audio/Video, Video Conferencing	$98 per hr.
Network, IaaS, Server, or Storage	$175 per hr.
Program or Project Manager	$145 per hr.
SQL, .NET, SharePoint	$195 per hr.
VoIP, Security, Mobility, VMware, or Citrix	$195 per hr.
DevOps/SSO/Orchestration Engineer	$210 per hr.
Incident Response Resource	$350 per hr.
After Hours Technical Support (4 hr. min, less than 24 hr. notice and/or after hrs./weekends)	
Data Cabling	$95 per hr.
Desktop/Printer	$125 per hr.
Video Surveillance, Access Control	$135 per hr.
Audio/Video, Video Conferencing	$150 per hr.
Network, IaaS, Server, or Storage	$210 per hr.
SQL, .NET, SharePoint	$250 per hr.
VoIP, Security, Mobility, VMware, or Citrix	$250 per hr.
DevOps/SSO/Orchestration Engineer	$285 per hr.

- Emergency Incident Response Services: $350/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.