STATEMENT OF WORK

Project Name:	MDUSD - Assured Data Protection	**Seller Representative:** Jeff Mitchell +1 (847) 4656000 jeffmit@cdw.com
Customer Name:	MT DIABLO UNIFIED SCHOOL DISTRICT	
CDW Affiliate:	CDW Government LLC	
Subcontractor:	Assured DP	**Solution Architect:** Matt Ingenito John Harbour
Date:	January 15, 2025	
Drafted By	Michelle Caron	

This statement of work ("**Statement of Work**" or "**SOW**") is made and entered into on the last date that this SOW is fully executed as set forth below ("**SOW Effective Date**") by and between the undersigned, CDW Government LLC ("**Provider**," and "**Seller**,") and MT DIABLO UNIFIED SCHOOL DISTRICT ("**Customer**," and "**Client**,").

This SOW shall be governed by that certain Sourcewell Vendor Agreement 071321#CDW between CDW Government LLC and Sourcewell effective November 13, 2021 (the "**Agreement**") If there is a conflict between this SOW and the Agreement, then the Agreement will control, except as expressly amended in this SOW by specific reference to the Agreement.

PROJECT DESCRIPTION

PROJECT SCOPE

The Seller Data Protection and Retention Servicescovered by this Statement of Work includes the following services listed in Sections 1 and 2 below ("Services"), which are subject to the Grant of License and Use of Appliance and Services provisions in Sections 3 and 4:

1. One-time Enrollment and Implementation Services
2. Recurring Data Protection and Retention Services
3. Grant of License
4. Use of Appliance and Services

1. One-time Enrollment and Implementation Services

A. Project Kick-Off Meeting

Sellerwill begin with a project kick-off meeting with the Customer's enrollment project team. The kick-off meeting will include:

- Introductions of Customer and Seller team members

- Review of Customer's organization and project objectives
- Review ofData Protection and Retention Services
- Create a design plan/completion of Site Survey
- Create project schedule

B. **Planning & Design**

Planning and Design Workshop

This session is a meeting with the key members of the Customer's organization including business and technical stakeholders as well as the project team. The discussions will focus on the current environment and processes and the identification of business and technical requirements for Data Protection and Retention. Any requirements outside the scope of this Statement of Work that cannot be met will be identified. Seller and Customer will together develop timelines for an anticipated schedule ("Anticipated Schedule") based on Seller's project management methodology. Any dates, deadlines, timelines or schedules contained in the Anticipated Schedule, in this SOW or otherwise, are estimates only, and the Parties will not rely on them for purposes other than initial planning. At the conclusion of this session, the project team will have a clear understanding of the Project and the Data Protection and Retention Service and will be able to assist in meeting the Customer's business objectives.

Key Customer technical resources and subject matter experts must be available throughout the enrollment process to assist the enrollment team.

This session will cover the following topics:

- Overview of Managed Data Protection and Retention Services, including:
  - Data Protection Managed Solution
  - Data Protection Service Delivery
  - Service Guidelines
  - Customer Responsibilities
  - Plan for the administration of the integration on an ongoing basis for the term of this SOW.
  - Successful completion of Site Survey document

C. **Project Closure Meeting**

The project team will meet to recap the enrollment project activities, provide required documentation, discuss any next steps, and formally close the enrollment project. During this meeting, Seller and Customer will review the acceptance criteria for the solution and a formal acceptance document will be prepared and signed.

Data Protection and Retention Service Implementation

Installation and Initial Configuration

Seller's Engineers perform the installation and initial configuration in cooperation with the customer. Installation and configuration time is generally considered to be less than a half day if all the required prerequisites are available.

Sellerwill either bring or ship in advance the hardware required to perform the installation. Included in that hardware will be mid-length cabling for both power and connectivity, as well as any required connectors needed on the hardware provided by Seller. Any required SFPs in the customer hardware will be provided by the customer.

Customer Provided Information

The customer is required to provide and configure their environment ahead of installation so that the installation can go smoothly. Detailed in Customer Responsibilities, this information is critical to ensuring that an installation can be performed without delay.

Data Protection Installation

Installation of the Managed Solution is performed by a Seller Project team in cooperation with Customer remotely. Ensuring that all steps are completed properly, the Seller engineer will leverage the installation checklist (Site Survey) as provided during enrollment services. The list below is an abbreviated version of the checklist that provides a baseline of what will be completed during the installation. These tasks will be performed by the Seller engineer remotely with the customer engineer on hand as a training exercise.

1) All equipment racked, cabled and configured.
2) Configure monitoring platform and validate connectivity.
3) Base SLA created.
4) Critical Data SLA created.
5) Assign Base and Critical Data SLAs to the initial backup targets requested by the customer to begin the initial ingest of data.
6) Set initial ingest windows for remaining data.
7) Educate customer on the portal, ticketing and other support functions

2. Recurring Data Protection and Retention Services

The Seller's Services provides a Managed Data Protection and Retention Service to Customer on Seller, or customer-provided infrastructure and software. Seller will proactively monitor the environment for data protection performance, perform backups and restorations as described in this SOW.

Managed Data Protection and Retention Services Description

Platform Feature Descriptions

Converged Data Management features:

Seller's Services are based on Rubrik technology that combines backup software and deduplicated storage into a single scale-out fabric to form a converged data management platform. Distributed design allows for horizontal scale out capability to thousands of nodes to support the largest backup environments.

Rubrik delivers backups, instant recovery, replication and archiving as key features of the converged data fabric. Rubrik removes the traditional 'backup job' setup with policy driven management; admins can automate the protection of their entire virtual estate through a handful of policies that ensure SLAs are met.

Data Protection Features:

- Flash-optimized Ingest: Ingest large volumes rapidly, minimizing impact to production and eliminating application stun for highly transactional apps.
- Scale-out Deduplication: Maximize storage efficiency with global deduplication across the platform and extended to the cloud.
- App-Consistent Snapshots: Take application-consistent snapshots for Microsoft Exchange, SharePoint, SQL Server, Active Directory and Oracle RDBMS
- Encryption:
  - Inflight: Data transmission between nodes in a secure cluster is encrypted with the Transport Layer Security (TLS) protocol, preventing attackers from access to the transmitted data even when the transmission is intercepted.

  - At Rest: Seller replication clusters secure data with the Advanced Encryption Standard (AES) symmetric-key algorithm, using a 256-bit key length (AES-256).
- Immutable Backups: Data stored in the Rubrik Filesystem is unable to be altered once it is written, ensuring that backup data cannot be changed once committed.

System Management Features:

- Policy-based Management: click to assign out-of-the-box SLA policies to protect your VMs. Additionally, create custom SLA policies for snapshot capture frequency, retention duration, and data location to meet the needs of your business.
- Unified Console: Manage your data through responsive and modern web console, delivering clear visibility into VM protection status, snapshots, SLA policies, storage usage, ingest throughput, and more.
- Compliance Reporting and Alerts: Track SLA compliance, backup tasks and system capacity. Detailed reporting and notification for process workflow and ease of management.

Data Recovery Features:

- Instant Recovery: Instantly recover VMs and applications by mounting directly from Rubrik to your virtual environment. No rehydration or data copying to be back online.
- Global Real-Time Search: Instantly search for files across all snapshots with predictive search that delivers suggested search results as you type.

Data Retention Features:

The Service leverages the Rubrik data retention methodology of SLAs to govern the retention history of protected data in the ecosystem. Rubrik SLAs provide the option to select the frequency the data is collected and the length of time those points in time, or snapshots, are kept. Retained data is stored in a deduplicated state on the Rubrik appliance (physical or virtual) until the SLA moves the data to a configured archive target.

Recovering data from the local appliance or from the archive repository is performed the same way through the user interface, intelligently pulling only the required data from the remote storage locations to minimize the required network traffic and to ensure speed of recovery for the workload.

Data can be replicated to a partner Rubrik cluster that is paired with the source cluster and the customer can set via the UI the amount of retention to keep on that destination cluster. Seller's Data Protection and Retention Services can provide for any retention period, provided and available by Rubrik policies and storage.

Managed Data Protection and Retention Services Options

The CDW Data Protection and Retention Services provides the following services options.

I. Data Protection Service Tier I – Banded or Consumption Based Pricing (Foundation or Enterprise Software Edition)

II. Data Protection Service Tier II – Banded or Consumption Based Pricing (Foundation or Enterprise Software Edition)

III. Data Protection Service Tier III – Banded or Consumption Based Pricing (Foundation or Enterprise Software Edition)

IV. Data Protection Service Management Only or Tier II/III Hybrid (management of customer-owned equipment and software)

The service description for each option is provided below.
The Customer selected Tier with the associated pricing is outlined in the Services Fees section of the SOW.

Data Protection and Retention Service Descriptions

Supported Data Protection/backup types

The backup types supported include:

- File Level Only
- Bare Metal (e.g. file level + system state backups)
- Snapshot
- Database/Application (SQL, Exchange, etc.)

Monitoring

Seller monitors all managed Rubrik clusters 24/7, leveraging proprietary tools which detects hardware, software, and backup issues in the customer environment. Triggered issues are converted into internal ticket and worked by the Seller's support team. Customer is contacted on any issues and changes required to be made to deployed Rubrik systems.

Update and Patch Management

Seller tracks all deployed software versions of managed Rubrik clusters to ensure that patches and updates are applied as needed to keep the platform both secure and up to date. Management tools included with the service are also updated for OS and application fixes as available to keep them as reasonable current and stable as possible.

Services not specified in this SOW are considered out of scope and will be addressed with a separate SOW or Change Order.

Description of Services – Tier I & II

Standard services are defined below, any custom service options would be configured and documented with a custom statement of work (SOW).

Seller delivers Data Protection and Retention in defined tiers. Each tier calls out specific service delivery components from the CDW Data Protection Service Delivery section that follows. All service offerings are fully managed services.

Tier I & II Features:

	Tier I	Tier II
Rubrik Appliance on Premises	✓	✓
Management	✓	✓
Archive (Cloud or ADP)	✓	✓
Second Site Replication		✓

Tier I – Fully managed Rubrik appliance on-premises and archive enablement. Software level and storage capacity as described in the Services Fees section of the SOW.

Tier II – Fully managed Rubrik appliance on-premises, archive enablement, and replication to a second Rubrik instance. Software level and storage capacity in the Services Fees section of the SOW.

Description of Services – Tier III

Tier III – Features

The Disaster Recovery Services tier include all the delivery components in Tiers I and II, plus additional Tier III components:

	Tier I	Tier II	Tier III
Rubrik Appliance on Premises	✓	✓	✓
Management	✓	✓	✓
Archive (Cloud or ADP)	✓	✓	✓
Second Site Replication		✓	✓
DRaaS			✓

The Seller Data Protection and Retention Services covered by this Statement of Work includes the following Services when purchasing Tier III - Disaster Recovery Services

Description of Services – Tier III

The Disaster Recovery Services tier include all the delivery components in Tiers I and II and can not be implemented separately.

Disaster Recovery Service Description:

Seller's provided Disaster Recovery (DR) Services are delivered on top of Replication customers. Customer is responsible for all the same responsibilities as described in the Replication Only service option. Seller's Disaster Recovery Services include all the components listed as part of the disaster services and are provided out of Seller or Seller-partnered facilities on Seller or Seller-partnered equipment. Disaster Recovery services delivered on top of 3rd party clouds, are not underneath this umbrella and are considered custom and out of scope.

Providing Disaster Recovery (DR) services creates an avenue for your business to be back to full operations after suffering an outage. Comparing DR services starts with understanding the difference between a true DR and a business continuity service. Business continuity allows your business to limp along after a disaster, typically running at partial capacity with just enough resources to keep your services available. DR service allows your business to run at full speed, creating the experience for your customers of no degradation in performance or functionality.

Seller's DR Service allows customers to select whether a given part of their service requires full DR, or simply continuity. Reserving resources and guaranteeing performance allows those workloads designated for full DR to perform as they would in production. Whereas those workloads specified for business continuity leverage on-demand resources that may contend with other cloud-workloads for full performance. Customers are enabled to design a solution to meet the needs of their business with well-defined costs.

Disaster Recovery Service Features:

On-Demand Resources

Customers leveraging the Seller's DR solution have the option to leverage available On-Demand resources. On-Demand resources can be enabled by recovering any of the protected images stored in the replicated Rubrik platform, or by deploying an available template from the Seller's catalog. On-Demand resources leverage available capacity in the Seller's or Seller-partnered infrastructure and are subject to fluctuations in available performance.

Steady State Operations

Steady state operations is considered achieved once all initial backups have been successfully completed and data is flowing to the archive targets. DR customers are considered to be in steady state once the initial seed of DR data has been successfully transmitted to the replication target.

Disaster Recovery Installation (Tier III):

Seller Data Protection Disaster Recovery services consist of a replication target for the customer premise Rubrik cluster, network connectivity, and available compute capacity for recovery. Disaster Recovery is configured if the customer has purchased the service as part of their on-premise installation, or if the customer is an Edge installation where DR is included. Customers who are existing Rubrik customers can add replication to Seller's DR services and become configured in the same manner as described here.

Environment Design Baseline:

Seller Engineers engage with the customer to build a design baseline of the customer's DR environment. The Design Baseline is a joint exercise where the customer audits the workloads they will require in DR so that the networks and base environment can be built. Included in this design baseline is determining the appropriate method of connectivity between the customer environment and the Seller DR platform. Once the Design Baseline is complete, the Seller team will build the base environment in their DR platform and a date for initial connectivity will be set.

Connectivity:

Connectivity between the Customer environment and the Seller DR environment facilitates the consistent communication between the source and destination replication Rubrik clusters as well as creating the avenue for connectivity needed during a DR event. Seller can support almost any connectivity the option preferred by the customer. The primary methods are broken out as follows below:

Layer 3:

Layer 3 connectivity refers to a type of connectivity where traffic is routed from the customer's environment to the DR environment. Connectivity of this type are typically VPN or private line type connections. The advantage to a Layer 3 topology is they are quick to configure and allow the customer to create a well-defined logical network space for their DR environment. The disadvantage to Layer 3 environments comes with duplicate IP addresses produced by recovered virtual machines. Such duplicates either need to be isolated or re-addressed, both of which create significant effort at the time of DR.

Layer 2:

Layer 2 connectivity refers to an extension of the customer's network into the DR space. Connectivity of this type are typically performed over MPLS, Private Line, SD-WAN (Software Defined Wide Area Network), or a 3rd party service such as Equinix Cloud Exchange. Layer 2 connectivity can be blended with Layer 3 to offer customers both the ability to route traffic into devices on isolated networks with in the Seller DR platform as well as extend existing virtual networks (VLANs) from their primary locations. The key advantage to layer 2 connectivity is enabling the recovery of a single VM on a network segment without needing to change IP addresses or routing choices. The primary disadvantage to layer 2 connectivity is the time to configure.

Initial Ingest of Data:

Established communication between the customer location and the Seller environment enables the initial ingest of data from the customer premise Rubrik platform and the Seller repository. Sizing of the initial ingest and the amount of bandwidth available plays a large part in the method of consuming the initial ingest of data. The vast majority of customers grow their bandwidth at a rate consistent with the size of their environment, making the available bandwidth for performing the initial ingest to be appropriate at the onset. Many bandwidth providers also bursting capabilities to facilitate the ingest.

Customers who have a significant data set can be seeded using a physical appliance for transportation. Physical seeding leverages local networks to ingest the first round of data. Once ingested, the physical appliance would then be transported to the Seller facility and incremental updates would pick up from that point forward.

Description of Services – Management Only or Tier II/III Hybrid

Management Only (Remote Managed Services):

Existing Rubrik installations are eligible to be managed in-place by Seller. The Management Only option overlays the Seller management and includes all monitoring and troubleshooting involved in the management component services. Customer is responsible for ensuring that the Rubrik maintenance is kept current for any managed installation.

Tier II Hybrid - Replication Only Existing Rubrik installations in search of a secondary target for replication can leverage Seller's Replication Only services. Seller provides a Rubrik target and bandwidth to receive replication traffic for Customer owned Rubrik installations. The Customer is responsible for ensuring the source environment is under Rubrik support and within the supported release schedules. Replication Only can stand alone (Hybrid Tier II) or coupled with our Disaster Recovery Services (Hybrid Tier III).

Tier III Hybrid - Disaster Recovery Services (Tier III) Seller provided Disaster Recovery Services are delivered on top of Replication customers. The customer is responsible for all the same responsibilities as described in the Replication Only service option. Seller Disaster Recovery Services include all the components listed as part of the Seller disaster services and are provided out of the Assured facilities on Assured equipment. Disaster Recovery services delivered on top of 3rd party clouds, are not underneath this umbrella and are considered custom.

Additional Services – Available Add-Ons or Options

Seller may provide additional services to accompany Managed Data Protection and Retention Services that are optional to Services as described in this SOW. Examples include, but are not limited to additional Object Storage Options, Disaster Recovery Options, SaaS Protection Options, Data Center or Cloud Based Charges or other Professional Services.

IF ANY ADDITONAL SERVICES ARE IN SCOPE, THE SERVICE DESCRIPTION AND APPLICABLE PRICING IS INCLUDED IN THE SERVICES FEES SECTION OF THE SOW.

Steady State Operations

Steady state operations is considered achieved once all initial backups have been successfully completed and data is flowing to the archive targets.

The following tasks are included with Seller's Data Protection and Retention Services:

Responsibilities	Seller
MONITORING	
Monitor Data Protection and Retention Services/backup server	●
Monitor backup success	●
Upgrade Data Protection and Retention Services/backup software	●
OPERATIONS AND MAINTENANCE	
Maintain helpdesk ticketing workflow	●
Provide incident management for software (break/fix)	●
Perform software updates for backup and monitoring software	●
Perform security audit and patching: notification and compliance	●
Conduct full backup	●

Responsibilities	Seller
Conduct incremental backups	●
Conduct data retention and archiving as described in Customer enrollment documentation (Site Survey)	●
Perform ad hoc backups, per customer or maintenance requirements	●
Perform file restores, per customer or maintenance requirements	●
Perform complete data restore	●
Perform virtual machine restores of servers using snapshot backups only	●
Perform virtual and/or physical machine restores of servers not using snapshot backups	○
Adjust customer configuration to exclude unnecessary files	●
Remediate issues with nightly Data Protection/backups	●
Perform hardware incident management (break/fix)	●

INCREMENTAL RESPONSIBILITIES: TIER III	Seller
OPERATIONS AND MAINTENANCE	
Notification of DR invocation	●
Execution of DR Runbook	●
Discontinuation of DR Environment	●
Notification of DR Test	●
Notification of discontinuing DR	●

Service Guidelines

Overview

The Support Guidelines section outlines the support provided by service component across the Service portfolio. The Support Guidelines documentation is superseded by any called out items in the Master Services and License Agreement.

Severity and Response Guidelines

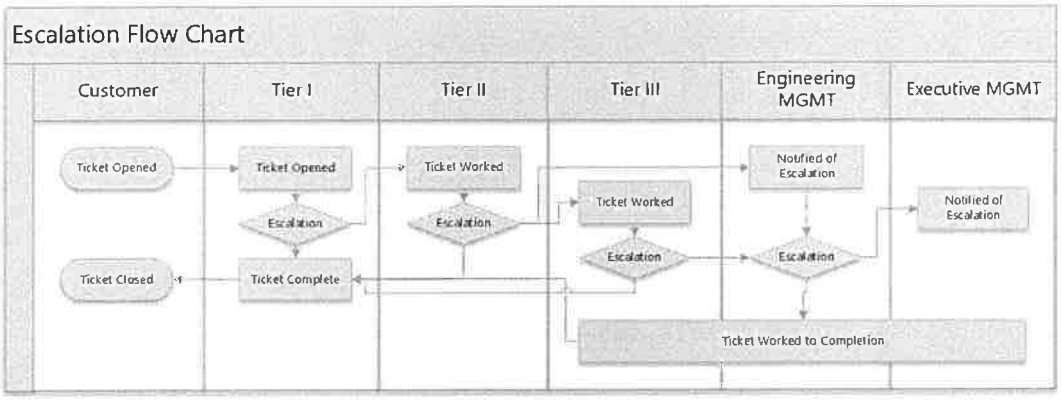
Severity levels are determined by the level of impact related to the customer's usage of the Services. Severity level is assigned by the responding engineer based on the described or determined impact based on the initiating event. Customer may request a change in severity if there is a change in the impact during the course of trouble resolution.

Definitions

Severity - Severity is defined as the business level impact of the ticketed event. Business impact levels are determined by engineering analysis against the severity levels defined below.

Escalation - Escalation is defined as the increased visibility and urgency to correct a problem as it relates to the amount of time the ticketed event has existed. Escalation does not change the severity of a ticketed event without request by customer or change in the nature of the event. The Escalation path is shown in table below:

Escalation Path:



Response Time - Response Time is defined as the amount of time between the initiation of a ticketed event and the confirmation by the Seller support team that the ticket has been received and being worked by an engineer. Tickets can be initiated by programmatic alerting or via direct customer contact through e-mail, telephone, or web-based ticketing.

Severity Levels

Severity	Description of Classification
P1 – Critical	Service unavailable preventing a recovery action or where there is a direct impact to business functionality Examples: 1. Disaster Recovery environment offline during a live event 2. Hardware failure of on-site appliance where data is unable to be restored 3. Failure to restore an object due to service availability
P2 – High	Service degraded or unavailable with potential impact to business function or capability Examples: 1. Replication link down 2. Hardware failure causing intermittent interruption to backups 3. Errors across many object backups
P3 – Standard	Service degraded but still meeting continuing service levels Examples: 1. Hardware redundancy failure (HD in RAID group, redundant node, etc.) 2. Errors in isolated object backups (single VM, single fileset, etc.)

	3. Disaster Recovery environment performance of On Demand resources
P4 – Low	Non-service impacting or degraded issue or concern Examples: 1. Request version upgrade 2. Change or modify SLA set 3. Schedule a DR test

Severity levels are set upon ticket creation by the responding engineer based upon the generated alert or customer request.

Response and Escalation Time Guidelines

Severity	Response Time	Escalation Time
P1 – Critical	Within 60 Minutes	2 hours
P2 – High	Within 90 Minutes	6 hours
P3 – Standard	Within 1 Business Day	24 hours
P4 – Low	Within 2 Business Days	48 hours

Hardware Servicing and Repair

Seller hardware servicing is included as part of managed services delivered to a customer on Seller provided equipment. Any hardware furnished by the customer is outside the scope of this section of the support guidelines.

Rubrik OEM Hardware:

Hardware provided by Rubrik is subject to the Rubrik Return Materials Authorization (RMA) process. The Rubrik RMA process provides next business day for all parts requiring replacement with end customer acting as the "Smart Hands" to perform the replacement of the failed component. Seller acts as the intermediary on the customer's behalf to contact Rubrik upon a ticketed event found to be a hardware issue and facilitate the RMA.

Seller Provided Hardware:

Hardware provided by Seller as part of the service is provided with a next business day advance-delivery parts warranty. Seller facilitates any hardware RMA through ticketed events where the issue is found to be hardware related. Physical replacement of the part is contract dependent. Customers with on-premises engineers can care for physical replacement. Customers with no on-site engineers can request this option be added in the contract.

Hardware Support Table:

Hardware Type	Responsible	Part Delivery Time	Part Replacement
Rubrik OEM Hardware	Seller DP	Next Business Day	Contract Dependent
Seller Provided Hardware	Seller DP	Next Business Day	Contract Dependent
Customer Provided Hardware / Software only	Customer	Customer OEM Provider	Customer / OEM

CUSTOMER RESPONSIBILITIES

The Customer shall provide to Seller the following:

1. Information as necessary for Seller to perform its responsibilities as stated in this SOW.
2. Unless provided as a part of this SOW, software and hardware maintenance coverage for Customer's systems.
3. A defined and adequate maintenance window to perform maintenance activities for Purchased Services that require maintenance windows.
4. In the event Seller is an authorized agent to dispatch Customer's equipment maintenance or other third-party provider service, Customer shall grant Seller authorization (via Letters of Agency) to troubleshoot, diagnose, and/or dispatch provider's technicians on Customer's behalf, and otherwise to perform all of Customer's responsibilities as stated in this SOW.
5. Continuous electronic access on a 24x7 basis to Customer's supported infrastructure.
6. Notification of any planned maintenance that impacts the Seller's ability to provide service.
7. Physical Device Intervention activities:
    a. A response to Seller requests for PDI activities in a timely and professional manner. Seller will provide Customer 24-hours' notice of any non-emergency maintenance activities that may require Customer PDI activity.
    b. A PDI escalation contact list with contact names and contact information, including any and all updates and contact unavailability notice.
8. All customer provided information as illustrated in the table below.

Customer Responsibility	Description
Power	Management Server requires 2x NEMA 5-15 or C13 available outlets (specified type in advance) Rubrik appliance requires 2x NEMA 5-15 or C13 available outlets.
Rack Space	Rack Units expected standard 19" width rack with standard depth. 1 Rack Unit for Seller Management Server 2 Rack Units per physical Rubrik appliance
vSphere Credentials	vSphere local or domain user with the appropriate rights to perform backup and recovery (Document Provided by Project Team)
Server / Application Credentials	Local or domain credentials for target physical or application only data protection targets (SQL, Linux)
Provision IP Addresses	IP Addresses on the customer's internal network are required for the following devices (Base install is 8 IPs): 1) 1 IP per node for Rubrik. Middle number in model indicates number of nodes (R348 = 4 nodes) 2) 1 IP for Lights Out controller of management server 3) 1 IP for management ESX 4) 2 IP for management collectors
Network Ports	3x 100/1000Gbps Copper Ethernet connections: 1x Management Lights Out (optional) 1x Seller Monitoring Node Manage port 1x Rubrik Management per Appliance 2(4)x 10Gbps SFP+ compatible ports (w/SFPs installed) 2x 10Gbps SFP+ per Rubrik Appliance

Customer Responsibility	Description
	2x 10Gbps SFP+ per Management node (optional if management only, recommended if EDGE installation)
VLAN Configuration	Assigned VLANs for (can all be the same): Management Network Data Protection Network
Firewall Configuration **All ports:** (Document Provided by Project Team)	Outbound 443 for: Rubrik Call Home / Remote Support Seller ProtectView remote support / logging BiDirectional 7785 TCP to Seller for: Rubrik Replication (if enabled)
Archival Target Preparation	S3 Targets: AWS access ID and Secret with appropriate permissions for bucket creation, read, and write capabilities. Generated RSA key also required for encryption. NFS Targets: NFS path with available permissions for Rubrik Cluster IPs
Protection Scheme	Base SLA: The Base SLA is the default backup policy that will "catch" any created VM to ensure backups are being completed at a minimum level for any created VM. Critical Data SLA: The Critical Data SLA is the most stringent data retention policy that should be applied to any targets (virtual machines, filesets, or databases) that need to meet compliance or strict company restrictions for retention Other SLAs: Any additional SLAs the customer requires.

SERVICE LEVEL AGREEMENT

DEFINITIONS

For the purpose of this SLA, the following terms shall have the corresponding definitions:

"Availability" means the total percentage of time within a Calendar Month that the Service are available, excluding Scheduled Downtime and Emergency Maintenance, and shall be calculated as follows:

Availability = Maximum Availability – Service Outage / Maximum Availability x 100

"Calendar Month" means each calendar month during the License Term.

"Emergency Maintenance Support" means instances where it is not practical for Seller to provide advance notice of a maintenance event, such as an unforeseen disruption of a critical service. Addressing these events may require that emergency maintenance be performed which may result in the disruption of the Hosting Services in order to conduct this emergency maintenance without prior notice.

"Incident" means a report issued to Seller by Client informing Seller that the Service is experiencing a Service Disruption.

"Maximum Availability" means the total number of minutes in a Calendar Month less the Scheduled Downtime.

"Scheduled Downtime" means routine tests, maintenance, upgrades, or repairs performed by Seller on the Hosting Environment; provided, Seller will use reasonable commercial efforts to provide Client fourteen (14) days prior notice of Schedule Downtime.

"Service Disruption" means each occasion of 10 or more consecutive minutes in which Client is unable to access the Service.

"Service Level" means the Availability of the Service in a Calendar Month.

"Service Level Exceptions" means the exclusions from a Service Outage set out in Section 3, below.

"Service Outage" means the aggregate of Service Disruptions in a Calendar Month, excluding the Service Level Exceptions.

INCIDENT PRIORITIZATION

All Incidents that are reported to Seller or that Seller otherwise becomes aware of will initially be assigned a priority by Seller as set forth in the Support Guidelines.

SERVICE CREDITS/CHRONIC FAILURE

Subject to the Service Level Exceptions, Seller shall provide Client with the following Service Level Credits if in any Calendar Month the Service Availability is 99.5% or lower:

AVAILABILITY	SERVICE LEVEL CREDIT
99% - 99.49%	2.5%
95% - 98.90%	5%
90.1% - 94.9%	10%
<90.0%	20%

SCHEDULED MAINTENANCE SUPPORT

Standard Support, including the implementation of Enhancements and routine maintenance for the Service shall be scheduled outside of standard business hours. The expected window for standard Support is Tuesdays from 10:00AM until 3:00PM Eastern Time Zone. Seller shall notify Client as provided herein if Scheduled Downtime is required.

NOTICE OF SERVICE OUTAGE; REMEDY

If Client is unable to access the Service, Client shall promptly notify Seller. To receive a Service Level Credit, Client must notify Seller during the occurrence of the outage problem to provide Seller an opportunity to resolve the outage. Upon the conclusion of each Calendar Month, Seller shall determine the Service Level for such Calendar Month. If Client is entitled to a Service Level Credit, Seller shall, as Client's sole and exclusive remedy for the Service Outage, include the Service Level Credit on the subsequent monthly invoice. If the Service Level Credit occurs in the last month of the License Term, Seller shall provide Client with a refund equal to the Service Level Credit within thirty (30) days following termination of the applicable License Term.

SERVICE LEVEL EXCEPTIONS

Seller shall not be liable for any failure to meet the Service Levels, to the extent such failure was caused by one or more of the following:

- Scheduled Downtime or Emergency Maintenance.
- non-production use of the Services.
- a Force Majeure.
- any act or omission of Client, including the failure to comply with the Agreement or Order.
- an outage caused by Client's hardware, software or other third-party equipment procured, licensed, or controlled by Client, including network connections and telecommunication problems.
- Deactivation or unavailability of the Call-Home Utility
- Protected Devices that are offline, unavailable, or quarantined
- The time from recognition and notification of Customer of a Physical Device Intervention (PDI) requirement to the completion of the PDI activity will be exempted from availability calculations.
- Any outage of a Customer System caused by infrastructure for which Seller is not providing Availability Management.

RESPONSE TO SERVICE LEVEL FAILURE

In the event of a Service Failure, Seller shall promptly address such failure as provided herein:

- *Promptly investigate and report on the causes of such problem based on the assigned severity level.*
- *Provide a root cause analysis of such failure as soon as practical after such failure or at Client's request.*
- *Correct such Service Failure that is Seller's fault or responsibility as provided herein.*
- *Advise Client of the status of remedial efforts being undertaken with respect to such problem.*
- *Demonstrate that the causes of such problem (that is Seller's fault or responsibility) has been, or shall be, corrected.*
- *Take corrective actions to prevent any recurrence of such problem (that is Seller's fault or responsibility).*

3. GRANT OF LICENSE

1. DEFINITIONS

As used in this Grant of License only, the following terms shall have the corresponding definitions set forth below:

"**Appliance**" means the computer server, including standard embedded software, additional components set out in an Order and any Enhancements, that shall be installed at Customer's facility and shall submit Customer Data to the Service.

"**Customer Data**" means Customer's data and information submitted to the Service.

2. LICENSE GRANT

SELLER HEREBY GRANTS CUSTOMER A NON-EXCLUSIVE, NON-TRANSFERABLE LICENSE DURING THE LICENSE TERM TO: (I) ACCESS AND USE THE APPLIANCE FROM CUSTOMER'S LOCATION IN THE UNITED STATES; AND (II) TO SUBMIT CUSTOMER DATA TO THE SERVICE, AS PROVIDED HEREIN, AND SUBJECT TO THIS STATEMENT OF WORK. THE GRANT OF RIGHTS HEREUNDER IS NOT A SALE OF THE SERVICE OR APPLIANCE. SELLER AND ITS THIRD-PARTY PROVIDERS RESERVE ALL RIGHTS NOT EXPRESSLY GRANTED BY THIS AGREEMENT.

4. USE OF APPLIANCE AND SERVICE

1. ENTITLEMENTS

Customer will only use the Services and Appliance by and for Customer's benefit in accordance with this Statement of Work. Unless permitted in this Statement of Work or agreed to by the parties in writing, Customer will not use the

Service as a service provider, and will not use or access the Service excess of the entitlements set out in this Statement of Work.

2. RESTRICTIONS

Customer will not: (i) copy the Services or Appliance, including any portion thereof; (ii) make derivative works of the Services or Appliance, reverse engineer or decompile the Services or Appliance, including any portion thereof; (iii) attempt to unlock or bypass any initialization system, encryption methods or copy protection devices in the Services or Appliance ; (iv) modify, alter or change the Services or Appliance, including any proprietary notices; (v) use the Appliance independent of the Services; or (vi) use the Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or in violation of third party rights.

3. COMPLIANCE

Customer shall comply with all applicable law, and the terms of services of any non-Seller provided applications that Customer may use with the Services or Appliance. Customer shall use commercially reasonable efforts to prevent unauthorized access to or use of the Services and shall promptly notify Seller of any unauthorized access or use that it becomes aware of. Customer shall not export, re-export or provide access to the Services to: (i) persons located in any country to which the United States has embargoed goods; (ii) any person on the United States Treasury Department's list of Specially Designated Nationals or United States Commerce Department's Denied Persons List; or (iii) in violation of any United States export control or regulation.

OUT OF SCOPE ENGINEERING AND CONSULTING SERVICES

For all engineering and consulting services not provided as part of the Purchased Services, if Customer desires Seller to perform such services, it is Customer's responsibility to request such services from Seller. Customer shall pay for such services on a time and materials basis as set forth in the table below. Services are provided by Seller subject to resource availability. Seller response and resolution times for Out of Scope Engineering and Consulting Services are not guaranteed.

Seller's Hours of Operations	Hourly Rate	Billing Increment	Minimum Billed
Normal Business Hours 7:00 a.m. – 7:00 p.m. Central Time Monday – Friday Also includes After Hours services that are scheduled at least 5 days in advance.	1X of Hourly Rate	15 minutes	15 minutes
After Hours - Unscheduled 7:00 p.m. – 7:00 a.m., Central Time Monday – Friday, Weekends, Holidays	2X of Hourly Rate	1 hour	2 hours

In the event Customer requires Out of Scope Engineering and Consulting Services in excess of twenty-four (24) hours of total engineering time per engagement, Customer shall purchase engineering and consulting services pursuant to a separate SOW.

ADDITIONAL TERMS, LIMITATIONS AND DISCLAIMERS

1. Seller may change all or any portion of the equipment used to provide the Purchased Services at any time if Seller, in its sole discretion, determines such change is necessary or desirable, but Seller agrees to perform

modification(s) in a manner that does not result in any permanent, substantial, materially adverse alteration to the Purchased Services provided to Customer under this SOW.

2. Notwithstanding anything to the contrary in the Agreement, the Parties acknowledge and agree that Seller may subcontract some or all of the Purchased Services, provided: (i) Seller ensures that subcontractors strictly comply with Seller's obligations contained within this SOW; (ii) any such subcontractor enters into a nondisclosure agreement with Seller containing terms substantially similar to the confidentiality provisions contained in the Agreement; and (iii) Seller remains responsible for the performance of any such subcontractors.

3. Notwithstanding anything to the contrary in the Agreement, subject to the limited rights expressly granted hereunder, Seller reserves all rights, title and interest in and to the Purchased Services, including all related systems and intellectual property rights. No rights are granted to Customer hereunder other than as expressly set forth herein. Seller shall have a royalty-free, worldwide, transferable, sublicensable, irrevocable, perpetual license to use, modify, and/or incorporate into the Purchased Services any suggestions, enhancement requests, recommendations or other feedback provided by Customer, relating to the operation of the Purchased Services.

4. Seller does not warrant that the purchased services will be uninterrupted, error-free, virus-free, or completely secure. The service level credits referred to herein shall be seller's sole liability and customer's exclusive remedy for interruptions, delays, impairments, inadequacies, or other defects in service with regard to any and all of the purchased services.

5. Seller shall not be liable for any loss or damage resulting from unsupported Client provided hardware or software (whether such lack of support results from Client's failure to maintain a current maintenance and support agreement with the applicable vendor or the vendor's failure to maintain support for any other reason). Failure of Client to maintain a current maintenance and support agreement with the applicable vendor for each of the Client provided hardware or software shall release Seller from any service level agreement ("SLA") or associated penalty resulting from a missed SLA, its financial penalty, or grounds for breach as defined herein.

6. Support will be provided by global based resources.

TERM AND TERMINATION

This SOW will be effective as of the date of Seller's signature and will be for an initial term of three (3) years (the "Initial Term") from the start of the recurring services fees. This SOW will automatically renew for additional one (1) year terms (each a "Renewal Term") unless either party provides the other party with a notice of termination at least thirty (30) days prior to the expiration of the Initial Term or the then-current Renewal Term. The Initial Term and each one-year Renewal Term, if any, may be referred to herein individually as a "Service Term" or collectively as the "Service Terms."

Notwithstanding anything to the contrary in the Agreement, the Parties agree that the following represent the termination options relative to this SOW:

1. End of Service Term. Either Party may terminate this SOW effective as of the end of the then current Service Term, by providing written notice of such termination at least thirty (30) days prior to the expiration of the then current Service Term.
2. Breach. Either Party may terminate this SOW if the other Party materially breaches any of its representations, warranties, or obligations under this SOW and such breach is not cured within thirty (30) days of breaching Party's receipt of written notice specifying the breach.

3. Convenience. Either Party may terminate this SOW for convenience by providing sixty (60) days written notice of such termination to the other Party. In the event of any convenience termination of this SOW by Customer, Customer will pay to Seller an early cancellation charge equal to the current annual fee for the number of years remaining in the current term.

For any termination by Customer, the notice of cancellation must be accompanied by payment in full for all Purchased Services through the effective date of termination. In the event of any Convenience Termination by Customer, Customer's notice of cancellation must also be accompanied by payment of the applicable cancellation charge(s) as previously indicated. The Parties agree that the cancellation charge(s) are in addition to any other fees or payments of any nature owed by Customer.

In addition to its right to terminate as provided for herein, Seller may suspend all or part of Customer's access to the Purchased Services (i) if Customer is delinquent on payment obligations; (ii) upon receipt of a subpoena or law-enforcement request; or (iii) when Seller has a commercially reasonable belief that Customer has breached this SOW or that Customer's use of the Purchased Services poses an imminent security risk.

Services not specified in this SOW are considered out of scope and will be addressed with a separate SOW or Change Order.

GENERAL RESPONSIBILITIES AND ASSUMPTIONS

- Customer is responsible for providing all access that is reasonably necessary to assist and accommodate Seller's performance of the Services.
- Customer will provide in advance and in writing and Seller will follow, all applicable Customer's facility's safety and security rules and procedures.
- Customer is responsible for security at all Customer-Designated Locations; Seller is not responsible for lost or stolen equipment, other than solely as a result of Seller's gross negligence and willful misconduct.
- Customer acknowledges that in order to efficiently and effectively perform the Services CDW may need to collect information from Customer's systems by using software tools developed or used by CDW ("Tools"). In some cases, these Tools will need to be loaded onto the Customer's systems to gather necessary information, and CDW may also use them to make changes in the Customer's systems consistent with the agreed upon scope. Tools will be used only for purposes of performing the Services and will be removed or automatically deleted when CDW has completed use of them. Customer hereby consents to CDW's use of the Tools as set forth in this paragraph.

CONTACT PERSONS

Each Party will appoint a person to act as that Party's point of contact ("**Contact Person**") as the time for performance nears and will communicate that person's name and information to the other Party's Contact Person.

Customer Contact Person is authorized to approve materials and Services provided by Seller, and Seller may rely on the decisions and approvals made by the Customer Contact Person (except that Seller understands that Customer may require a different person to sign any Change Orders amending this SOW). The Customer Contact Person will manage all communications with Seller, and when Services are performed at a Customer-Designated Location, the Customer Contact Person will be present or available. The Parties' Contact Persons shall be authorized to approve changes in personnel and associated rates for Services under this SOW.

CHANGE MANAGEMENT

This SOW may be modified or amended only in a writing signed by both Customer and Seller, generally in the form provided by Seller ("**Change Order**"). Services not specified in this SOW are considered out of scope and will be addressed with a separate SOW or Change Order.

In the event of a conflict between the terms and conditions set forth in a fully executed Change Order and those set forth in this SOW or a prior fully executed Change Order, the terms and conditions of the most recent fully executed Change Order shall prevail.

PROJECT SCHEDULING

Customer and Seller, who will jointly manage this project, will together develop timelines for an anticipated schedule ("**Anticipated Schedule**") based on Seller's project management methodology. Any dates, deadlines, timelines or schedules contained in the Anticipated Schedule, in this SOW or otherwise, are estimates only, and the Parties will not rely on them for purposes other than initial planning.

TOTAL FEES

The total fees due and payable under this SOW ("Total Fees") include both fees for Seller's performance of work ("Services Fees") and any other related costs and fees specified in the Expenses section ("Expenses"). Unless otherwise specified, taxes will be invoiced but are not included in any numbers or calculations provided herein. The pricing included in this SOW expires and will be of no force or effect unless it is signed by Customer and Seller within thirty (30) days from the Date list on the SOW, except as otherwise agreed by Seller.

Seller will invoice for the Total Fees.

The Service Fees hereunder include both the one-time enrollment fees ("Enrollment Fees") and the annual recurring services fees ("Recurring Services Fees").

This SOW may include multiple types of Services Fees; please reference below Services Fees section(s) for further details.

SERVICES FEES

Enrollment Fees (One-time)

Milestone	Percentage	Fee
Deployment Fee - Set Up and Onboarding	100%	$2,000.00
Totals	**100%**	**$2,000.00**

Recurring Services Fees (Annual)

Services	Unit	Amount	Annual Unit Fee	Annual Total Fee
Assured Data Protection Service Tier III – Hybrid Customer owned Rubrik appliance on-premises, replication to 2nd Rubrik instance, DRaaS and archive enablement; Minimum Commit: 15TB	TB	15	$2,700.00	$40,500.00
Assured Data Protection Service Tier III – Hybrid OVERAGES	TB	Actuals	$2,700.00	Actuals
Total (Minimum Annual Fee)				**$40,500.00**

PRICING NOTES:

- Customer may alter services without penalty and will be billed for actual usage, subject to the annual minimum charge.
- Setup fees are billed upon signature.
- Service billing will begin upon commencement of the Service Term.
- Service Term will commence upon Service delivery or the month following the arrival of on-premises hardware, whichever comes first. Notwithstanding, all billing will commence within 60 days of contract signature.

RECURRING SERVICES FEES

Customer has chosen to purchase the Purchased Services indicated above and agrees to pay Seller the fees, charges, and other amounts indicated. Except as otherwise stated in this SOW, Seller and Customer agree to follow the billing and payment terms, conditions, and procedures set forth in the Agreement.

Customer agrees to maintain the annual minimum commitment for the Purchased Services, if any, as indicated.

Customer is protected against any price increase for Purchased Services for the duration of the Initial Term. Effective on the first day of each Renewal Term (each a "Renewal Date"), and for all subsequent auto-renewals the prices for Purchased Services may be adjusted to Seller's then current Recurring Services Fees or increased by 3% whichever is greater for such Purchased Services. Such revised pricing will be effective for that Renewal Term.

Customer will not be required to pay charges for Services initially invoiced more than 6 months after close of the billing period in which the charges were incurred. If Customer disputes a charge, Customer will provide notice to Seller specifically identifying the charge and the reason it is disputed within 6 months after the date of the invoice in which the disputed charge initially appears, or Customer waives the right to dispute the charge. The portion of charges in dispute may be withheld and will not be considered overdue until Seller completes its investigation of the dispute. Following Seller's notice of the results of its investigation to Customer, payment of all properly due charges must be made within ten (10) business days.

EXPENSES

Seller will invoice Customer for Seller's reasonable, direct costs incurred in performance of the Services. Direct expenses include, but may not be limited to: airfare, lodging, mileage, meals, shipping, lift rentals, photo copies, tolls and parking. Seller will charge actual costs for these expenses. Any projected expenses set forth in this SOW are estimates only.

Travel time will not be billed for this project.

TRAVEL NOTICE

Two (2) weeks' advance notice from Customer is required for any necessary travel by Seller personnel.

CUSTOMER-DESIGNATED LOCATIONS

Seller will provide Services benefiting the following locations ("**Customer-Designated Locations**")

Location	Address
MT DIABLO UNIFIED SCHOOL DISTRICT	1936 Carlotta Drive, Concord, CA 94519

SIGNATURES

In acknowledgement that the parties below have read and understood this Statement of Work and agree to be bound by it, each party has caused this Statement of Work to be signed and transferred by its respective authorized representative.

This SOW and any Change Order may be signed in separate counterparts, each of which shall be deemed an original and all of which together will be deemed to be one original. Electronic signatures on this SOW or on any Change Order (or copies of signatures sent via electronic means) are the equivalent of handwritten signatures.

CDW Government LLC	**MT DIABLO UNIFIED SCHOOL DISTRICT**
By:	By:
Name: Brock Lambert	Name: ADRIAN VARGAS
Title: Mgr Partner Svcs- Mgd Svcs	Title: CHIEF BUSINESS OFFICER
Date: Feb 4, 2025	Date: 2/4/25
Mailing Address:	Mailing Address:
200 N. Milwaukee Ave.	1936 CARLOTTA DR, FISCAL SERVICES DEPT
Vernon Hills, IL 60061	CONCORD, CA 94519-1397