



HOSTED AND MANAGED SERVICES

STATEMENT OF WORK - 2015-6793

CLIENT	Milwaukee County
CONTACT	Laurie Panella
PROJECT	Milwaukee County ReliaCloud Data Center
DATE/VER.	February 15, 2016 / v6

SUBMITTED BY
Brian Osterhaus
District Sales Manager
(608) 204-8668

PREPARED BY
James Brown
Solutions Architect
(608) 206-7443

CLOUD AND HOSTING

INTERNET

Item ID	Description
110003	Colocation Internet Committed
Company's Responsibilities and Included Features	
<p>Colocation Committed Internet Bandwidth is purchased as an additional service to Colocation Cabinets. It shall be reflected on the service order if selected by Client. Company will provide a redundant, managed Internet Bandwidth service to provide high performance, highly available internet access. Company Internet Bandwidth service will load balance traffic over multiple upstream internet backbone providers.</p> <ul style="list-style-type: none">-Service may be capped up to the maximum allocation size indicated on the service order.-Service may also leverage Burstable Internet bandwidth calculated on the 95% of peak usage.-Deliver committed Internet bandwidth allocation measured 1 Mbps increments.-Deliver services via Ethernet on 2 RJ-45 CAT5e or CAT6 from redundant Internet delivery switches-Provide a base allocation of up to 8 usable via (/29 network) Internet routing IPv4 Public addresses, unless the Client provides their own ASN and IPv4 portable address space.-Provide access to upstream and downstream bandwidth usage graphs via Client portal.	
Client's Responsibilities and Out-of-Scope Notes <small>(unless otherwise covered via a different Item ID)</small>	
<ul style="list-style-type: none">-Comply with acceptable use policy.-Provide termination hardware for service. Requires RJ-45 Ethernet termination ports.-Notify Company if additional bandwidth is needed beyond the committed allocation.-Commit to at least 1 Mbps of Internet bandwidth	

Item ID	Description
110004	Colocation Internet Burstable
Company's Responsibilities and Included Features	
<p>Colocation Burstable Internet Bandwidth is purchased as an additional service to ReliaCloud Committed Internet Bandwidth, and will be reflected on the service order if selected by Client. Company will provide a redundant, managed Internet Bandwidth service to provide high performance internet access. Company Internet Bandwidth service will load balance traffic over multiple upstream internet backbone providers. This service includes:</p> <ul style="list-style-type: none">- Bandwidth port with burstable bandwidth in 1Mbps increments billable at the 95th percentile of peak usage- Clients will of have maximum burst capacity of 1Gbps or 3x times the committed rate, whichever is smaller. Clients will receive a minimum of 100mbps burst capacity regardless of committed rate. <p>Bandwidth utilization in excess of the Committed Bandwidth will be billed as Burstable Bandwidth and calculated using the 95th Percentile Method. The 95th Percentile Method involves polling both inbound and outbound bandwidth utilization every five (5) minutes during each calendar month. All such samples are ordered from highest to lowest.</p>	

The top 5 percent of readings are discarded, and Client is billed an additional charge based on the next highest reading. The amount of pre-purchased Committed Bandwidth is subtracted from the 95th Percentile to determine the Burstable Bandwidth usage to be billed. Committed Bandwidth is billed in advance; Burstable Bandwidth is billed in arrears, the month after usage occurs. By requesting a hard limit higher than the Committed Bandwidth, Client agrees to be subject to the Burstable Bandwidth for bandwidth consumed beyond the Committed Bandwidth rate level on a monthly basis

- Deliver burstable Internet bandwidth allocation calculated on the 95th percentile of peak method, measured in 1 Mbps increments
- Client will have maximum burst capacity of 1Gbps or 3x the committed rate, whichever is smaller. Client will receive a minimum of 100mbps burst capacity regardless of committed rate.
- Provide access to upstream and downstream bandwidth usage graphs via client portal

Client's Responsibilities and Out-of-Scope Notes (unless otherwise covered via a different Item ID)

- Comply with Internet acceptable use policy
- Notify Company if additional bandwidth is needed beyond the committed allocation
- Commit to at least 1 Mbps of Internet bandwidth

IPv4 ADDRESS SPACE

Item ID	Description
110005	Additional IPv4 Internet Public Addresses Space

Company's Responsibilities and Included Features

Company provides a base allocation of IPv4 public addressable Internet address space with our committed Internet products. Clients may request additional address space to their base allocation, and additional IPs will be indicated on the service order. Company reserves the right to reclaim any unused address space, or space that is not supplied with proper ARIN documentation.

- Provide additional allocations of IPv4 publically routable Internet address space.
- Maintain Internet routing tables
- Maintain all IP documentation
- Enforce IP conservation policies

Client's Responsibilities and Out-of-Scope Notes (unless otherwise covered via a different Item ID)

- Comply and provide justification documentation with IP documentation requirements from the American Registry for Internet Numbers (ARIN)
- Request additional IPv4 Internet address as necessary

LOAD BALANCING

Item ID	Description
110045	Global Load Balancing Service
Company's Responsibilities and Included Features	
<p>The Global Load Balancing service at Company provides internet traffic management across multiple data centers. It works by acting as an intelligent Domain Name Service (DNS) authoritative server, such that when a user's web browser sends a request for a URL they receive the best of all possible global answers (DNS A record) for that particular user at that particular time. The service is provided per domain name that is hosted.</p> <ul style="list-style-type: none">- Highly available redundant hardware- Maintain DNS answering information- If necessary manually adjust A record response information	
Client's Responsibilities and Out-of-Scope Notes <i>(unless otherwise covered via a different Item ID)</i>	

CLOUD INTEGRATION

Item ID	Description
110048	RIC LAN Connection 1Gbps
Company's Responsibilities and Included Features	
<p>ReliaCloud Integration Cabinet LAN connection service 1Gbps provides connectivity services to RIC integrated devices. The service requires at least two connections to provide path and infrastructure diversity such that ReliaCloud standard SLA can be delivered.</p> <ul style="list-style-type: none">- Provide managed LAN services which provides speeds up to 1Gbps- Service is layer 2- Provide all physical cabling to interconnect the hosted device to the ReliaCloud switching infrastructure- Deliver services over Cat5e or greater RJ-45 Ethernet- Design, manage and maintain VLAN configuration- Maintain ACLs- Notify Client of any performance challenges or link-state issues with the service- Provide monitoring statistics on port speed and performance	
Client's Responsibilities and Out-of-Scope Notes <i>(unless otherwise covered via a different Item ID)</i>	
<ul style="list-style-type: none">- Provide physical device for connection service- Ensure device supports at least 2 10Gbps RJ-45 Ethernet interfaces- Configuration of attached device for teaming or multipathing	

Item ID	Description
110046	ReliaCloud Integration Cabinet (RIC)

Company's Responsibilities and Included Features

The ReliaCloud Integration Cabinet (RIC) service is designed to provide an answer for a mostly virtualize computing environment that needs colocation space for infrastructure that can't be operated appropriately as part of the virtualized stack. Examples of these types of devices would be:

- Vendor provided and managed routers
- Non X86 processor class work loads
- Equipment which supports legacy applications that won't perform well under virtualization
- Devices which terminate a physical connection (USB, TDM, Serial)

The RIC is delivered as a bundle of physical space cabinet space (1 RU = 1.75") and power of 140 watts, whichever comes first. Multiple quantities of the RIC bundle may be used to support 1 larger device. The RIC cabinet is a multi-tenant cabinet and therefore no Client physical access is granted to the devices collocated in the RIC. The service will require ReliaCloud LAN services to attach the physically hosted infrastructure to the ReliaCloud services stack.

- Provide secure 4 sided locking enclosure for purpose of hosting the equipment
- Ensure proper airflow
- Provide continuous power to the device (requires A & B side power supplies per device)
- Ensure proper power load distribution across A & B power feeds
- Maintain environmental standards for HVAC consistent with primary hosting facility
- Maintain security for the environment
- Provide all physical moves, adds, and changes for the environment
- Provide data cables, cabling, and cable management from device to ReliaCloud LAN and or SAN services
- Provide alerts for any visual or audible alarms being provided by the machine

Client's Responsibilities and Out-of-Scope Notes (unless otherwise covered via a different Item ID)

- Provide secure controls for any lockout devices such as faceplate keys

Devices must follow the guidelines of:

- May be Client-owned, Company-owned or third-party owned
- May be Client-managed, Company-managed or third-party managed
- 120 volt power supported only
- Must be rack-mountable within 4-post locking cabinet, either using front-side mounting. only (maximum protrusion: 1 inch) or four-post mounting
- Must use 1920 watts per power cord or less (including failover scenario)
- If more than one A-side and one B-side cord is needed per-device, Company will use split cords. Power receptacles may plug-in directly behind a device's power supply, requiring a planned power-down of the device in order to replace a power supply/fan in the device.

110047

RIC LAN Connection 10Gbps

Company's Responsibilities and Included Features

ReliaCloud Integration Cabinet LAN connection service 10Gbps provides connectivity services to RIC integrated devices. The service requires at least two connections to provide path and infrastructure diversity that the ReliaCloud standard SLA can be delivered.

- Provide managed LAN services which provides speeds up to 10Gbps
- Service is layer 2
- Provide all physical cabling to interconnect the hosted device to the ReliaCloud switching infrastructure
- Deliver services over Cat6 or greater RJ-45 Ethernet
- Design, manage and maintain VLAN configuration
- Maintain ACLs
- Notify Client of any performance challenges or link-state issues with the service
- Provide monitoring statistics on port speed and performance

Client's Responsibilities and Out-of-Scope Notes (unless otherwise covered via a different Item ID)

- Provide physical device for connection service
- Ensure device supports at least 2 10Gbps RJ-45 Ethernet interfaces
- Configuration of attached device for teaming or multipathing

Item ID

Description

110052

Virtual Router Service

Company's Responsibilities and Included Features

The Virtual Router Service provides endpoint termination equipment for metroE class services for up to 1Gbps in size. The service is delivered via a single port, 1 Gbps interface.

- Provide managed LAN services which provides speeds up to 1Gbps
- Service is layer 3
- Includes cross-connection from telco room to ReliaCloud WAN infrastructure
- Deliver services over Cat5e or greater RJ-45 Ethernet
- Design, manage and maintain VLAN configuration
- Maintain ACLs
- Notify Client of any performance challenges or link-state issues with the service
- Provide monitoring statistics on port speed and performance
- Service is not designed for Internet Routing table
- Service does not provide VPN termination

Client's Responsibilities and Out-of-Scope Notes (unless otherwise covered via a different Item ID)

- Secure Telco services contract with vendor
- Financial responsibility of contract with Telco vendor
- Ensure Telco vendor does not require the delivery and hosting of a vendor provided managed device
- Provide endpoint for termination
- Provide configuration services for WAN turn-up on remote devices

Item ID	Description
80016	Virtual Router Service - 10 Gbps
Company's Responsibilities and Included Features	
This SKU has no scope attached.	
Client's Responsibilities and Out-of-Scope Notes <i>(unless otherwise covered via a different Item ID)</i>	
This SKU has no scope attached.	

STORAGE

Item ID	Description
500143	Silver - Block level storage services (NextGen)
Company's Responsibilities and Included Features	
<ul style="list-style-type: none"> -Present shared SAN space to hosted environment leveraging Company's shared SAN infrastructure -Tier II general workload performance disk presentation .5 IOPS/GB -Administration of the SAN Storage Systems includes: <ul style="list-style-type: none"> -Backend disk storage management including: <ul style="list-style-type: none"> - RAID group configuration - Volume configuration -SAN: LUN provisioning -Monitoring and reporting of disk space usage -Triage and troubleshoot SAN/NAS infrastructure, performance and presentation issues -Global settings/configuration management including LUN definitions -SAN: Dynamic/Redundant path presentation. (may require proprietary multi-path software) (if applicable) 	
Client's Responsibilities and Out-of-Scope Notes <i>(unless otherwise covered via a different Item ID)</i>	
<ul style="list-style-type: none"> -Data Backup (unless covered under additional Company services) 	

Item ID	Description
500149	Bronze - Block level storage services (NextGen)

Company's Responsibilities and Included Features

- Present shared SAN space to hosted environment leveraging Company's shared SAN infrastructure
- Redundancy provided by redundant SAN head units
- Tier III low data use disk presentation .1 IOPS/GB
- Administration of the SAN Storage Systems includes:
 - Backend disk storage management including:
 - RAID group configuration
 - Volume configuration
 - SAN: LUN provisioning
- Monitoring and reporting of disk space usage
- Triage and troubleshoot SAN/NAS infrastructure, performance and presentation issues
- Global settings/configuration management including LUN definitions
- SAN: Dynamic/Redundant path presentation. (may require proprietary multi-path software) (if applicable)

Client's Responsibilities and Out-of-Scope Notes *(unless otherwise covered via a different Item ID)*

- Data Backup (unless covered under additional Company services)

DRAFT

Item ID	Descriptions
80012	MANAGED SECURITY MONITORING AND INCIDENT RESPONSE
Company's Responsibilities and Included Features	
<p>Phase 1 – Validation: OneNeck validates “in-scope” services and devices:</p> <ul style="list-style-type: none"> ▪ Application and Operating System (OS) versions ▪ Peak and average Log volumes and bandwidth utilization ▪ Proper placement of ActiveGuard appliance(s) ▪ Appropriate information provided in Client Service Profile <p>Phase 2 – Device Configuration: OneNeck installs pre-configured ActiveGuard appliance(s) installation at Client site(s).</p> <p>Phase 3 – Installation: OneNeck installs ActiveGuard appliance(s) on network as determined in Phase 1 and configures “in-scope” devices to ensure appropriate communication with ActiveGuard appliance(s).</p> <p>Phase 4 – Implementation: OneNeck activates “in-scope” devices and confirms connectivity to the ActiveGuard appliance(s). This phase includes, but it not limited to, the following tasks:</p> <ul style="list-style-type: none"> ▪ Verify receipt of feeds from all “in-scope” sources ▪ Validate configuration of Client’s “in-scope” devices to receive appropriate Security Logs ▪ Validate Log format and compatibility with ActiveGuard classifiers ▪ Modify existing classifiers and LTAs if necessary ▪ Create new classifiers and LTAs for un-supported devices as indicated in the “Scope of Work” <p>Phase 5 – Normalization: ActiveGuard generates statistical analysis in accordance with the project plan and OneNeck works with Client to establish threshold criteria. The following activities during the Normalization process:</p> <ul style="list-style-type: none"> ▪ Ensure audit settings are configured appropriately ▪ Map software errors ▪ Establish Client specific baseline by Classifier ▪ Establish (with Client) minimum and maximum Log quantity thresholds in appropriate time intervals, specific to each Log source ▪ Issue a “Go-Live” notice for appropriate devices <p>Phase 6 – Ongoing Tuning and Support: This phase lasts for the duration of the SOW and consists of performing the following functions:</p> <ul style="list-style-type: none"> ▪ Generating events from ActiveGuard based on settings established during Normalization. ▪ Escalating Alerts based on documented escalation procedures. 	

Client's Responsibilities and Out-of-Scope Notes (unless otherwise covered via a different Item ID)

Client is responsible for providing or accepting all applicable license and maintenance agreements and service specification documents, including ActiveGuard® Monitoring Service Specifications Document", "Intersect Alliance End User License Agreement", "CorreLog End User License Agreement", "CorreLog Alliance Software Maintenance Agreement .

Item ID	Description
500070	Standard Backup Service (24hr RPO, 4hr RTO, 35 day retention)

Company's Responsibilities and Included Features

- RPO: 24 hours (Maximum continuous window of time that data loss may occur)
- RTO: 4 hour (Maximum allowable time to elapse until restoration of data begins)
- Retention: Last 35 days daily, last 180 days monthly (Maximum time window to choose a restoration point)
- Daily incremental (synthetic full) backups taken every 24 hours during Client specified backup window
- Weekly full backup taken during Client specified backup window
- Monthly full backup taken during Client specified backup window
- Backups processed from the Client hosted environment to Company backup storage infrastructure
- Backup job monitoring, reporting and notification
- Advanced administration support for backup infrastructure issues including triage of backup failures
- Support for initiating backup restorations (standard support SLA based on ticket severity)
- Company provided engineering support for agent software upgrades as dictated by server side application software
- Initial configuration of agent software and backend infrastructure components
- All subsequent adds/moves and changes to the agent and backend backup infrastructure including inclusions and exclusions from backup
- Incident ticket creation and tracking
- Service availability announcements (e.g. scheduled and unscheduled maintenance)
- Operate the service infrastructure and provide an escalation point for technical support related requests
- Management and execution of regular service operations
- Support and troubleshooting for Client side technical issues
- Service capacity management
- Implementation of major changes to the service
- Ad-Hoc technical requests
- Provide support to service desk and service administrator personnel and act as an escalation point
- Last line of support before escalating to vendor support for product issues

Client's Responsibilities and Out-of-Scope Notes (unless otherwise covered via a different Item ID)

- Responsible internally for service delivery to end users

Item ID	Description
500071	Economy Backup Service (File/VM only, 24hr RPO, 8hr RTO, 14 day retention)

Company's Responsibilities and Included Features

- Restricted to File System and VMware virtual machine backups only, no application agents
- RPO: 24 hours (Maximum continuous window of time that data loss may occur)
- RTO: 8 hour (Maximum allowable time to elapse until restoration of data begins)
- Retention: Last 30 days daily, last 180 days monthly (Maximum time window to choose a restoration point)
- Daily incremental (synthetic full) backups taken every 24 hours during Client specified backup window
- Weekly full backup taken during Client specified backup window
- Backups processed from the Client hosted environment to Company backup storage infrastructure
- Backup job monitoring, reporting and notification
- Advanced administration support for backup infrastructure issues including triage of backup failures
- Support for initiating backup restorations (standard support SLA based on ticket severity)
- Company provided engineering support for agent software upgrades as dictated by server side application software
- Initial configuration of agent software and backend infrastructure components
- All subsequent adds/moves and changes to the agent and backend backup infrastructure including inclusions and exclusions from backup
- Incident ticket creation and tracking
- Service availability announcements (e.g. scheduled and unscheduled maintenance)
- Operate the service infrastructure and provide an escalation point for technical support related requests
- Management and execution of regular service operations
- Support and troubleshooting for Client side technical issues
- Service capacity management
- Implementation of major changes to the service
- Ad-Hoc technical requests
- Provide support to service desk and service administrator personnel and act as an escalation point
- Last line of support before escalating to vendor support for product issues

Client's Responsibilities and Out-of-Scope Notes (unless otherwise covered via a different Item ID)

- Responsible internally for service delivery to end users

Item ID	Description
---------	-------------

500072	Remote Site Auxiliary Replication (requires Standard or Premium Backup service)
--------	---

Company's Responsibilities and Included Features

- Requires Standard backup services
- Auxiliary Copies: 1 (Additional replicas of the primary backup in a remote datacenter)
- Advanced administration support for backup infrastructure issues including triage of backup failures
- Support for initiating backup restorations (standard support SLA based on ticket severity)
- Company provided engineering support for agent software upgrades as dictated by server side application software
- Initial configuration of agent software and backend infrastructure components
- Incident ticket creation and tracking
- Service availability announcements (e.g. scheduled and unscheduled maintenance)
- Operate the service infrastructure and provide an escalation point for technical support related requests
- Management and execution of regular service operations
- Support and troubleshooting for Client side technical issues
- Service capacity management
- Implementation of major changes to the service
- Ad-Hoc technical requests
- Provide support to service desk and service administrator personnel and act as an escalation point
- Last line of support before escalating to vendor support for product issues

Client's Responsibilities and Out-of-Scope Notes (unless otherwise covered via a different Item ID)

- Responsible internally for service delivery to end users

DISASTER RECOVERY

Item ID	Description
---------	-------------

110031	Site Recovery Manager (SRM)
--------	-----------------------------

Company's Responsibilities and Included Features

- Includes VMware SRM or equivalent licensing for replication
- RPO definable from 30 minutes to 24 hours (depending on need/architecture)
- RTO of 24 hours or less
- VPS replication monitoring
- VMware licensing and maintenance including DRS and VMotion for optimum virtualized performance and reliability in disaster recovery site during Disaster Recovery event/usage
- Includes replication bandwidth within ReliaCloud infrastructure
- Includes support for disaster recovery testing of the environment (annual test)
- Work with Client to develop disaster recovery plan documentation

Client's Responsibilities and Out-of-Scope Notes (unless otherwise covered via a different Item ID)

--	--

- Disaster Recovery target machine resources (vCPU, RAM, Storage)
- Requires virtual machine production or Disaster Recovery instances to be hosted/managed at a Company qualified facility
- Requires guest virtual machine management in ReliaCloud environment
- Requires target SAN space allocation in disaster recovery site
- Requires Client connectivity and network design, deployment and management in stand-by Disaster Recovery facility
- Requires hypervisor virtual machine management in production and Disaster Recovery ReliaCloud environment

MANAGED DEDICATED HARDWARE

Item ID	Description
500065	Dedicated Blade Cisco UCS B200 M3 - 256GB
Company's Responsibilities and Included Features	
<p>The ReliaCloud dedicated blade service delivers a dedicated server blade solution to the Client with a fixed configuration of system resources. The dedicated blade model is designed to support a single operating system environment, verses a multiple operating system environment such as VMware.</p> <ul style="list-style-type: none"> - Provide access to a dedicated blade (not shared with another Client blade) - 2 Socket, 10 Cores of At least 3.0Ghz (~60Ghz total processor power) - 256 GB RAM - Requires SAN services for Storage. Storage services (LUNs) are directly mapped via 8GBPs fiber channel to the storage array. LUNs are not shared or accessible by other Clients. - Requires Managed O/S by Company - Basic setup of Blade configuration and load specified operating system. -The blades leverage an N+1 style model across the chassis. -24x7 expert-to-expert engineering support -Infrastructure maintenance and support - Notify Client of any detected host level issues - Maintain Blade Profile - Provide administrative O/S account(login) to Client 	
Client's Responsibilities and Out-of-Scope Notes <i>(unless otherwise covered via a different Item ID)</i>	
<ul style="list-style-type: none"> -Provide O/S and Application Licenses -Install application software and data 	

CLOUD TRANSPORT

Item ID	Description
110102	Ethernet VPLS Service - EDP to MSN

Company's Responsibilities and Included Features

The Ethernet VPLS Service is designed to provide connectivity between the Eden Prairie (EDP) and Madison (MSN) data centers in committed 10mbps increments. Service details:

- Managed transport services in committed increments of 10Mbps
- The port size for circuit is 1Gbps for service speeds between 10mbps and 1Gbps
- The service is designed and delivered as a non protected route, with single electronics, and a single handoff at each location
- Service delivery support on Cat5e (Copper) or Fiber
- The service is a layer 3 private connection meaning no other Client can see or share the traffic on the same service segment.
- VLAN Tagging is allowed (single or double)
- Service supports 9000 byte layer 3 IP frames
- Service doesn't provide any encryption level services such as IPSec, or GRE.
- The service has a performance target of 10ms round trip time (RTT) as tested via ICMP ping originating from and terminating on Company equipment.
- The services requires a cross-connection from Telco room(s) to the Client terminating devices
- Provide notification the Client of any performance challenges or link-state issues with the service
- Provide monitoring statistics for port bandwidth

Client's Responsibilities and Out-of-Scope Notes (unless otherwise covered via a different Item ID)

- Provide termination equipment at both ends of the service
- Manage termination equipment infrastructure
- Ensure termination equipment supports Ethernet service delivery
- Ensure termination equipment has throughput capacity to support the contract service speeds
- For the purpose of troubleshooting, provide physical or administrative level access

MANAGED SERVICES

Monitoring

- Hardware port (when applicable)
- System performance thresholds
- Critical services
- Non-security event log monitoring

Reporting

- Performance via Client portal
- Standard dashboard

Patching and Updating

- On-going assessment of critical OS/Application security patches
- Apply, test and troubleshoot critical security patches and updates during maintenance window
- Install, test and troubleshoot service packs during maintenance window
- Install, test and troubleshoot OS bug fixes

Incident Management

- Alerts sent to Client via email based on event severity and escalated by phone
- Hardware and software vendor escalation
- Execute Client escalation procedures
- Troubleshoot incidents and problems
- Assess potential hardware failure
- 24x7x365 help desk support

Configuration Management

- Manage administrative access and ownership
- Maintain access permissions and control list
- Perform startup/shutdown of physical device
- Audit access rights

Security Management

- Monitor anti-virus for signature updates (when applicable)
- OS hardening using a secure OS template (when applicable)

MANAGED SERVERS

Hardware Maintenance Management

- Manage hardware replacement and or repair with hardware vendor
- Perform analysis of any hardware additions or upgrades
- Apply hardware BIOS updates as necessary

Security Management Services

- Provisioning and maintenance of OS local user security and permissions
- Management of any standard operating system security features

Server Management Documentation

- Document applicable hardware and OS administration procedures and policies

System Administration

- Operating system configuration
- Performance tuning

MANAGED SERVERS ITEMS

Item ID	Description
100031	Microsoft Windows Server Management
Company's Responsibilities and Included Features	
<p>Antivirus management of file systems and operating system</p> <ul style="list-style-type: none"> - Installation of a managed antivirus console - Application of updates and patches to the antivirus software on server platforms only - Configuration and validation of virus protection and scanning on server platforms only 	
<p>Built in OS Applications Management</p> <p>Administration of "built-in" OS components that are bundled with the OS:</p> <ul style="list-style-type: none"> - Performance Monitor - Teaming Software - Device Manager - DHCP - DNS - WINS <p>Excluding:</p> <ul style="list-style-type: none"> - Terminal Services Licensing/Terminal Server Gateway - Windows SharePoint Services (WSS) - Active Directory Services/ADAM/ADFS - Server Virtualization Services - Application Server(s) IIS/WWW-IIS/FTP-IIS/SMTP - Certificate Services- Certificate Authority - Distributed File System - DFS Management/DFS Replication Services 	
<p>Virus Protection Software Licensing</p> <ul style="list-style-type: none"> - Procurement of virus protection software and licensing for current version of virus protection system 	

- Provide software media for installation, maintenance and configuration of the software
- Procurement of current software maintenance where applicable

Windows Server Monitoring

- Installation of monitoring agents where applicable
 Configuration of monitoring thresholds and parameters
- Monitoring and reporting of key metrics including:
 - Disk utilization
 - Processor load
 - Memory usage

Operating System Patch Management

- Periodic review of Microsoft Operating System updates (Critical/Important/Security)
- Review of updates to be applied to server(s)
- Change notice submission, approval and application of updates

Operating System Upgrades

- Periodic next version analysis and recommendations
- Upgrades to a new major version of the operating system or embedded OS application will be provided on a time and material project basis

Client's Responsibilities and Out-of-Scope Notes (unless otherwise covered via a different Item ID)

End User Support

- Support of non-expert OS users (typically refers to non-IT department staff or application end users)

Hardware Maintenance Coverage

- Procurement of hardware maintenance
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Ensure that Company is an authorized caller to maintenance service providers

Operating System Software Licensing*

Procurement of OS software and licensing for current version of operating system, including any user access licensing
 Provide software media for installation

Procurement of current software maintenance where applicable

* Servers deployed on Company's ReliaCloud platform include a license for supported versions of Microsoft Server

Remote Hardware Support

Designate a person or group to perform the following types of "hands and eyes only" activities on an ad hoc or regular basis as defined by the applicability of device being supported:

- Rack and connect device
- Backup tape handling.
 - Insert and remove backup tapes as directed by a Company administrator.
 - Provide and manage offsite tape storage if required
- Provide accompanied access to the device for maintenance technicians
- Provide ad hoc on-site non-technical "hand and eyes only" support under direction of a Company administrator to assist in device management

Item ID	Description
---------	-------------

100019	Linux Server Management
--------	-------------------------

Company's Responsibilities and Included Features

Server Monitoring

Installation of monitoring agents where applicable
 Configuration of monitoring thresholds and parameters

- Monitoring and reporting of key metrics including:
 - Disk space usage
 - Disk IO
 - Hardware logs
 - Special plug-ins (like PowerPath)
 - Processor load
 - Memory usage
 - Processes (abandoned and run-away)
 - Server availability

Operating System Patch Management

- Periodic reviews of critical patches
- Quarterly routine review of same-version patch
- Application of updates and patches during approved maintenance windows

Operating System Upgrades

- Periodic next version analysis and recommendations

Upgrades to a new major version of the operating system or embedded OS application will be provided on a time and material project basis

Client's Responsibilities and Out-of-Scope Notes (unless otherwise covered via a different Item ID)

End User Support

- Support of non-expert OS users (typically refers to non-IT department staff or application end users)

Hardware Maintenance Coverage

- Procurement of hardware maintenance
- Provide contract numbers and phone numbers for applicable hardware maintenance service providers
- Ensure that Company is an authorized caller to maintenance service providers

Operating System Software Licensing

- Procurement of OS software and licensing for current version of operating system, including any user access licensing
- Provide software media for installation
- Procurement of current software maintenance where applicable

Remote Hardware Support

Designate a person or group to perform the following types of "hands and eyes only" activities on an ad hoc or regular basis as defined by the applicability of device being supported:

- Rack and connect device
- Backup tape handling.
 - Insert and remove backup tapes as directed by a Company administrator.
 - Provide and manage offsite tape storage if required
- Provide accompanied access to the device for maintenance technicians

Provide ad hoc on-site non-technical "hand and eyes only" support under direction of a Company administrator to assist in device management

Item ID	Description
100051	VMware Host Server Management
Company's Responsibilities and Included Features	
<ul style="list-style-type: none"> - Scope is covered under item category descriptions. 	
Company's Responsibilities and Included Features	
<p>End User Support Support of non-expert OS users (typically refers to non-IT department staff or application end users)</p> <p>Hardware Maintenance Coverage</p> <ul style="list-style-type: none"> - Procurement of hardware maintenance - Provide contract numbers and phone numbers for applicable hardware maintenance service providers - Ensure that Company is an authorized caller to maintenance service providers <p>Operating System Software Licensing</p> <ul style="list-style-type: none"> - Procurement of OS software and licensing for current version of operating system, including any user access licensing - Provide software media for installation - Procurement of current software maintenance where applicable <p>Remote Hardware Support Designate a person or group to perform the following types of "hands and eyes only" activities on an ad hoc or regular basis as defined by the applicability of device being supported:</p> <ul style="list-style-type: none"> - Rack and connect device - Backup tape handling. <ul style="list-style-type: none"> - Insert and remove backup tapes as directed by a Company administrator. - Provide and manage offsite tape storage if required - Provide accompanied access to the device for maintenance technicians - Provide ad hoc on-site non-technical "hand and eyes only" support under direction of a Company administrator to assist in device management <p>Third Party VMware Utilities and Applications</p> <ul style="list-style-type: none"> - Management of third party VMware enhancement tools, utilities or applications 	

MANAGED APPLICATIONS

Patch Management

- Monthly review of critical patches in collaboration with underlying OS administrator
- Up to quarterly routine review same version patch analysis and application
- Application of updates and patches during approved maintenance windows

Incident Diagnosis and Resolution

- Diagnosis of system incidents
- Resolutions of system incidents
- Engagement of software providers Help Desk support
- Where necessary Company will engage and log service requests with the software vendor to rectify software issues
- Provide Client with updates
- Document user issues and system errors

MANAGED APPLICATIONS ITEMS

Item ID	Description
900082	Microsoft Active Directory Management
Company's Responsibilities and Included Features	
Active Directory Reporting	
<ul style="list-style-type: none">- Reporting of user counts- Disabled/inactive accounts	
Domain User Administration	
Provisioning of Active Directory domain users:	
<ul style="list-style-type: none">- Group Membership updates- Password resets- Termination of Active Directory domain users	
Single Domain Forest (Standard)	
System administration of a single forest, single domain including:	
<ul style="list-style-type: none">- Local DNS configurations- Design/Implement Active Directory roles (FSMO/GC placement)- AD sites & subnets definition<ul style="list-style-type: none">- Creation of site(s)- Creation of AD replication topology- Creation of inter-site connectors- Creation of subnets and assigned to site(s)- Design/Implement - OU container structure- Develop/Implement - logon scripts (limited to printer and drive mapping)- Implement - Group Policy Objects- Develop/implement security groups / distribution groups- Delegation of administrative roles- Domain controller promotions- Domain controller demotions- Removal of Active Directory roles (FSMO or GC)	

- Removal of domain controller object from sites and subnets
- Domain Admins/Enterprise Admins access is limited to Company

End User Support

24 x 7 end user helpdesk support related to:

- Password resets
- Account lockout resets

Client's Responsibilities and Out-of-Scope Notes (unless otherwise covered via a different Item ID)

Active Directory Policy

Define Active Directory domain policy including:

- User naming standards
- Account password policy
- Account Lockout policy
- User add/change/delete policy
- Security policies

Advanced User Identity/Credential Management:

Administration of advanced identity or credential managements system, i.e:

- Biometric identities
- Smart cards
- RSA tokens

DRAFT

Item ID	Description
80010	SQL Managed Environment

Company's Responsibilities and Included Features

Database Incident Diagnosis and Resolution

- Diagnosis of database system incidents
- Resolution of database system incidents
- Engagement of database software providers help desk support
- Document user issues and database system errors

Database Management Documentation

- Document applicable database administration procedures

Database Software Patch Management

- Monthly reviews of critical patches
- Up to quarterly routine review same-version patch analysis and application
- Periodic next version upgrade analysis and recommendations
- Application of updates and patches during approved maintenance windows

Major of Point Release Upgrades

- Any Major or Point release version upgrades will be scheduled as an independent project and shall be billed to Client on a time and materials basis as agreed upon by the Parties.

Database Instance Management

An instance of SQL is defined as the set of Microsoft SQL Server software or set of SQL server binaries loaded on a single instance of the operating system. Multiple instances of MS SQL may occur on a single instance of a MS Windows OS

Database Instance Monitoring

Configuration of database instance monitoring thresholds and parameters

- Monitoring and reporting of key metrics including:
 - Database availability
 - SQL Services

Database Management Documentation

- Document applicable database administration procedures

SQL Database Security Management

- User creation and security maintenance
 - Database authentication management via SQL authentication
- Database encryption management where appropriate

SQL database administration is defined as the tasks to maintain the individual databases on an existing SQL instance managed by OneNeck.

Management Tasks - These tasks includes management and tuning the following areas within the database:	
Task	
Transaction log maintenance	Yes
Memory utilization/configuration	Yes
Transaction log files	Yes
Table and index storage parameters	Yes
Table and index fragmentation	Yes
Database storage parameters	Yes
Database configuration options	Yes
Table statistics	Yes
Database issues such as table locks/record contention	Yes
Deployment of Schema changes	Yes
Recommendations/Review - Review and/or make recommendations within the following areas:	
Task	
Physical and logical disk layout AND new database provisioning	Yes
Physical and logical disk layout	Yes
Backup and disaster recovery design strategies based on business needs	Yes
Repository database creation for reporting or other peripheral tools creation	Yes
Redistribution of data files	Yes
* Implementation of recommendations will be handled on a per project T&M basis	
Database Incident Diagnosis and Resolution	
Task	
Diagnosis of database system incidents	Yes
Resolution of database system incidents	Yes
Engagement of database software providers help desk support	Yes
Document user issues and database system errors	Yes
Database Monitoring	
Configuration of database monitoring thresholds and parameters. Monitoring and reporting of key metrics including:	
Task	
Database availability	Yes
Space usage	Yes
Database Backup Management	
Task	
Configuration of database backup	Yes
Monitoring of database backup status	Yes
Rectification and resubmission of failed backup jobs as appropriate	Yes
Adhoc backup or restore on request, limited to four per year	Yes
Quarterly test restores	Yes
SQL Database Security Management	
Task	
User creation and security maintenance	Yes
Database authentication management via SQL authentication	Yes
Database encryption management where appropriate	Yes
Database Cloning	
Task	
Cloning/copying/refreshing of databases to a non-production environment for system testing, training or development. Requires a 5 business day notification for planning.	Yes
Database Management Documentation	
Task	
Document applicable database administration procedures	Yes

Client's Responsibilities and Out of Scope Notes:

Existing SQL Instance

- This service requires the existence of a Microsoft SQL instance already managed by Company

Third Party Application Dependency Management

- Management of third party application interface to the database

Domain User Administration

Provisioning of Active Directory domain users:

- Group Membership Updates
- Password resets
- Termination of Active Directory domain users
- No change notice required for User Administration

Third Party Application Dependency Management

- Management of third party application interface to the database

Database Schema and Content Management

- Development and/or customization of database schema

MANAGED NETWORKS

Hardware Maintenance Management

- Manage hardware replacement and or repair with hardware vendor
- Perform analysis of any hardware additions or upgrades
- Apply hardware IOS\OS updates as necessary

Software Management

- Global device configuration including:
 - Management interface IP (if needed)
 - Basic device parameters
 - AAA configuration
 - NTP service configuration (if needed)
 - Troubleshooting of IOS/OS issues
 - IOS\OS patch\upgrade management
 - Configuration backups

MANAGED NETWORKS ITEMS

Item ID	Description
100297	Dedicated Layer-3 Switch Management w/ Basic Routing (up to 48 ports)
Company's Responsibilities and Included Features	
<p>Layer 2 Switch Management</p> <ul style="list-style-type: none">- Spanning tree configuration- VLAN assignment- Port assignment- EtherChannel configuration and management- 802.1Q VLAN trunk configuration and management <p>Layer 3 Switch Management (Basic)</p> <ul style="list-style-type: none">- Management of interface IP addresses- Configuration of basic routing (Static, RIP, IGRP/EIGRP, single-area OSPF, etc.)- IP interface availability monitoring and performance reporting- NTP service management if needed	
Client's Responsibilities and Out-of-Scope Notes <small>(unless otherwise covered via a different Item ID)</small>	
<p>Hardware Maintenance Coverage</p> <ul style="list-style-type: none">- Procurement of hardware maintenance- Provide contract numbers and phone numbers for applicable hardware maintenance service providers- Ensure that Company is an authorized caller to maintenance service providers	

MANAGED SECURITY ITEMS

Item ID	Description
100288	Dedicated Security Appliance/Firewall Management (up to 500 rules)
Company's Responsibilities and Included Features	
<p>Basic Firewall Management Basic firewall rules including:</p> <ul style="list-style-type: none">- Address translation (NAT/PAT)- Firewall rule management- Cluster configuration (if needed)- L2L VPN tunnel configuration and support- RAVPN (client based or AnyConnect; only when firewall is NOT contextualized) configuration and support- Supports local DB and LDAP authentication	
<p>Hardware Maintenance Management</p> <ul style="list-style-type: none">- Manage hardware replacement and or repair with hardware vendor- Perform analysis of any hardware additions or upgrades- Apply hardware IOS\OS updates as necessary	
<p>Remote Access VPN Management Deployment and support of Client based remote access VPN including:</p> <ul style="list-style-type: none">- Group policy definitions- External user database authentication integration- Certificate management- Client VPN access utilizing Cisco client software- Limited to 20 named users if local device authentication is used	
<p>Site-to-site VPN Management</p> <ul style="list-style-type: none">- Management of the VPN tunnel configurations on one side of a point-to-point VPN connection- Troubleshooting/support of VPN tunnel establishment	
Client's Responsibilities and Out-of-Scope Notes <i>(unless otherwise covered via a different Item ID)</i>	
<p>Hardware Maintenance Coverage</p> <ul style="list-style-type: none">- Procurement of hardware maintenance- Provide contract numbers and phone numbers for applicable hardware maintenance service providers- Ensure that Company is an authorized caller to maintenance service providers	
<p>Internet Connectivity</p> <ul style="list-style-type: none">- Internet connectivity with sufficient bandwidth	

PRICING DETAILS

MONTHLY RECURRING FEES

Item ID	Description	Location	UOM	QTY	Unit Price	Total Price
80027	Monthly Archive Tape	ANY	Each	1	\$600.00	\$600.00
100031	Microsoft Windows Server Management	ANY	Each	278	\$120.22	\$33,421.16
900082	Microsoft Active Directory Management	ANY	Group	1	\$1,064.57	\$1,064.57
100019	Linux Server Management	ANY	Each	12	\$120.22	\$1,442.64
100288	Dedicated Security Appliance/ Firewall Management (up to 500 rules)	ANY	Device	2	\$188.58	\$377.16
100288	Dedicated Security Appliance/ Firewall Management (up to 500 rules)	ANY	Device	2	\$188.58	\$377.16
80029	OneNeck Connect - EDP to MKE	ANY	Each - 1 Gbps	1	\$3,000.00	\$3,000.00
80016	OneNeck Connect - WAN Link Demarc Switches	ANY	Each	2	\$528.57	\$1,057.14
100297	Dedicated Layer-3 Switch Management w/ Basic Routing (up to 48 ports)	ANY	Device	2	\$224.99	\$449.98
80012	AG Enterprise Monitoring ONLY of one (1) Firewall/VPN <2Gb Cisco ASA Firewalls - High Availability Pairs	ANY	Each	2	\$625.00	\$1,250.00
80012	AG Enterprise Monitoring ONLY of one (1) Network-based IDS/IPS <2Gb Cisco ASA IPS Modules - High Availability Pairs	ANY	Each	2	\$1,000.00	\$2,000.00

Item ID	Description	Location	UOM	QTY	Unit Price	Total Price
80012	AG Enterprise Monitoring ONLY of Security Event Logs from z/OS - per LPAR (<= 5 users or user groups AND <= 5,000,000 logs per month)	ANY	Each	0	\$1,250.00	\$0.00
80012	AG Enterprise Monitoring ONLY of Linux Servers - per device	ANY	Each	12	\$41.66	\$499.92
80012	AG Enterprise Monitoring ONLY of Windows Servers - per device	ANY	Each	81	\$41.66	\$3,374.46
80012	AG Enterprise Monitoring ONLY of VMWare ESX Hosts - per device	ANY	Each	11	\$41.66	\$458.26
80012	Enterprise Snare Agent use license & support for Windows Servers (including Domain Controllers) - per device per year	ANY	Each	295	\$1.35	\$398.25
80012	Vulnerability-Threat Correlation (VTC) Customer brings and imports their own data; (up to 2,000 IPs or FQDNs)	ANY	Each	1	\$583.34	\$583.34
80012	AG Enterprise Monitoring ONLY of Security Event Logs from Domain Controllers Based on up to 25 DCs and up to 5,000 User/Service Accounts	ANY	Each	1	\$1,770.84	\$1,770.84
80012	AG SEIM Monitoring ONLY of Windows Servers - per device	ANY	Each	54	\$8.34	\$450.36
80012	AG HPA Monitoring ONLY of Windows Servers - per device	ANY	Each	135	\$18.75	\$2,531.25
80010	Microsoft SQL Management	ANY	Each	1	\$4,934.22	\$4,934.22

Item ID	Description	Location	UOM	QTY	Unit Price	Total Price
100051	VMware Host Server Management	ANY	Each	8	\$365.00	\$2,920.00
100051	VMware Host Server Management	ANY	Each	3	\$365.00	\$1,095.00
500143	Silver - Block level storage services (NextGen)	EDP	GB	23373	\$0.15	\$3,505.95
500149	Bronze - Block level storage services (NextGen)	EDP	GB	2232	\$0.10	\$223.20
110003	Colocation Internet Committed	EDP	Mbps	100	\$5.00	\$500.00
110004	Colocation Internet Burstable	EDP	Mbps	0	\$5.00	\$0.00
110048	RIC LAN Connection 1Gbps	EDP	Port	9	\$41.27	\$371.43
110046	ReliaCloud Integration Cabinet (RIC)	EDP	140W	10	\$33.60	\$336.00
110047	RIC LAN Connection 10Gbps	EDP	Port	4	\$81.67	\$326.68
110102	Ethernet VPLS Service - EDP to MSN	EDP	10 mbps	100	\$5.00	\$500.00
110052	Virtual Router Service	EDP	Port	1	\$88.33	\$88.33
80026	Managed Dedicated Firewall	EDP	Each	2	\$3,020.44	\$6,040.88
500065	Dedicated Blade Cisco UCS B200 M3 - 256GB	EDP	Blade	3	\$825.40	\$2,476.20
110031	Site Recovery Manager (SRM)	MSN	Per VM	76	\$43.52	\$3,307.52
500143	Silver - Block level storage services (NextGen)	MSN	GB	62757	\$0.15	\$9,413.55
500149	Bronze - Block level storage services (NextGen)	MSN	GB	15599	\$0.10	\$1,559.90
110005	Additional IPv4 Internet Public Addresses Space	MSN	Per IP	128	\$2.86	\$366.08
110003	Colocation Internet Committed	MSN	Mbps	100	\$5.00	\$500.00
110004	Colocation Internet Burstable	MSN	Mbps	0	\$5.00	\$0.00
110048	RIC LAN Connection 1Gbps	MSN	Port	9	\$41.27	\$371.43
110046	ReliaCloud Integration Cabinet (RIC)	MSN	140W	10	\$33.60	\$336.00
110047	RIC LAN Connection 10Gbps	MSN	Port	4	\$81.67	\$326.68
80016	Virtual Router Service - 10 Gbps	MSN	Each	2	\$300.00	\$600.00
500070	Standard Backup Service (24hr RPO, 4hr RTO, 35 day retention)	MSN	GB Protected	62757	\$0.25	\$15,689.25

Item ID	Description	Location	UOM	QTY	Unit Price	Total Price
500071	Economy Backup Service (File/VM only, 24hr RPO, 8hr RTO, 14 day retention)	MSN	GB Protected	8928	\$0.20	\$1,785.60
500072	Remote Site Auxiliary Replication (requires Standard or Premium Backup service)	MSN	GB	62757	\$0.04	\$2,510.28
80026	Managed Dedicated Firewall	MSN	Each	2	\$3,020.44	\$6,040.88
80029	OneNeck Connect - MSN to MKE	MSN	Each - 10 Gbps	2	\$6,500.00	\$13,000.00
110045	Global Load Balancing Service	MSN	Domain	2	\$95.02	\$190.04
500065	Dedicated Blade Cisco UCS B200 M3 - 256GB	MSN	Blade	8	\$825.40	\$6,603.20

TOTAL MONTHLY FEES: \$141,024.79

ONE TIME IMPLEMENTATION FEES

Item ID	Description	Unit Price
80015-N	Server Services	\$ 390,000
80015-N	Storage and Backup Services	\$ 45,000
80015-N	Network Services	\$ 75,000
80015-N	Security Services	\$ 105,000
80015-N	Data Circuits Costs	\$ 20,000
80015-N	Disaster Recovery Services	\$ 97,000
Total		\$ 732,000

PRICING SUMMARY

CONTRACT TERM 60 MONTHS

MONTHLY RECURRING FEES \$141,024.79

The number provided is an estimated total monthly service price. The quantities listed are assumed service totals for the first billed month, and may not represent future growth numbers for your organization.

NON RECURRING FEES \$732,000.00

The total cost for the professional services associated with the service turn-up and installation of the proposed solution. Please see the service transition scope for more details.

PRICING VALID UNTIL June 30, 2016

SUMMARY NOTES

Pricing reflects discounts associated with a 60 month term. Modification to contract term can affect unit prices.

Pricing reflects discounts with commitments to unit volume. Modification to unit quantity / volume levels can affect unit prices.

Professional Services will be contracted separately between the parties on an hourly basis or fixed project basis, and will be billed monthly based on either a percentage of project completed or hours provided, as applicable.

Item ID Number 80029 OneNeck Connect - EDP to MKE and OneNeck Connect - MSN to MKE will be at the discretion of Client. Client may choose to contract that item directly with carriers.

First full contract billing will occur following the Commencement Date as identified in the Acceptance and Commencement Addendum executed by Company and Client ("Commencement Date"). Services provided during the service transition period shall be billed monthly.

This SOW is limited to the scope of services specifically identified herein. Any services identified in the Milwaukee County Data Center Operations Professional Services RFP dated November 2015 ("RFP") which are not included herein are outside of the scope of services being provided by Company.

Upon the Effective Date of this SOW, the Parties will commence a 90 day discovery period to verify the scope of services to be provided hereunder. The Parties will enter into an amendment to this SOW to reflect any deviation from the terms of the SOW following such discovery period.

Unit pricing as provided herein will remain unchanged for the Initial Term of this SOW, provided the monthly recurring fees are not reduced by more than 25% of the amounts stated herein.

DELIVERY SCOPE

Item ID	Description
800016	Virtual Router Service 10 Gbps

Company's Responsibilities and Included Features

The Virtual Router Service 10 Gbps provides endpoint termination equipment for metroE class services for up to 10Gbps in size.

The service is delivered via a single port, 10 Gbps interface.

- Provide managed LAN services which provides speeds up to 10Gbps
- Service is layer 3
- Includes cross-connection from telco room to ReliaCloud WAN infrastructure
- Deliver services over Fiber
- Design, manage and maintain VLAN configuration
- Maintain ACLs
- Notify Client of any performance challenges or link-state issues with the service
- Provide monitoring statistics on port speed and performance
- Service is not designed for Internet Routing table
- Service does not provide VPN termination

Client's Responsibilities and Out-of-Scope Notes

- Secure Telco services contract with vendor
- Financial responsibility of contract with Telco vendor
- Ensure Telco vendor does not require the delivery and hosting of a vendor provided managed device
- Provide endpoint for termination
- Provide configuration services for WAN turn-up on remote devices

Item ID	Description
80027	Monthly Archive Tape (requires Standard or Premium Backup service)

Company's Responsibilities and Included Features

Company will provide a monthly archive tape service.

Company will provide the following services:

- Tapes produced from primary data center
- Tapes provided by Company

Client's Responsibilities and Out-of-Scope Notes

- Requires Standard or Premium Backup service

Item ID	Description
80026	OneNeck Connect – Managed Dedicated Firewall

Company's Responsibilities and Included Features

Company's Responsibilities and Included Features:

This service provides a Cisco ASA firewall with the Firepower IPS module. This appliance is dedicated for the Client's exclusive use within the Company's data center. This device is comprised of the following configuration.

Manufacturer Part #	Description	Qty
	ASA 5585-X SSP-10	
ASA5585-S10F10XK9	ASA 5585-X SSP-10, FirePOWER SSP-10,16GE,4SFP+,2AC,3DES/AES	1
CON-SNT-A85S1F10	SNTC-8X5XNBD ASA 5585-X SSP-10, FirePOWER SSP-10,16GE	1
ASA5585-BLANK-HD	ASA 5585-X Hard Drive Blank Slot Cover	2
ASA5585-10CTRL-LIC	Cisco ASA5585-10 Control License	1
CAB-US620P-C19-US	NEMA 6-20 to IEC-C19 13ft US	2
ASA5585-PWR-AC	ASA 5585-X AC Power Supply	1
SF-ASA-X-9.2.2-K8	ASA 9.2.2 Software image for ASA 5500-X Series,5585-X,ASA-SM	1
ASA5500-SC-20	ASA 5500 20 Security Contexts License	1
ASA-VPN-CLNT-K9	Cisco VPN Client Software (Windows, Solaris, Linux, Mac)	1
ASA-SSP-10-INC	ASA 5585-X SSP-10 with 8GE,2SFP, incl with bundle	1
ASA5500-ENCR-K9	ASA 5500 Strong Encryption License (3DES/AES)	1
ASA5585-PWR-AC	ASA 5585-X AC Power Supply	1
ASA-ANYCONN-CSD-K9	ASA 5500 AnyConnect Client + Cisco Security Desktop Software	1
ASA5585-SEC-PL	ASA 5585-X Security Plus License (Enables 10G SFP+ Ports)	1
ASA-SFR-10-INC-K9	ASA 5585-X FirePOWER SSP-10, 8GE	1
SF-FP5.3.1-K9	Cisco FirePOWER Software v5.3.1	1

	Cisco ASA5585-10	
L-ASA5585-10-TA=	Cisco ASA5585-10 FirePOWER IPS License	1
L-ASA5585-10-TA3Y	Cisco ASA5585-10 FirePOWER IPS 3YR Subscription	1
	Cisco FireSIGHT Management Center	
FS-VMW-2-SW-K9	Cisco FireSIGHT Management Center,(VMWare) for 2 devices	1
CON-SAU-VMWSW2	SW APP SUPP + UPGR Cisco FireSIGHT Mana	1
	Cisco AnyConnect	
L-AC-APX-3YR-G	Cisco AnyConnect / RA VPN 3-Yr Apex License Group	1
AC-APX-3YR-25-S	Cisco AnyConnect 3-Yr 25 User Apex License	1
AC-APX-3YR-25	Cisco AnyConnect 3-Yr 25 User Apex Subscription	1
AC-APX-3YR-50-S	Cisco AnyConnect 3-Yr 50 User Apex License	1
AC-APX-3YR-50	Cisco AnyConnect 3-Yr 50 User Apex Subscription	1
L-AC-APX-S-3Y-25	Cisco AnyConnect 3-Yr 25 User Apex (ASA License Key)	99999
L-AC-APX-S-3Y-50	Cisco AnyConnect 3-Yr 50 User Apex (ASA License Key)	99999
	SFP Module	
SFP-10G-SR=	10GBASE-SR SFP Module	2

Client's Responsibilities and Out-of-Scope Notes

- This product requires the firewall to be managed by Company

Item ID	Description
---------	-------------

80016	OneNeck Connect - WAN Link Demarc Switches
-------	--

Company's Responsibilities and Included Features

This service provides a switch that will be the demarcation for Company services within the Client’s data center. This device is comprised of the following configuration..

Manufacturer Part #	Description	Qty
	WS-C3850-12XS-S	
WS-C3850-12XS-S	Cisco Catalyst 3850 12 Port 10G Fiber Switch IP Base	1
CON-SNTP-WSC3851X	SNTPC-24X7X4 Cisco Catalyst 3850 12 Port 10G Fiber Sw	1
S3850UK9-37E	CAT3850 Universal k9 image	1
CAB-TA-NA	North America AC Type A Power Cable	1
STACK-T1-50CM	50CM Type 1 Stacking Cable	1
SFP-10G-LRM=		
GLC-SX-MMD=	1000BASE-SX SFP transceiver module, MMF, 850nm, DOM	1

Client's Responsibilities and Out-of-Scope Notes

- Provide secured cabinet space within Client’s data center and LAN connectivity to the Client’s network.
- Provide power within Client’s data center and connectivity to the Client’s network.
- Provide remote hands assistance to Company and or escorted access to Company or supported manufacturer for the purpose of hardware replacement or troubleshooting.
- This product requires the device to be managed by Company

Item ID	Description
80029	OneNeck Connect - EDP to MKE

Company's Responsibilities and Included Features

Company will provide a single backup 1 Gbps connection from the 949 North 9th Street, Milwaukee, WI 53233 location to 10290 70th Street W, Eden Prairie, MN 55344 data center.

Company will provide the following services:

- 1 connection Milwaukee County data center to EDP data center

Client's Responsibilities and Out-of-Scope Notes

- Provide entrance into Milwaukee County data center location for each connection
- Provide cross connection to Company WAN Link Demarc switches and connectivity into Client's network

Item ID	Description
80029	OneNeck Connect - MSN to MKE

Company's Responsibilities and Included Features

Company will provide a pair of 10 Gbps connections that are carrier and path diverse. Connections will come from two separate entrances at the 949 North 9th Street, Milwaukee, WI 53233 location to 5515 Nobel Dr, Fitchburg, WI 53711 MSN data center.

Company will provide the following services:

- 2 diverse 10 Gbps links from Milwaukee County data center to MSN data center

Client's Responsibilities and Out-of-Scope Notes

- Provide entrance into Milwaukee County data center location for each connection
- Provide cross connection to Company WAN Link Demarcation switches and connectivity into Client's network

SERVICE MANAGEMENT

SERVICE MANAGEMENT OVERVIEW

OneNeck is primarily responsible for incident management, service request management, change management, problem management, and configuration management for all technology components that it manages on behalf of the customer. This includes notifications, escalations, and other necessary communications to the customer to fulfill the service. The specifics regarding the detailed escalations and contacts are developed as part of the transition process and are subject to change as the customer environment and staffing model evolves.

SERVICE MANAGEMENT SERVICE LEVEL MEASURES

INCIDENT MANAGEMENT

Service Level
All Incident Resolution Times for Priority 1 Events shall be less than or equal to 4.0 hours
(a) 98.00% of Incident Response Times for Priority 1 Events shall be less than or equal to 15.0 minutes; and (b) 100.00% of Incident Response Times for Priority 1 Events shall be less than or equal to 20.0 minutes
Completion time for root cause analyses shall be less than or equal to 15.0 Business Days
(a) No more than 4.0 Chronic Incidents shall occur during any Measurement Period; and (b) For any planned remediation activity for a Chronic Incident that is scheduled to be completed during a Measurement Period, Company shall complete such remediation activity in accordance with such schedule

SERVICE REQUEST COMPLETION TIME

Service Level
90.00% of Service Request Completion Times shall be less than or equal to their corresponding completion time set forth in Table 1

Table 1 SERVICE REQUESTS AND TARGET COMPLETION TIMES

Service Request	Completion Time
Computing Service Services	
• Server - reboot	2.0 hours
• System parameters - modify	2.0 hours
• Password reset	30.0 minutes
• Virtual machine - Clone or create (where addition of a new blade is not required)	6.0 hours
• Virtual machine - Modify (CPU, memory, storage)	8.0 hours
• Virtual machine - Remove	6.0 hours
Network Service Services	
• Firewall and router access control list additions, deletions or modifications (10 or less)	24.0 hours
• Adding, enabling, disabling or modifying existing router or switch ports (10 or less)	24.0 hours
Managed Security Services	
• Configuration management - standard rule changes	24.0 hours
• Configuration management - emergency rule changes	(a) 4.0 hours if the request is initiated during the hours of 8:00 a.m. - 8:00 p.m. CT; and (b) 8.0 hours if the request is initiated outside of the time period referenced in (a).
• Event notification	(a) 15.0 minutes for Severity 1 Events; and (b) 24.0 hours for Severity 2 Events and Severity 3 Events

SERVICE LEVEL AGREEMENT

The terms and conditions of this Service Level Agreement ("SLA") shall apply to the Services provided by Company to Client. This SLA is subject to and conditioned upon Client's compliance with the terms herein, the MSA, and the Acceptable Use parameters, if applicable, and as described below.

Company will provide the Services in accordance with the SLAs described in this Section. If Company fails to meet these SLAs, Client will be eligible for a Service Credit. The Service Credit represents an estimate of the costs associated with failure to meet the SLAs and shall not be deemed or construed as a penalty.

Service Credits will be calculated from the time unavailability is reported to Company by Client or logged by Company and a "trouble-ticket" is generated by Company.

DEFINITIONS

Compute: A specific amount of RAM ('pool') made available to the client for provisioning of virtual machines within their organizational environment.

Desktop Workstations: A desktop computer, a laptop computer, or a tablet computer which is intended to be operated directly by an end user and is limited to Microsoft operating systems.

Net Monthly Base Fees (Net MBF): The monthly recurring charge for the services excluding any add-on or optional services which are not included as part of the base service plan but are included as part of such Client's monthly recurring charge.

Network: Virtual firewalls and/or load balancer services made available to the Client organizational environment and include only the Client's access ports (the ports on the Company devices within the Company facility upon which the Client's local circuit terminates).

Scheduled Downtime: The time during which the Services are not available due to planned Company maintenance.

Service Credit: The credit(s) provided to Client in accordance with the SLA.

Services: Shall mean and include only such Services described in this SOW that the Client has purchased from Company.

SLAs: On a collective basis the service level agreements described in this SLA.

Storage: The specific amount of disk space as measured in gigabytes made available to the Client for use by the virtual machines or backup processes within its organizational environment.

Service Levels

Service Component	SLA
Enterprise Firewall	100% service availability
Basic Firewall	100% service availability
Enterprise Load Balancing	100% service availability
Network Availability	100% service availability; defined as the ability for data to be transmitted and received across the network by Company and Client. This definition excludes instances of Client's acts or omissions of its end users, a force majeure event as defined in the MSA, or Scheduled Downtime
Internet Bandwidth	100% service availability
Cross Connections	100% service availability
Site to Site VPN	100% service availability
Dedicated Blade - supporting infrastructure	100% service availability of supporting infrastructure
Dedicated Blade - hardware replacement	1 hour for standard blade configuration; 4 hours for non-standard
Hosted Private Cloud	100% service availability of supporting infrastructure; Considered not available if service fails to function properly as a result of hardware and hypervisor layer problems on the Host Server. "Host Server" means the hardware, computing and storage nodes, and software hypervisor of the physical server.
Software and Virus Protection	100% service availability; any system determined to be infected by a virus, where such virus matches antivirus signatures published by the leading antivirus software providers, the effected device shall be considered unavailable until such virus is removed.
Public Cloud	100% service availability of supporting infrastructure; Considered not available if service fails to function properly as a result of hardware and hypervisor layer problems on the Host Server. "Host Server" means the hardware, computing and storage nodes, and software hypervisor of the physical server.
CommVault File Agent Service	99.9% backup service availability; defined as the ability for data to be transmitted to and restored from the Company data centers and Company backup infrastructure. This definition excludes instances of Client's acts or omissions of its end users, a force majeure event as defined in the MSA, or Scheduled Downtime

Avamar Remote Backup Service	99.9% backup service availability; defined as the ability for data to be transmitted to and restored from the Company data centers and Company backup infrastructure. This definition excludes instances of Client's acts or omissions of its end users, a force majeure event as defined in the MSA, or Scheduled Downtime
------------------------------	---

Power Availability. Company will use commercially reasonable and good faith efforts to ensure that the entire quantity of Client's purchased electrical power will be delivered 100% of the time, except as part of mutually agreeable Scheduled Downtime. This service level metric requires that Client utilizes the 2N configuration (primary AND secondary outlets) offered by Company. For example if primary power is available and secondary power is not available, this is considered 100% available.

- a) Measurement – Power usage is measured by the cabinet, cage or room, depending on the services purchased by Client. It is measured at the Power Distribution Unit or Transformer. Power is delivered and measured in a primary/secondary configuration with a specified per circuit, per phase limit.
- b) Conditions – Client utilizing more than 40% of the amperage rating of either the A or B branch circuits supplying power to Client equipment waives its rights to both the Power Availability SLA and the Power Availability Service Credit. Client utilizing more the 80% of the amperage rating of any branch circuit waives its rights to both the Power Availability SLA and the Power Availability Service Credit, and will also be considered in violation of the National Electrical Code, allowing Company to take remedial action.
- c) Remedies – A power outage lasting fifteen (15) seconds or longer which results in the loss of both primary and secondary power to the same equipment makes Client eligible for a Service Credit. Power outages are deemed to have commenced upon the initial awareness (or automated recording) of an outage and ending when the electrical service has been restored.

HVAC/Environment. Company will use commercially reasonable and good faith efforts to ensure that data room 30 minute average temperature and relative humidity or dew point will remain within engineering thresholds applicable for each data center (see Table below). These service level metric commitments do not apply to local conditions within a particular Client cabinet, row, or other cage space.

- a) Measurement - Measurement of ambient temperature and humidity shall be taken at a distance of no lower than 5 feet above the floor level, along the center line of the active cold aisles, and averaged across the room.
- b) Conditions:
 - i. Company reserves the right to assist in and recommend the design of cabinet, cage or room layout, applying industry best practices as applicable. If Client's measured power density exceeds the facility rating as described above, spot cooling will be employed by Company at Client's expense. Spot cooling methods and equipment will be designed and installed by Company.
 - ii. As stated above, all the SLA's are conditioned upon Client's compliance with, among other terms, the Colocation Applicable Use Policy, which

includes, but is not limited to, the requirement that Client must use blanking panels and vent consistent with data center HVAC design. If Client fails to block the unabated direct flow, within its cabinet(s), of cooled supply air into the hot air return by neglecting to install blanking panels or the equivalent, blanking panels will be installed by Company at Client's expense and the HVAC/Environment obligations of Company and the SLAs applicable thereto shall be waived by Client.

- c) Remedies - If the temperature or humidity does not comply with these parameters, Client may be eligible for a Service Credit. Environment violations are deemed to have commenced upon the initial awareness (or automated recording) of a metric infraction and ending when the environment has been returned to normal operating ranges.

Data Center Facility Engineering Thresholds

<u>Data Center</u>	<u>Environmental - Ambient Temperature</u>	<u>Environmental - Relative Humidity</u>	<u>Dew Point</u>
BND	64.4°F (18°C) to 80.6°F (27°C)	20% and 80%	
CDF	average temperature will not exceed 77°F	40% and 55%	
DSM	average temperature will not exceed 80.6°F (27°C)	40% and 55% (data rooms 1 & 2)	40.9°F to 59.0°F (data rooms 3-6)
EDP	64.4°F (18°C) to 80.6°F (27°C)	20% and 60%	
MSN	average temperature will not exceed 80.6°F (27°C)	40% and 55% (data rooms 1 & 2)	40.9°F to 59.0°F (data rooms 3-6)
TDC	average temperature not to exceed 85.0°F	20% and 55%	

Internet Bandwidth Availability. Company will use commercially reasonable and good faith efforts to ensure that the entire quantity of Client's purchased Internet bandwidth will be available 100% of the time (except as part of Scheduled Downtime) on Client's access port (which is the port on the Company access router or switch within the Company facility upon which the Client's local circuit terminates), the Company designated routers, and the links between these routers.

- a) Measurement - Unavailability is deemed to have commenced upon initial report to Company by Client and an incident ticket is generated by Company and ending when availability has been restored.

MANAGED SERVICES WITHIN RELIACLOUD

Your applications, operating systems and network components within ReliaCloud that are managed by Company have an availability guarantee based on the technologies and architecture deployed in your specific infrastructure as well as the health of your systems.

Managed Service Audit and Remediation

For a Client's environment within ReliaCloud to qualify for an SLA, Company must perform an audit of the environment to ensure it is in compliance with manufacture and Company best practices. Company will test failover and redundancy scenarios, as well as documented best practices. Any items found to be outside of these best practices will be noted in a remediation report. Once all remediation items are resolved (billable under a separate project) the environment will qualify for the Company Managed Services SLA. **If Company performs the installation, this audit is waived.**

Managed Service Within ReliaCloud SLA

Type	Description	Availability Guarantee	Qualifier for Service Credit
Audited and Remediated Applications	Applications configured for application-level failover/ redundancy. SLA is defined as the availability of the application, not the individual components.	100%	Yes – for affected services
Audited and Remediated Operating System	Network and server operating systems. SLA is defined as the availability of the operating system, not the functionality of the individual services or processes.	100%	Yes – for affected services
Audited and Remediated Network Components	Network components configured for network-level failover/ redundancy. SLA is defined as the	100%	Yes – for affected services
	availability of the network, not the individual components.		
Audited and Remediated Network Components (without failover/ redundancy)	Network without network-level failover/ redundancy. SLA is defined as the availability of the network, not the individual components.	99.9%	Yes – for affected services
Non-audited systems, or systems with outstanding remediation tasks	Applications, operating systems and network components that have not been audited by Company or have outstanding remediation issues.	N/A	No

REMOTE MANAGED SERVICES

Your non-ReliaCloud environment(s) managed by Company have an availability guarantee based on the technologies and architecture deployed in your specific infrastructure as well as the health of your systems.

Remote Managed Service Audit and Remediation

For a Client's remote environment to qualify for an SLA, Company must perform an audit of the environment to ensure it is in compliance with manufacture and Company best practices. In most cases, Company will perform this audit onsite and will test fail over and redundancy scenarios, as well as documented best practices. Any items

found to be outside of these best practices will be noted in a remediation report. Once all remediation items are resolved (billable under a separate project) the environment will qualify for the Company Remote Managed Services SLA. **If Company performs the installation, this audit is waived.**

Remote Managed Service SLA

Type	Description	Availability Guarantee	Qualifier for Service Credit
Audited and Remediated Applications	Applications configured for application-level failover/redundancy. SLA is defined as the availability of the application, not the individual components.	99.9%	Yes – for affected services
Audited and Remediated Network and Server Operating System	Network and server operating systems. SLA is defined as the availability of the operating system, not the functionality of the individual services or processes.	99.9%	Yes – for affected services
Audited and Remediated Network Components	SLA is defined as the availability of the network, not the individual components.	99.9%	Yes – for affected services

Non-audited systems, or systems with outstanding remediation tasks	Applications, operating systems and network components that have not been audited by Company or have outstanding remediation issues.	N/A	No
--	--	-----	----

Service Credits

Failure to meet the above Service Levels, as measured by Company, during any one calendar month period, will result in a Service Credit in the amount of five percent (5%) of the Net Monthly Base Fees for the affected Services for every whole one (1) hour period of Service disruption. The total Service Credit due to Client for failure to meet the Service Levels in any calendar month shall not exceed the Net Monthly Base Fees for the affected Services for that calendar month.

SLA LIMITATIONS

1. Exclusions. Notwithstanding anything herein to the contrary, no otherwise applicable Service Level, including any remedies thereunder, shall apply with respect to any Excluded Event. "Excluded Event" means any event that adversely impacts the Service to the extent caused by: (a) the acts or omissions of Client, its employees, consultants, agents or subcontractors; (b) Scheduled Downtime, and testing for which Client has been provided notice; (c) the failure or malfunction of Client-provided equipment; or (d) an event beyond Company's reasonable control. SLA objectives and credits contained herein apply only to Company and Client; they do not apply to clients of Client.

2. Exclusive Remedy. **EXCEPT FOR THE TERMINATION PROVISION SET FORTH BELOW, THE SERVICE CREDITS SHALL BE CLIENT'S SOLE AND EXCLUSIVE REMEDY FOR ANY FAILURE OF THE SERVICES TO OPERATE IN ACCORDANCE WITH THE SLAS. ANY DISPUTES OR CLAIMS ARISING OUT OF OR RELATING TO THIS SERVICE LEVEL AGREEMENT MUST BE BROUGHT WITHIN SIX MONTHS OF THE OCCURRENCE OF ANY SUCH DISPUTE OR ACCRUAL OF ANY SUCH CLAIM.** No Services Credits shall be due if Client fails to notify Company in writing of a failure to meet the SLAs within ten (10) days of any such failure. Client's notice of a failure to meet the SLAs must contain the Client's invoice number as shown on its invoice, the dates and times of the unavailability of the Service, and such other Client identification reasonably requested by Company. Service Credits are determined and calculated on a per-occurrence basis, commencing upon the initial awareness (or automated recording) of an outage and ending when the Service has been restored. Under no circumstances will any tests performed by Client or any other party be recognized by Company as a valid metric for outage determination for the purposes of establishing a service credit herein. Service Credits shall be applied within sixty (60) days of the Client's request. In no event shall the Service Credit for any one calendar month exceed the Net Monthly Base Fees. Notwithstanding anything else herein, if Client is eligible for multiple measures of Service Credits during any calendar month, the total Service Credit issued to Client for that month shall be limited to the largest single Service Credit available.

3. Service Level Termination Event. Client has the right, but not the obligation, to terminate all or any portion of the applicable Statement of Work for cause upon written notice to Company and without further opportunity for cure if Company fails to meet the SLA obligations contained herein on more than three (3) unrelated occurrences (i.e., separated by time and not arising out of the same root cause) during any consecutive nine (9) month period, and which reasonably represents a material degradation in Services; any such right to terminate must be exercised within three (3) months or is deemed waived.

SERVICE DESCRIPTIONS

Upon execution of this Statement of Work ("SOW") by Milwaukee County ("Client") and OneNeck IT Solutions LLC ("Company") (the "Effective Date"), the Parties shall begin working together to complete the logistical prerequisites for the delivery and use of the Services purchased by Client.

BILLING EVENTS

Client billing events include but are not limited to a) initial creation and hand-off to Client of the committed pool of resources, b) static monthly billing for the committed pool of resources, c) bandwidth, data transport, or use of other metered offerings, d) use of billable software licenses, e) changes or modifications to the environment such as expansions of committed resources or configuration of network services, f) change management requests and professional services requests not covered by the Statement of Work, and/or g) sign-off of the Acceptance and Commencement Addendum.

TERM

The Term of this SOW shall commence on the Commencement Date and continue to be in effect for this SOW until the expiration or termination of this SOW according to its terms. Unless specifically stated otherwise, any related Executed Order stemming from the Services contained herein will be coterminous with this SOW and shall expire or terminate according to the terms of this SOW. Any applicable Executed Order will automatically renew for twelve (12) months unless either Party provides notice at least 90 days prior to the commencement of a renewal term.

By its signature below, Client certifies that it has read and agrees to the provisions set forth in this SOW and to the terms and conditions of the Master Services Agreement executed by Company and Client.

IN WITNESS WHEREOF, the parties hereto have executed this Statement of Work the day and year first written below.

OneNeck IT Solutions LLC

By: _____
Signature - Authorized Representative

Print Name

Title

Milwaukee County

By: _____
Signature - Authorized Representative

Print Name

Title