

Data Center Operations Professional Services Proposal for: Milwaukee County

Version: 1.0



Brian Osterhaus
District Sales Manager
1/8/2016

Table of Contents

EXECUTIVE SUMMARY3

SERVICE PROVIDER’S BACKGROUND INFORMATION5

DISCLOSURES, ACKNOWLEDGEMENTS, AND DECLARATIONS14

PROPOSED SOLUTION15

PROPOSED PROJECT HOURS27

TRANSITION AND TRANSFORMATION STRATEGY AND APPROACH.....28

REQUIREMENTS MATRIX48

EXPERIENCE MATRIX.....49

PROPOSED PRICING50

EXHIBIT 1 – INTENT TO RESPOND FORM51

EXHIBIT 2 – VENDOR INFORMATION52

EXHIBIT 3 – MILWAUKEE COUNTY’S MINIMUM WAGE PROVISION53

EXHIBIT 4 – INSURANCE AND INDEMNITY ACKNOWLEDGEMENT FORM54

EXHIBIT 5 – CONFLICT OF INTEREST STIPULATION57

EXHIBIT 6 – SWORN STATEMENT OF BIDDER.....58

EXHIBIT 7 – COVER SHEET FOR TECHNICAL PROPOSAL59

EXHIBIT 8 – COVER SHEET FOR PRICING PROPOSAL60

EXHIBIT 9 – EEOC COMPLIANCE61

EXHIBIT 10 – CERTIFICATION REGARDING DEBARMENT AND SUSPENSION63

EXHIBIT 11 – PROPRIETARY INFORMATION DISCLOSURE FORM64

ATTACHMENT 1 – ONENECK LEGAL EXCEPTIONS.....65

ATTACHMENT 2 – SAMPLE COLOCATION SLA AND AUP67

MILWAUKEE COUNTY ADDENDUM 3 – DISADVANTAGED BUSINESS ENTERPRISE UTILIZATION.....81

Executive Summary

Milwaukee County is the most populous county in Wisconsin with a population approaching one million residents. There are 33 departments that provide critical services ranging from Child Support, Court Services to Law Enforcement, just to name a few. The delivery of these services is essential for the success of Milwaukee County and its' residents. Information Technology is vital to support the applications that provide these functions. We recognize the role Excipio Consulting is providing to help with the strategic direction of Milwaukee County to become a more agile and flexible IT organization focused on the issues of its' constituents.

OneNeck IT Solutions understands that many organizations have changed the way they are approaching IT and in particular, the data center and its ongoing management. As significant changes in technology, and our industry as a whole have taken place over the past several years this has created a higher demand and visibility for greater operational efficiencies, a desire to redirect the focus of in-house IT staff to more strategic initiatives of the county and an overall holistic look at what tasks and responsibilities make sense to manage internally and which ones do not.

OneNeck IT Solutions is proud to respond with a hosted, managed services solution located in our state of the art Tier III data center facility in Fitchburg, WI. We will provide disaster recovery services connected to our Eden Prairie, MN location. The solutions provided will enable the County to be more efficient with utilization of storage and compute resources and to deliver IT services at a lower cost.

OneNeck IT Solutions is part of TDS Telecommunications Corp. which is headquartered in Madison, WI. As a leading provider of next-generation, production-grade data center solutions with seven (7) data center facilities throughout the upper Midwest and Arizona (as well as, a new Tier III data center coming in Colorado in 2014) and an organization that is today, 650 people strong, our core capabilities include Data Center Colocation, Managed Services, IaaS Cloud Solutions consisting of multiple, regionally-based environments, ERP Application Management, Disaster Recovery, Professional Services Consulting, and Network and Systems procurement and solutions.

OneNeck IT Solutions is partnered with Solutionary to provide expert security services for our proposal. Solutionary, an NTT Group security company, is the next generation managed security services provider (MSSP) that delivers Managed Security Services (MSS), Global Threat Intelligence and Professional Security Services. Comprehensive Solutionary security monitoring and security device management services protect traditional and virtual IT infrastructures, cloud environments and mobile data. Solutionary clients are able to optimize current security programs, make informed security decisions, achieve regulatory compliance and reduce costs.

Founded in 2000, the company's services are based on next generation security intelligence, proven processes and proprietary, patented technology. Solutionary provides clients with advanced service delivery, thought leadership, years of innovative groundwork and proprietary certifications that exceed industry standards, enabling the company to have one of the highest client retention rates in the industry.

Solutionary has been acknowledged as a leader by industry experts and analysts. Services are delivered 24/7 to clients globally through multiple state-of-the-art security operations centers (SOCs). Solutionary provides superior security processes and technology, delivering managed and monitored services 24/7. OneNeck IT Solutions is currently working with Solutionary with another public sector entity.

OneNeck IT Solutions takes great pride in our customer partnerships and their business with the objective of being a true extension of their organization that you can rely on. We also pride ourselves on service and accountability, which is a key element in being a successful managed services and data center solutions provider.

We hold the highest level of sales and delivery certifications with our strategic partners, Cisco, EMC, VMware, Microsoft, Citrix, HP, NetApp, and F5, as well as many others. As a top level partner with the leading manufacturers, we not only buy at the highest levels of volume discount available but are also briefed on strategic direction and updates.

OneNeck is the strategic data center partner for many organizations within multiple vertical industries from healthcare, financial, retail, services, manufacturing and more. We will work to earn your trust to become your strategic partner.

Sincerely,



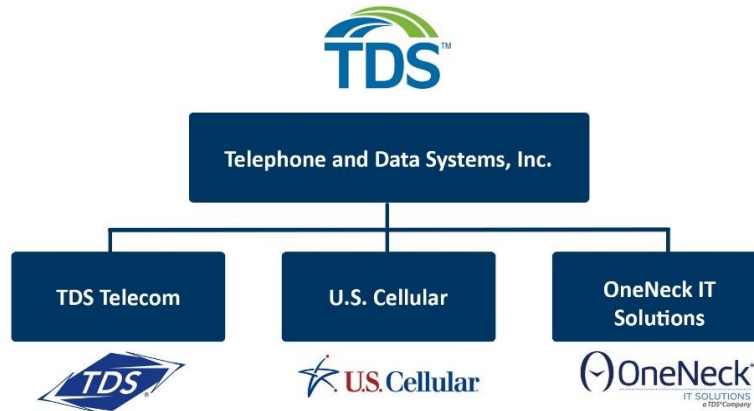
Brian Osterhaus
District Sales Manager
OneNeck IT Solutions

Service Provider’s Background Information

Provide background on the service provider’s business and operations including:

- Size and scope of service provider’s business

OneNeck IT Solutions, a TDS® company (OneNeck) was purposefully built over the past several years through the acquisitions of leading IT solutions providers, along with the organic growth of key engineering resources and executive management. It combines the managed services capabilities of OneNeck IT Services with the tremendous resources, data center facilities and capabilities of VISI, TEAM, Vital Support Systems and MSN Communications to create one of the most comprehensive providers of end-to-end, enterprise-class IT solutions. Backed by the Fortune 1000® strength of Telephone and Data Systems, OneNeck IT Solutions is owned by TDS Telecommunications Corp. which is headquartered in Madison, WI.



OneNeck IT Solutions has a combined 30 + years of experience in the data center solutions and managed services industry. The success of our company is based upon core values of Midwestern integrity, long-term relationships with our customers, and a commitment to customer service and results.

Over the past several years, we have methodically combined the people, operations, data center facilities, expertise and capabilities of our five specialized organizations into a single company, OneNeck IT Solutions. Our data centers are the key component to what differentiates us from our competition, providing a strategic foundation for our service capabilities.






ONENECK IT SOLUTIONS KEY STATISTICS:

Topic	Count
Total Employees	646
Engineers and Support Personnel	450
Colocation Customers	250
Cloud and Hosted ERP Customers	375

End Users Supported	20,000
Hardware and Professional Services	750
US Based Data Centers	8
US Based Cloud Pods	4

OneNeck Capabilities Overview

From a capabilities, solutions and services standpoint, our service offerings are organized into five main categories:

Cloud & Hosting Solutions	Managed Services	Application Management	IT Hardware Resale	Professional Services
<ul style="list-style-type: none"> • Cloud Servers • Private Clouds • Hybrid Clouds • Cloud Storage • Desktops in the Cloud (DaaS) • Colocation 	<ul style="list-style-type: none"> • Managed Applications • Managed Databases • Managed Networks • Managed Servers • End User Support • Disaster Recovery as a Service (DRaaS) • Security & Compliance • Communication & Collaboration 	<ul style="list-style-type: none"> • E-Business Suite • JD Edwards • Hyperion • Demantra • Agile • OBIEE • Informatica • Microsoft Dynamics AX • Infor LN 	<ul style="list-style-type: none"> • Cisco® • EMC® • HP® • VMware® • Citrix® • FS® • NetApp 	<ul style="list-style-type: none"> • IT Assessments • Design • Migration & Implementations • IT Roadmaps & Planning • Technology Consulting • Contact Center Consulting 

Data Center Colocation

The changes within the IT industry and in the Data Center in particular has organizations, both large and small, evaluating their current and future Data Center requirements. Companies of all sizes are considering options and alternatives to meet the demands and changes within their business, such as, growth, compliance and regulatory demands, security, greater operational and cost efficiencies. Not to mention, a reduced and/or significantly taxed IT staff, greater focus on the core business vs. “being in the data center business,” and an overall greater focus on IT budgets.

Data Center colocation is a core capability of OneNeck IT Solutions where we not only have world-class facilities and operations, but also work closely with our customers on developing a strategy and roadmap on what makes sense for your business and data center needs.

Managed Services Solutions

OneNeck’s Managed Services give you a wide range of benefits designed to free you from the necessary but time consuming chores of monitoring and managing your IT infrastructure. OneNeck’s Managed Services Solutions maintains highly skilled and experienced in-house staff for all support and network operations. Our systems management service provides you with advanced monitoring, reporting, and patching for your mission critical servers and databases. The OneNeck platform allows monitoring and/or management of any part of your IT infrastructure. You can have us monitor/patch/fully manage as much, or as little of your infrastructure as you like.

Our Managed Services offerings provide continuous support and monitoring with our 24x7x365 network operations centers (NOC). Moving away from the complexity of using multiple tools to monitor your infrastructure and network will reduce operational costs and maximize your IT performance while minimizing downtime. OneNeck's flexible solutions let you select the level of service and support that best matches your unique business needs, whether you call on us to manage some, most, or all of your data center and infrastructure needs. OneNeck can manage your IT infrastructure wherever it is located. Whether it is your headquarters, a branch office, a server in a third party data center, or a OneNeck data center, as long as there is Internet connectivity available, we can monitor and manage that location and environment.

OneNeck's 24x7x365 staffing and centralized NOC gives you increased levels of support and reliability. OneNeck takes on the day-to-day tasks of monitoring and maintenance, allowing you and your team to focus on more critical projects and your business' strategic needs while having the flexibility to adjust your service levels easily. Services can be quickly applied or cut back throughout any part of your network and systems as your business needs change.

ReliaCloud™ – Local, Enterprise-Class Infrastructure as a Service (IaaS)

OneNeck also offers Cloud Services where we have made significant investments in building Enterprise-Class, Infrastructure as a Service (IaaS) environments within four (4) of our geographically-disperse tier 3 data centers. The concept of Cloud Computing has several important concepts including on-demand availability, pay only for what you use, and rapidly scalable resources just to name a few.

ReliaCloud™ is enterprise class IT infrastructure designed for resource intensive applications and databases that require a secure and compliant operational framework. Built with enterprise-grade products and capabilities from Cisco, EMC and VMWare, ReliaCloud is specifically designed to run traditional business applications – the type of applications which require reliable and scalable computing infrastructure. Delivered in dedicated and shared resource pools from multiple Tier III data centers, ReliaCloud is designed for maximum flexibility and utilization of current IT investments. With colocation options and optimized metropolitan network connectivity, ReliaCloud is suitable for hybrid and disaster recovery solutions in addition to its focus on production computing applications.

The OneNeck ReliaCloud Infrastructure-as-a-Service leverages industry-leading solutions of VMware vSphere™ and vCenter™ Server, Cisco's state-of-the-art Nexus core switching and Unified Computing System (UCS) for compute and EMC's enterprise-class Symmetrix VMAX and VNX storage technologies; along with EMC Avamar and Data Domain for data backup options and Isilon for additional file-based NAS storage. ReliaCloud is operated out of our Tier III, highly secure and highly redundant data center facilities located in Wisconsin, Minnesota, Iowa and Arizona. We will have a fifth environment in our new Tier III facility in late 2014.

Professional Services

As mentioned earlier, OneNeck is a Data Center and IT solutions company providing network and systems solutions, cloud infrastructure, colocation and Managed Services. However, one of the key differentiators is our unique ability to offer our customers options. Options that our customers want to evaluate and need to understand in order to build out their strategies. At OneNeck, we can approach our customers with a true consultative approach and provide solutions that include a

customer on premise design, a colocation design in one of our data centers, a Cloud design using our ReliaCloud™ Infrastructure-as-a-Service (IaaS) or a combination of all of the above.

From a professional services standpoint, OneNeck provides technology solutions to businesses. Essentially, we offer a suite of consulting services and expertise which includes the pre-sales, technical engineering, planning, design, procurement, installation and management of business-critical infrastructure, systems and communication components (servers, security, local and wide area networks, wireless, storage, voice, video & IP telephony). By being highly certified in and key partners to global leaders such as Cisco, EMC, Citrix, VMware, HP, Microsoft and others, we are able to provide our customers with the best pricing available supported by top level engineering resources.

The breadth and depth of technical certifications held by our team members have allowed OneNeck to achieve the highest levels of partner status with Cisco (See below), EMC (Velocity Premier), VMware (Premier) HP (Elite), Citrix (Gold) and Microsoft (Gold).

ERP Managed Hosting

OneNeck® IT Solutions is the leading ERP managed hosting provider to mid-market companies. We support most major ERP applications including Oracle E-Business Suite, JD Edwards, Microsoft Dynamics AX, and Infor's Baan to name a few.

Our promise is to provide a single point of accountability for your ERP infrastructure. For many of our customers, we are the sole organization responsible for managing their entire Enterprise Application Environment.

As the leading independent provider of ERP solutions, OneNeck offers:

- **A Broad Scope of Services** - OneNeck offers application, database and network management, data center management, 24/7 customer support, disaster recovery and desktop support, all under one roof. You have access to all our skill, experience and expertise at a predictable monthly cost.
- **Tailored Solutions** - OneNeck takes a "one-to-one" approach. With this configurable methodology, we provide the right solution for each customer. As a result, we achieve greater visibility and control over our customers' IT environments and have an extensive list of long-tenured, highly satisfied clients.
- **Flexibility and Scalability** - There's one constant in business and that's change. Our staff is always on call and can scale your operations as needed as your business grows. With OneNeck, you'll always have immediate access to highly skilled IT professionals who already know your environment.
- **An Easy-to-Engage Relationship** - We're all about accountability, and that means we're at your service 24 hours a day, 7 days a week. We create specific points of contact for every customer and even offer self-service portals for those things you'd rather do yourself. With a proven methodology and track record, we resolve all issues quickly and make it easy to add new services as needed.

Industry Security Standards

OneNeck prides ourselves on our ability to achieve and maintain security standards. Below are our current standards and roadmap for 2014.

- ISO 27001:2013 certification
 - PCI DSS v3 certification
 - HIPAA/HITECH examination
 - SSAE 16 Type 2 SOC 1 examination
 - EDP Data center is Uptime Institute Tier 3 certified
 - OneNeck is US/EU and US/Swiss Safe Harbor compliant
- At least three customers where service provider provides services similar in nature and scope to those outlined in this request.
- City of Minneapolis
 - Otto Doll
 - Otto.doll@ci.minneapolis.mn.us
 - 612-673-3633
 - Louisville Metro
 - Sharon Meador
 - Sharon.Meador@louisvilleky.gov
 - 502 574 6499
 - Loudon County
 - Jakub Jedrzejczak
 - Jakub.Jedrzejczak@loudoun.gov
 - 703.737.8587
- Outline of key partnerships that will contribute to the performance of the services

Solutionary Overview

Solutionary, an NTT Group Security Company, is a next generation Managed Security Services Provider (MSSP) solely focused on delivering relevant, efficient and cost-effective managed security services and consulting services. Since inception in 2000, Solutionary has grown to be a global trusted advisor and has one of the highest client retention rates in the industry.

In 2011 and 2012, Solutionary was ranked by Gartner as a “Leader” in the MSSP Magic Quadrant, North America. Gartner ranked NTT as a Challenger in the first-ever Gartner Magic Quadrant for Global MSSPs in 2014.

Solutionary delivers services 24/7 through multiple state-of-the-art Security Operations Centers (SOCs), serving medium-to-enterprise businesses in a broad range of industries with a wide array of security needs. The primary purpose of Solutionary services is to keep client’s information technology (IT) secure and compliant. Solutionary assesses, manages, monitors and correlates data, turning it into relevant, decision-making information to enable the execution of intelligent IT

security actions. Solutionary provides clients with advanced service delivery, thought leadership, years of innovative groundwork and proprietary certifications that exceed industry standards.

Solutionary remains committed to improving our people, process and technology. We make sure our clients achieve greater information security at a lower cost than they would themselves.

Managed security services will continue to be the primary focus of the overall business strategy and is a key differentiator. Solutionary will also continue to grow and develop our Security Engineering Research Team (SERT) program to extend intelligence and predictive analysis services for clients. Our goal is not to be the biggest MSS provider but to be the best.

On August 7, 2013, Solutionary was acquired as a wholly-owned subsidiary by Nippon Telegraph and Telephone Corporation (NTT). NTT provides clients with solutions spanning a variety of cloud service and delivery models through group companies Dimension Data, NTT Communications, NTT DATA and Solutionary. NTT continues to aggressively expand its security capabilities to become one of the world's largest security integrators. NTT is currently providing services to over 50 countries through its cutting-edge R&D, world-class communications carrier Computer Security Incident Response Team (CSIRT). The NTT Group has a \$3.5 billion annual R&D budget* much of it focused on cybersecurity.

This acquisition has benefited existing and new Solutionary clients by enhancing worldwide security intelligence capabilities, expanding the R&D budget and supporting global growth goals. With the entirety of the Solutionary leadership team intact, Solutionary continues to operate with a customer-focused culture dedicated to providing clients with award-winning service and attention.

Our blend of expertise in managed security and log monitoring services allows Solutionary to provide a uniquely integrated service offering to help you accomplish the goals of the County's security program. Our years of experience have demonstrated that information security and compliance with various industry requirements are inextricably woven together, and that organizations holding leadership positions in these disciplines effectively manage these critical practices. We deploy our patented technology to help our clients manage complexity, solve problems and deliver results – in a secure manner. We believe that effective, efficient and proactive management of information security and compliance requirements is at the core of Relevant, Intelligent Security.

- Service provider's qualifications and differentiators

One Call. One source. One point of accountability for all your IT needs. We can provide Milwaukee County with a partnership for IT strategy and solutions from the traditional to the latest in IT services. OneNeck has been providing colocation services from our Madison facility since it was commissioned into operation in 2008.

OneNeck offers an alternative to investing in your own data center and operations facilities. Instead of building and staffing a data center or making significant investments to update your current environment, you can leverage OneNeck's mission critical facilities to lower your operating expenses, reduce capital expenditures and shorten the time it takes to accomplish your IT goals. You

can apply your limited and valued IT resources in a way that most positively impacts your business while maintaining the flexibility to scale your data center requirements as needed.

Our data center solutions span a wide spectrum, including:

- Colocation Services
- Disaster Recovery Services
- Cloud Infrastructure Services
- Fully Managed & Hosted IT Environments
- Internet Connectivity
- Transport Capabilities
- Remote Hands

Organizations including Healthcare, Finance and Insurance, Bio and Life Sciences and Government agencies select OneNeck as their data center partner to support their stringent audit and compliance requirements. OneNeck has a growing customer base of more than 250 colocation customers and more than 350 Cloud customers. On June 24, 2015, OneNeck announced the opening of our eighth wholly owned and managed data center in Denver, Colorado. Additionally, based on growth in our Madison Data center, OneNeck is constructing our fifth data center room with expected completion in late Q4 of 2015. Examples of the profile of customers we host in our Madison data center is provided in the Executive Summary section.

OneNeck's primary strengths and key differentiators are summarized below and further discussed in the Executive Summary and Solutions Overview sections of this RFP response.

- **Local Proximity:** OneNeck has the largest wholly owned and managed commercially available data center in the state of Wisconsin, located in Fitchburg, approximately 86 miles from the Milwaukee County Courthouse.
- **Focus on Security and Compliance:** As a Tier 3 Compliant (Tier 4 for Power) SSAE 16 Type II SOC1 Audited Data Center facility, OneNeck plays a key role in supporting the audit and compliance requirements of our customers.
- **Proven Success Supporting Similar Organizations with High Compliance Requirements:** Organizations including Healthcare, Finance and Insurance, Bio and Life Sciences and Government agencies select OneNeck as their data center partner to support their stringent audit and compliance requirements. Based on customer growth in our Madison Data center, OneNeck is constructing our fifth data center room with expected completion in late Q1 of 2016.
- **Portfolio of Data Center Services:** Complimentary data center services that include colocation, cloud services, application hosting, managed services and related professional services and technology.
- **Core Competency:** Managing a network of eight data centers, data centers and related offerings are our core competency. We successfully serve a growing base of high profile customers across the central, southwest and western U.S.

- Description of service provider's technical and service capabilities

To support the evolving requirement of our customers, OneNeck provides a comprehensive suite of complementary data center services:

- **Colocation** – highly available, secure and compliant, carrier neutral data center facilities
- **Data Center Optimization and Migration Services**
 - Assessment and Planning Services
 - Physical Relocation/Move Services
 - Project Management Services
- **Disaster Recovery and Back-up Services** - to support the disaster recovery and back-up requirements of our customers, OneNeck provides a network of eight data centers connected with high capacity fiber:
 - Madison, WI
 - Minneapolis, MN
 - Des Moines, IA
 - Cedar Falls, IA
 - Phoenix, AZ
 - Gilbert, AZ
 - Denver, CO (opened June 24, 2015)
 - Bend, OR
- **Managed IT Services** – providing monitoring, patching services and SLA management
- **Cloud Services (ReliaCloud)** – enterprise-class, high availability Infrastructure as a Service capabilities
- **Application/Database Hosting and Management** – mission critical Enterprise Resource Planning (ERP) and related application hosting and management for Oracle, SAP, and Microsoft
- **Professional Services and Tier 1 Technology** product and software solutions

- List of all quality certifications

As a Tier 3 Compliant (Tier 4 for Power) SSAE 16 (SOC 1) Type II audited data center facility, OneNeck plays a key role in supporting the audit and compliance requirements of our customers. Additional standards adherence include the following:

- ISO 27001 Certified
- PCI DSS Compliant
- HIPAA Audited Facilities (Execute BAAs as needed)
- FDA Audited
- ITIL Certified data center staff
- All Employees required to pass annual training and exam on HIPAA, PCI and Safe Harbor

- Must be willing to provide a copy of latest SSAE 16 Type II (or equivalent) audit upon request

Upon execution of our standard NDA between Milwaukee County and OneNeck, an electronic copy of our most current SSAE 16 Audit will be emailed to the designated Milwaukee County contact in a separate secure file.

- Must be able to produce the last three years of financial statements including income Statement and Balance Sheet upon request.

OneNeck IT Solutions is a wholly owned subsidiary of Telephone and Data Systems. As part of a publicly traded company, our financials are open to view at any time at the TDS corporate website: <http://investors.teldta.com/investor-relations/investor-relations-home>

Disclosures, Acknowledgements, and Declarations

Provide disclosures and declarations related to the following areas:

- All exhibits and attachments require acknowledgments and compliance.
OneNeck IT Solutions acknowledges and complies with all exhibits and attachments of this RFP. Please see Attachment 1 of this response for OneNeck's legal exceptions.
- Identify the sections in which service provider has elected not to respond and the reason for not responding.
OneNeck IT Solutions is not responding to the mainframe portion of this RFP. The partner we had elected to use decided to bid on this RFP and declined to partner with us for the mainframe portion of our response.
- Disclose the name, nature of the relationship, and the scope of the activities for any third party that the service provider is dependent on to provide services defined herein. Exclude normal purchasing relationships with vendors providing hardware and software or typical products and services (i.e. maintenance contracts).
We are partnered with Solutionary to provide the security functionality required in this RFP. We will use Coakley Brothers for the physical moving of equipment for this RFP. All other functions will be provided by OneNeck employees.
- Provide a list of all entities with which service provider has relationships that create, or appear to create, a conflict of interest with the work that is contemplated in this request. The list should indicate the name of the entity, the relationship, and a description of the conflict.
We are not aware of any such relationships with any entities.

Proposed Solution

Provide an overview and detailed information to describe the service provider's solution. At a minimum, the solution description should include a description of the service provider's strategy and approach, including any key assumptions regarding the following:

- Data center capabilities, features, location of major data center(s), etc.
- Service management framework
- Account and customer engagement process
- Innovation and service improvement strategies, capabilities, processes, etc.
- Service Level Management – establishing and managing service levels
- IT security (at a minimum, provide an outline that demonstrates the existence and depth of the organization's security practices)

Milwaukee County - ReliaCloud Data Center Design Notes

Recommendation

Milwaukee County Department of Administrative Services has asked for help in revitalizing their critical Information Manage Services Division. This strategic initiative would improve capabilities in people, process and technology to support the County's mission critical applications and support operations.

Overall – we recommend Milwaukee County utilize two OneNeck data centers and our ReliaCloud private cloud infrastructure to leap ahead to modernize their infrastructure and process. We recommend putting the Test/Dev environment at the DR data center – this would enable Milwaukee County to have an environment pre-setup that can be used for test and development and be available for running recovered workloads in the event of a disaster. OneNeck will leverage our existing partner relationship with Managed Security Services Provider (MSSP) Solutionary for the management of the security services requested.

OneNeck has a proven track record of managing critical applications and IT operations for clients for over 18 years. Over that time, we have continued to refine our capability to provide IT operations that achieve results for our clients:

- **Milwaukee County Desired Outcome - High quality and responsive support services**
 - OneNeck IT Solutions uses a shared services support model to provide exceptional customer service to our enterprise clients. We operate two 24/7 Network Operations Centers in Madison, WI and Minneapolis, MN. These centers are staffed with technical engineers and customer support personnel with varied expertise across our data center, ReliaCloud and Applications Infrastructure services. OneNeck provides local remote hands in the Madison and Minneapolis data center on a 24/7/365 basis for emergency services as well. Transform the organization to an agile and flexible IT organization focused on the real issue of our constituents
- **Milwaukee County Desired Outcome - Hybrid infrastructure across on premise, private cloud, and public cloud.**
 - OneNeck proposes a ReliaCloud Hosted Private Cloud service that delivers a private cloud solution leveraging our enterprise compute, network and storage

resources will provide a flexible IT environment for County mission critical applications. The County can selectively leverage management services for infrastructure and applications that fall outside of their target core competencies.

- **Milwaukee County Desired Outcome - Transform IT capabilities to provide more robust and mature IT processes and capabilities in line with the size and nature of Milwaukee County's constituent services**
 - At OneNeck® IT Solutions, our commitment is to be an expert provider of hybrid IT solutions tailored for mid-market and enterprise companies and to provide high-touch customer service. Through a single point of accountability, OneNeck offers end-to-end enterprise-class IT solutions including cloud and hosting solutions, managed services, ERP application management, professional services, IT hardware and top tier data centers.
 - Our thought leadership, innovative engineering and hybrid, custom-designed solutions help customers reduce costs, improve service levels, increase revenues and gain local-to-global competitive advantage. Our customers span a broad spectrum of industries including healthcare, manufacturing, financial services, retail, education and government. Customers choose us because our experienced team leverages ITIL based practices to manage mission-critical data centers, cloud, and customer infrastructure 24/7/365. Our facilities meet the highest industry standards, having successfully completed the Type 2 SSAE 16 (SOC1) examination, ISO/IEC 27001:2013 certification, HIPAA and HITECH examination, and PCI Data Security Standard validation. The bottom line, it ensures our customers that their data is secure, available and contributes to their compliance framework.

- **Milwaukee County Desired Outcome - Reduce risks inherent in Milwaukee County's current data centers and technology landscape**
 - OneNeck IT Solutions can also deliver world-class facilities, system availability, monitoring tools, and 24/7 customer support. Outsourcing today has evolved from a purely cost-based decision to one that improves a company's processes and systems, protects their reputation and assets and helps them achieve their goals.

- **Milwaukee County Desired Outcome - Provide cost effective IT capabilities**
 - Whether it's their payroll, legal services, application hosting, marketing or something as routine as printing business cards, no organization does everything in-house. Leading organizations focus on what they do best – their specialty. They exploit efficiencies to increase results on their core operational activities and in most cases, look to other organizations to complete tasks which are not within their core competencies. In this sense, outsourcing is really finding best-in-class partners who can provide exceptional knowledge and service in a specific area of need. This is a strategy to integrate more expertise into the organization, thus increasing efficiency and competitiveness. Information Technology is an excellent example of this. When done right, an IT partner like OneNeck IT Solutions, can give an organization economies of skill and scale by aggregating demand across our multiple clients. We can encourage and speed the adoption of proven

methodologies, best practices and procedures that create not only a more effective IT function, but a smoother running organization as well.

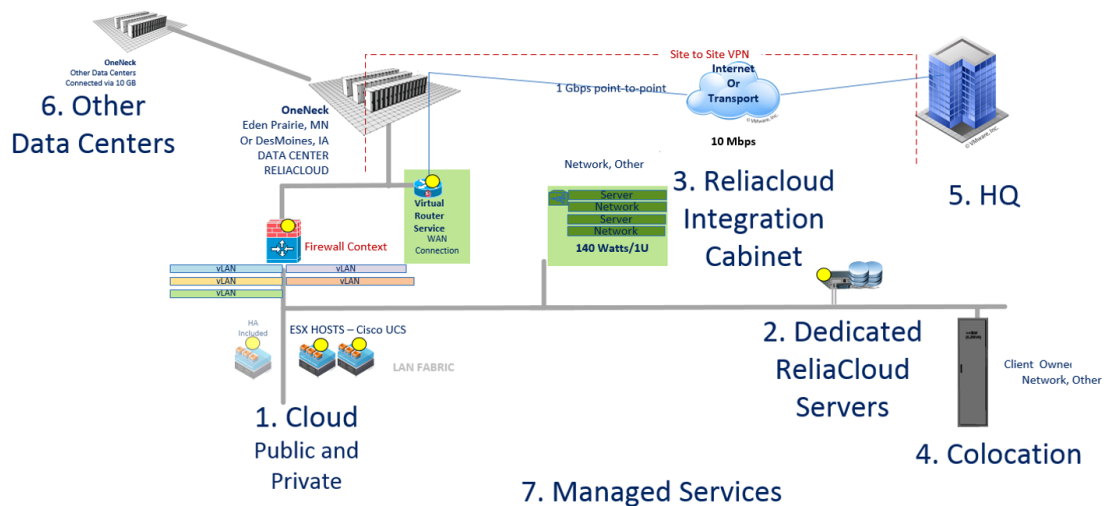
OneNeck Approach

OneNeck offers our customers a full hybrid IT model of service offerings from colocations services, cloud services, managed services, ERP hosted applications, and IT Hardware resale and professional services. This approach to the market place allows OneNeck to be nimble enough for customers as their IT needs and requirements evolve over time. This allows OneNeck customers to get their applications and data in the right place, on the right platform, at the right time.

Seamlessly Connected Environment

Flexible Options Under One Contract

Hybrid IT



1. ReliaCloud is specifically designed with flexibility to transition completely to a private cloud environment or offer access to resources as desired including – computing capacity, storage, security, routing, switching, and other components.
2. Dedicated ReliaCloud Servers – designed to provide compute resources for non-hypervisor based workloads that require dedicated hardware.
3. ReliaCloud Integration Cabinet – space for customer owned devices directly next to ReliaCloud enabling clients to leverage existing investments and specialty hardware integrated with their cloud environment.
4. Colocation - Just a cross connect away from the cloud, colocation enables a client to have a substantial presence in our Tier 3 data centers to support their mission critical applications.
5. HQ – client on-premise solutions can be seamlessly connected into OneNeck ReliaCloud and colocation resources.
6. Other Data Centers – OneNeck has 8 data centers, with cloud pods in 5 of them. Our data centers are all connected with the 5 cloud pods being connected via a sharable 10GB link.
7. Managed Services – We provide 24X7, ITIL based managed services of all of our facilities, infrastructure and customer owned infrastructure.

Milwaukee County desires to achieve the following capabilities in a new IT environment:

Given

Virtual Server Guests – 290 - 221 production, 69 pre-production
Total Storage Identified (74 TB)
Approximately 1800 GB of Memory in use
Production and Test/Dev Resource Environments
Security Requirements
Total Users – ~4,000
Required 2 Data Center Model with Remote Locations attached

Future State - ReliaCloud Private Data Center at a Primary and Disaster Recovery Sites (2 Sites)

OneNeck proposes a ReliaCloud Hosted Private Cloud service that delivers a private cloud solution leveraging enterprise compute, network and storage resources and will provide a flexible IT environment for County mission critical applications. The County can selectively leverage management services for infrastructure and applications that fall outside of their target core competencies.

OneNeck IT Solutions will design, architect and deliver a hosted private cloud. Private Cloud is defined as dedicated host machines (physical hardware) and associated hypervisor software (VMware ESX). Storage services (LUNs) are also directly mapped via 8GBPs fiber channel to the storage array. LUNs are not shared or accessible by other clients.

Built to

- Host production class / mission critical workloads
- Provide robust security controls
- Provide nearly all core infrastructure as a Service
- Integrate with colocation
- Interoperate with our Customers' existing infrastructure
- Support direct high-speed connectivity
- No longer just SSL/HTTPS
- Campus style extension design

Designed to

- Shorten the service adoption gap by using common components
- Backed by a 100% Service Level Agreement
- Provide the midmarket customer base with IT resources that are typically exclusive to the enterprise market.
- Provide a comprehensive technology stack which also allows for non-Cloud product integration points.

- Provide elastic resources which can be customer provisioned and manipulated.

This solution would leverage OneNeck's infrastructure in a dedicated compute/shared network environment at two data centers. OneNeck would provide a private cloud environment sized appropriately in Madison, WI (MSN) as a Primary data center with connectivity to Milwaukee County. OneNeck would have another private cloud environment sized appropriately in Eden Prairie, MN (EDP) as a Test/Dev and Disaster Recovery data center with connectivity to Milwaukee County. Both OneNeck data centers would be connected with an appropriately sized link for data and backup replication. The following capabilities are provided with this solution:

1. Private Cloud environment at each site
2. Enterprise Firewall Context at each site (10 vLANs)
3. Storage replication to alternate site for VMs and required for recovery
4. Centralized, managed backup of all data center resources
5. Replicated backup data to alternate site (Electronic Vaulting)
6. Network connectivity between data centers (provided by OneNeck) (sizing estimated at 1 Gbps for planning purposes)
7. Connectivity at each site to Milwaukee County (949 North 9th Street for planning purposes)
8. OneNeck provides VMware licensing and Infrastructure as a Service (IaaS)
9. OneNeck provides Windows Operating System licensing
10. 24X7 management of IaaS infrastructure – Compute, Storage, Network, Backup
11. 24X7 management of supported Windows and Linux Virtual Servers (Microsoft Supported Server OS, RedHat, Suse, and CentOS)
12. 24X7 management of Active Directory (two domains)
13. Milwaukee County provides all application licensing

OneNeck will provision the infrastructure and OneNeck will migrate or rebuild the existing resources into the new environment and migrate the data. **We do not recommend moving the existing infrastructure.**

Approach

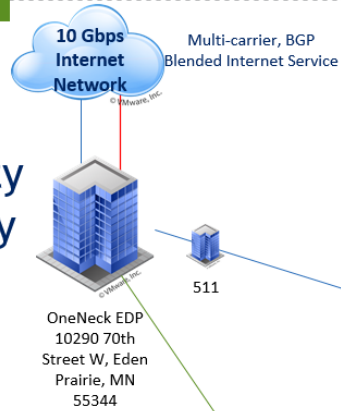
1. Perform assessment to finalize migration costs
2. Establish project team
3. Validate design, plan build and plan migration
4. Build private cloud at each location
5. Establish a connection from our data center to 9th Street
6. Build network between sites
7. Determine Replacement/Elimination, Migration or rebuild of data center resources depending on what is needed for each VM
8. Implement OneNeck management tool set
9. Install backup agents and configure backups
10. Establish second site for replication of backups
11. Develop a "run book" for operations

Proposed Network/Site Topology:



Milwaukee County Data Center Network

Milwaukee County
Disaster Recovery

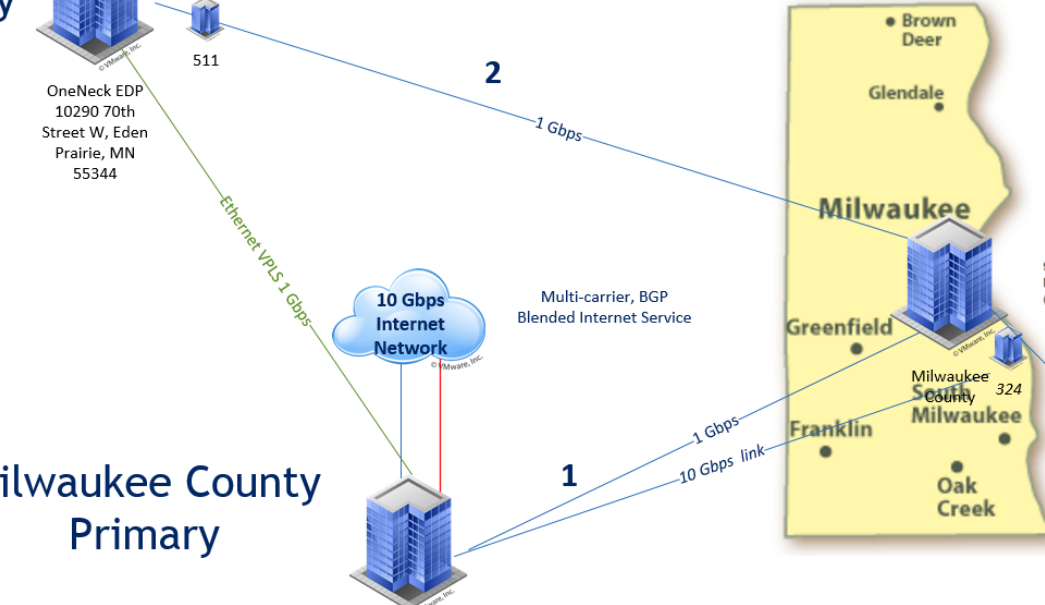
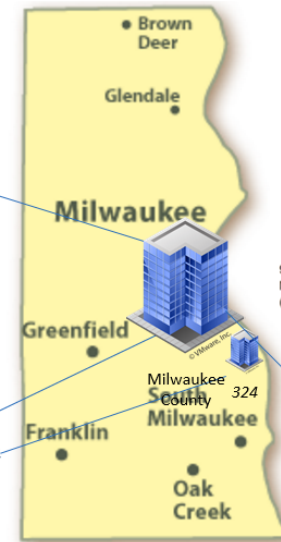
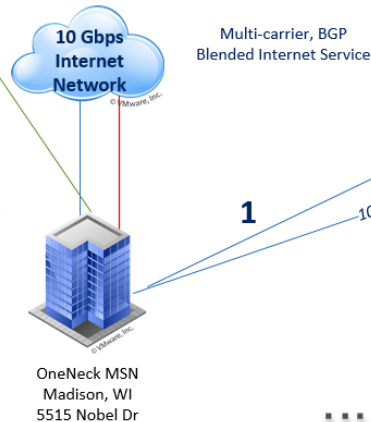


Solution Notes

1. Provide diverse telecommunications carrier infrastructure (multiple physical points of entry) of at least two carriers
2. Provide diverse local exchange carrier access of at least two carriers
3. Provide internet bandwidth of 10 Mbps
4. Provide flexibility to burst Internet bandwidth for short periods (i.e. hours) up to 100 Mbps
5. Milwaukee County may choose to connect their sites directly to the data centers using Time Warner or a Time Warner partner,

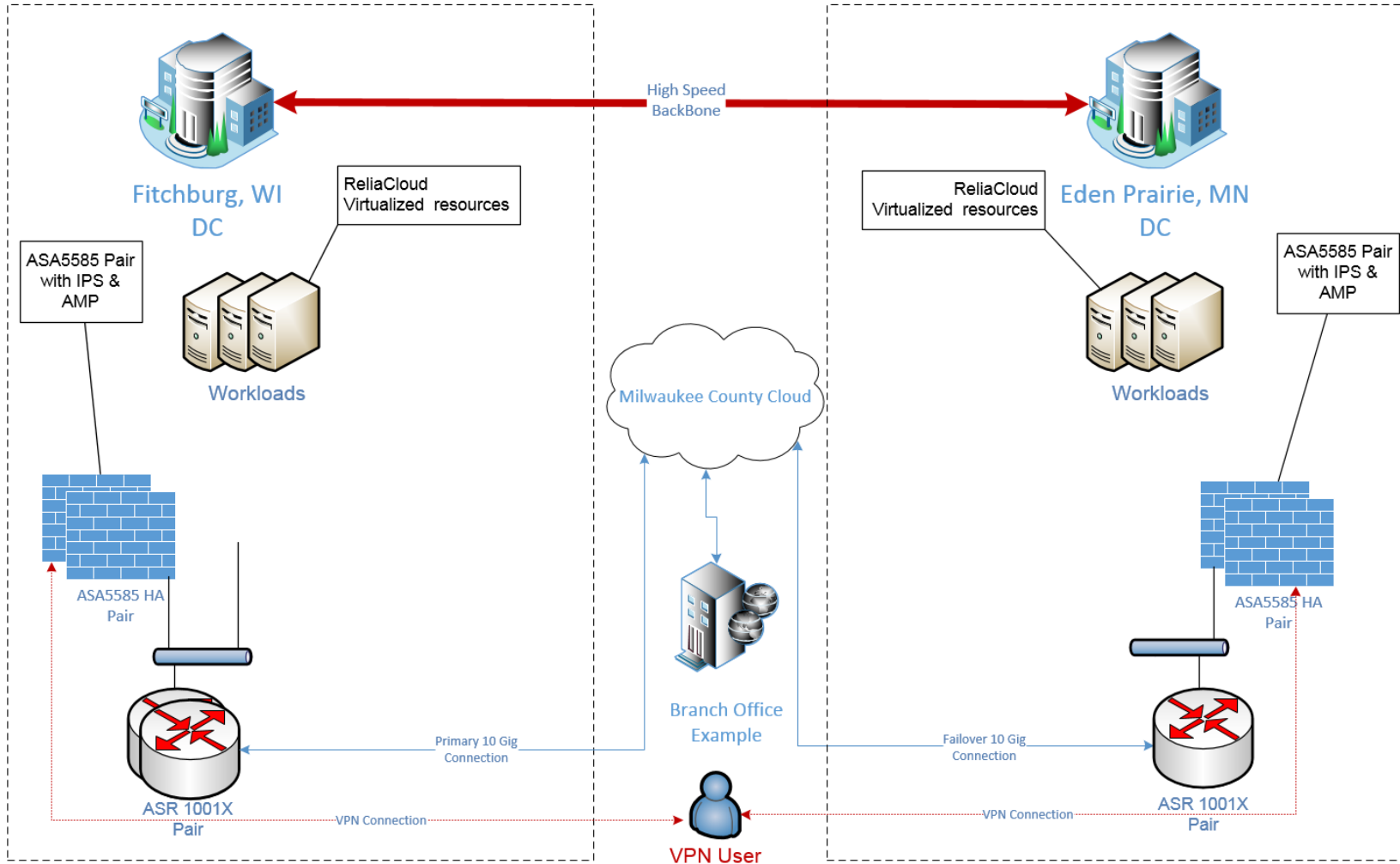
Last Edit Date: 12/23/2015

Milwaukee County
Primary



ReliaCloud Data Center Two Sites

Milwaukee County – ReliaCloud

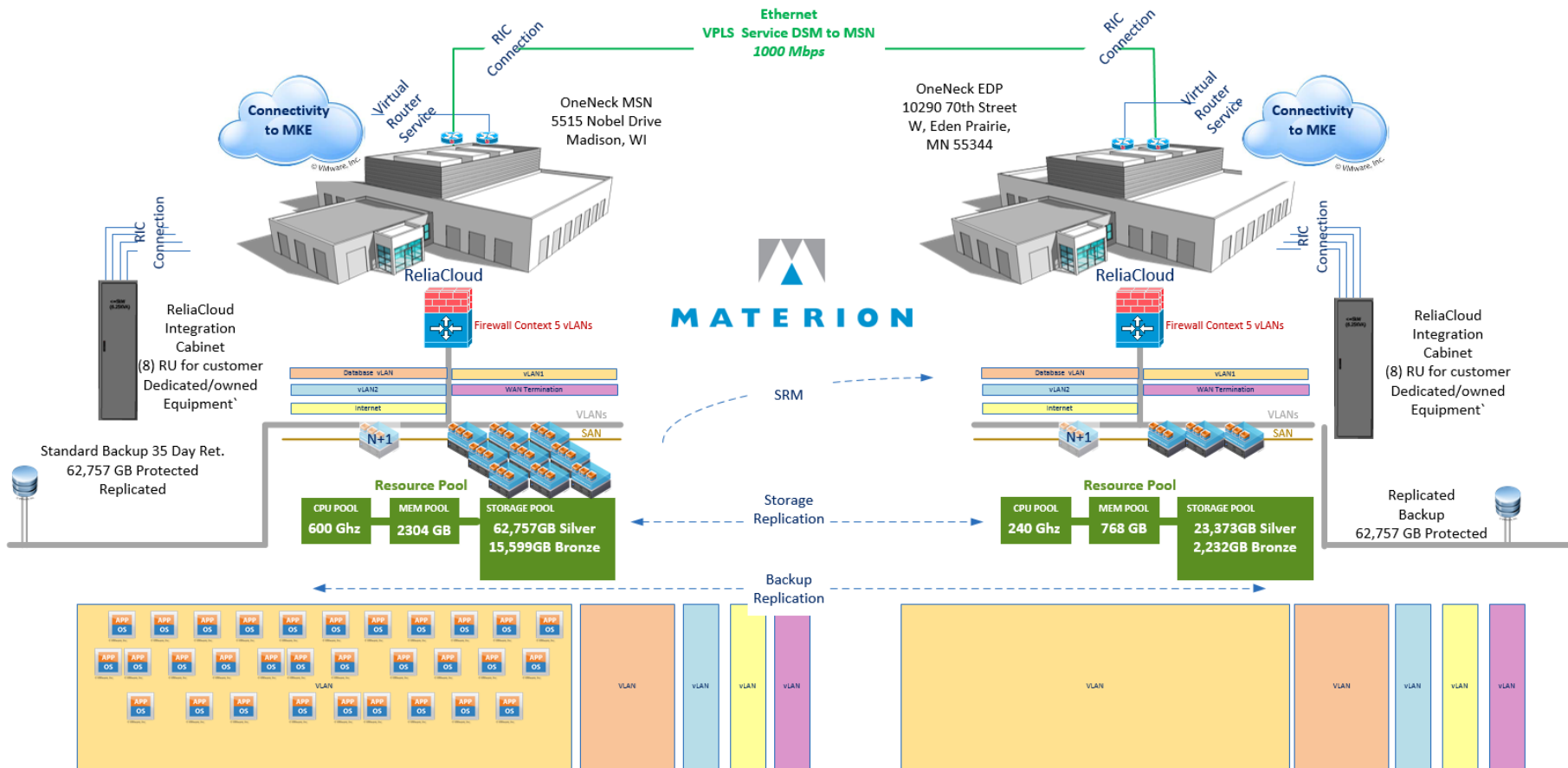


ReliaCloud Data Center Private Cloud at Two Sites

2 Site ReliaCloud Data Center

Production in MSN, 30% for Disaster Recovery in EDP

Last Edit Date: 1/8/2016



Service Innovation

OneNeck has a total company approach to providing innovative technology and service management solutions. We do this as an integral part of how we collaborate with our customers and stems from our belief that “although it might not be our fault – it’s always our problem.”

Solutions Architecture Shared Vision

The solution architecture group focuses on technology and service solutions that meet our clients now and future needs. Below is the Shared Vision for this group:

Our **Purpose** is to deliver creative solutions, built from standard building blocks, targeted to solve our customers’ business problems by providing the right solution, in the right place, on the right platform, at the right time – in the right cloud - to allow our customers’ to focus on their business.

Our **Vision of the Future** is one where Solutions are central to our organization.

- We enable our external customers to focus on their business while we architect and design creative solutions to solve their business problems.
- We support our internal customers in their objectives to increase revenue, decrease cost/expense and align OneNeck's strategy and direction with the market.
- We govern our solutions through a full lifecycle of innovation management, solution strategy, solution development, solution management and solution sales architecture.

We act in line with our **Guiding Values**:

1. Integrity - In our interactions with others, both inside and outside of OneNeck, we always act with honesty, integrity, accuracy and respect.
2. Responsiveness - we constantly work to get out of the way, providing feedback and setting expectations so that there is never a question of "When?" in working with our team.
3. Creativity - we think outside of the box just as well as we think inside the box, we strive to leverage proven techniques and enhance them through our application of those techniques to solve complex problems.
4. Knowledge and Expertise - we constantly strive to learn and expand our knowledge and deepen our knowledge through experience and we see it imperative to share our knowledge to the betterment of others.
5. Collaboration - we work well, and play well, with others, both inside our team and outside of our team, never hesitating to involve others in our day to day activities.

Shared Services Organization

OneNeck subscribes to methods of continuous improvement through our own support methodologies as well as ITIL. For example, OneNeck employees that are in customer facing engineering or support roles are required to become ITIL Foundations certified within the first year of service as a condition of employment. The role of the Service Delivery Manager is integral to our culture of continuous improvement and operational excellence. The SDM will be an escalation point for the County's stakeholders and will be in charge of the quality of service reporting and act as a service ambassador between OneNeck and the County. The SDM role is dually responsible for overseeing the care and feeding of the customer's environment including the steady state maintenance of the technical components as well as incident and change management. Acting as the customer advocate, the Service Account Manager manages customer related issues to help ensure that expectations are properly set and met; and that changes to delivery are proper.

OneNeck Managed Services

OneNeck offers a turnkey, full-service IT Managed Services solution that includes the best certified experts in the industry, live 24/7 expert-to-expert support, tested and proven ITIL best practices in IT managed services and world-class technology. All of this is wrapped in high availability service level agreement that financially guarantees satisfaction. OneNeck managed services are all supported with a detailed Service Catalog.

OneNeck can provide a wide variety of managed services for our customers, whether the systems are located in a OneNeck datacenter, OneNeck ReliaCloud environment or Customer's on premise infrastructure. OneNeck can provide managed services for core network components such as route, switch, firewalls, load balancing, voice & video, UC and more. From a systems perspective OneNeck can provide managed services from the OS and application layer for a wide variety of products including, but not limited to, many ERP applications i.e. SAP, JDE, Dynamics AX, Oracle E-Business Suite.

Shared Infrastructure Operations (SIO)

OneNeck IT Solutions uses a shared services support model to provide exceptional customer service to our enterprise clients. We operate two 24/7 Network Operations Centers in Scottsdale, AZ and Minneapolis, MN. These centers are staffed with technical engineers and customer support personnel with varied expertise across our data center, ReliaCloud and Applications Infrastructure services. OneNeck provides local remote hands in the Madison and Eden Prairie data center on a 24/7/365 basis for emergency services as well.

Your customer support starts with your Account Executive. The AE is responsible for the overall relationship between OneNeck IT Solutions and Milwaukee County. The AE has strategic responsibility to manage and deliver the needed resources for Milwaukee County in an effort to exceed your service expectations over the relationship period. The AE provides product information, pricing information, educational information and coordinates various resources to meet your needs. The AE works closely with an assigned Service Delivery Manager (SDM). The SDM provides day to day support activities for our enterprise clients. They

are closely connected to the required internal departments such as project management, billing, facilities and operations and will advocate for Milwaukee County to deliver your desired outcomes.

Customer Service is a strategic priority for OneNeck IT Solutions

OneNeck’s Customer Management Team (CMT) supports OneNeck’s commitment is to be an expert provider of hybrid IT solutions for mid-market and enterprise companies through high-touch customer service. OneNeck provides customer management focus based on ITIL. To that end, we provide a single role, the Service Delivery Manager (SDM), who is responsible for day-to-day operations of contracted services. For new services and solutions, an assigned Account Executive will be available to leverage technology **solutions for your business**. Your Service Delivery Manager is your single point of contact to ensure the successful coordination and execution of your contracted recurring services. This encompasses all areas, including service management, incident and change management, service improvement, and customer satisfaction. The Service Delivery Manager will have one more accounts depending on the complexity and scope of the services their assigned accounts have with us. The Service Delivery Manager has access to resources throughout our entire customer management team. The following table lists the management team associated with your account starting with the Service Delivery Manager all the way through executive management.

Escalation		
CONTACT TYPE	CONTACT DETAILS	USE GUIDELINES
Support Center (24 x 7 x 365)	Phone: (855) 820-0500	Can be used for any priority of request or issue, but is the best method to ensure P1/P2 items are handled with the appropriate urgency.
Support Center (24 x 7 x 365)	Email: support@oneneck.com	Lower priority requests (3 or less) that do not require immediate action.
Support Portal	Customer Portal: https://cms.tdc.oneneck.com	Can be used to view status on existing requests OR submit any priority of request or issue - follow-up via phone is base for items requiring P1/P2 urgency.
Service Delivery Manager	Name: Email: To Be Assigned Phone:	Any requests or questions at all - your Service Delivery Manager is your advocate and will route items as appropriate.
District Manager	Name: Brian Osterhaus Email: Brian.osterhaus@oneneck.com Phone: (608)204-8668	Strategic, tactical and operational business and IT initiatives – additional services.
Manager, Service Delivery Team	Name: To Be Assigned Email: Phone:	Escalation contact for concerns related to service delivery.

Manager, Service Delivery Team	Name: To be assigned Email: Phone:	Escalation contact for concerns related to service delivery.
VP of Service Transition	Name: Katie McCullough Email: katie.mccullough@oneneck.com Phone: (480) 315-3042	Escalation contact for concerns related to service delivery or account support and management.
VP of Operations	Name: David Arenas Email: david.arenas@oneneck.com Phone: (480) 302-6285	Escalation contact for concerns related to service delivery.
CTO and General Manager	Name: Clint Harder Email: clint.harder@oneneck.com Phone: (406) 646-6505	Escalation contact for concerns related to service delivery or account support and management.

Milwaukee County would also be assigned a Project Manager lead for the implementation and ongoing project management of the Milwaukee County implementation. The PM is a single point of accountability for project management on the OneNeck side and is typically paired with a Milwaukee County peer during project activity.

What are the Three Pillars of Shared Infrastructure Operations (SIO)?

Own IT! – The word "OneNeck" is synonymous with ownership. When all else fails; systems, process, people, or clarity; take ownership.

Understand IT! – The word "OneNeck" stands for unity between the customer and us in providing solutions that meet customer needs. Take time to view the world through the customer lens and provide more than just technical solutions.

Work IT! – Through effort we accomplish customer satisfaction. It may not be your job or your fault, but it is our problem. Being the "OneNeck" means; rising to the occasion, being the leader, and enlisting the aid of others to satisfying our customers.

Proposed Project Hours

Please use the following chart below to assume the amount of project time that should be included as part of the proposed solution(s). Regular technology refresh should not be considered project work.

Support Team	Estimated Annual Project Work Hours
Data Center	0
x86 Server	1,080
Mainframe	0
System Administration	800
Storage and Backup	760
Network	1,320
Security	800
Disaster Recovery	0

OneNeck is taking this chart into consideration for this response. OneNeck IT Solutions has a large and capable Professional services team with 70+ highly certified delivery engineers and project managers. Our methodology for handling the discretionary project hours would be multi-layered. First, we would plan to dedicate two Full-Time engineers to the County. Based on the estimated hours provided we would have one that would be focused on the systems (server\storage\backup) work and another on the network and security work. These would be added headcount to OneNeck and we would encourage existing County Staff to apply for those positions. After training and time-off we estimate a remaining 1,160 project hours still to be filled. We would utilize our existing delivery engineers or Solutionary engineers to fulfill those hours on a scheduled basis based on the County's needs. These would be utilizing a Statement of Work process and scheduled based on availability of engineering resources. To assist in scheduling and coordinating these efforts, we would also assign a Project Manager from the Professional Services organization. We estimate 260 hours of Project Management will be required annually.

Transition and Transformation Strategy and Approach

Provide a description of the proposed strategy and approach to transition and transformation including:

- A high level project plan indicating phases and timeframes

OneNeck Transition/Transformation Activities

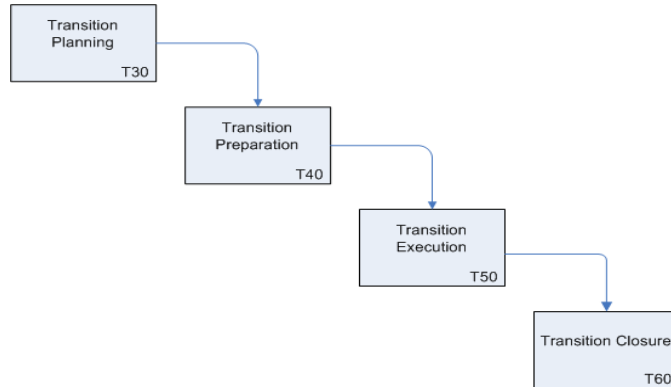
Approach. OneNeck’s approach to assumption of responsibility for customer-provided devices and server workload is to first perform a qualifying audit of the environment to ensure it is in compliance with manufacturer and OneNeck IT Solutions best practices. In most cases, OneNeck IT Solutions will perform 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 OneNeck IT Solutions Remote Managed Services SLA. If OneNeck IT Solutions or one of its companies performs the installation, this audit is waived. OneNeck’s approach to most of the County of Milwaukee applications will be to port them each to a new hardware & operating system environment based on OneNeck’s standard and current templates. This will obviate the need for per-system qualification and will also ensure that these applications will run on systems that qualify for the Managed Services SLA.

Assuming responsibility for managing the County of Milwaukee overall IT environment will involve several service transition projects that will be described in section (b).

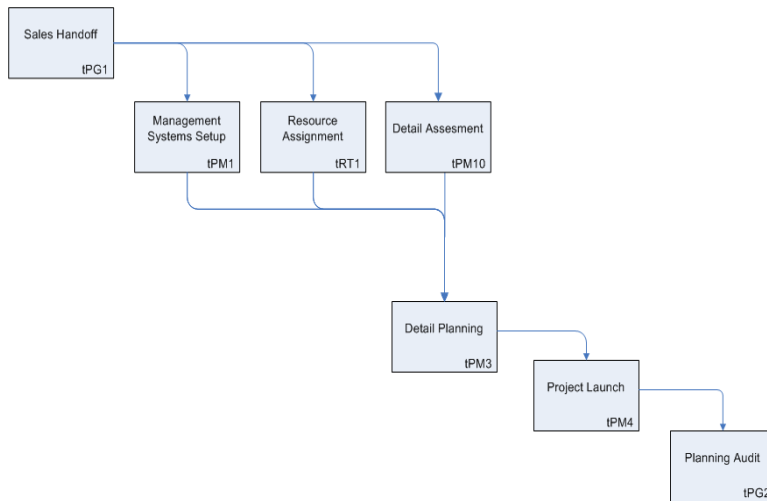
OneNeck has extensive experience assuming management of IT assets and systems, involving both directly managed environments as well as taking over from incumbent 3rd party service providers.

Projects. OneNeck has developed a comprehensive transition framework based on many years of experience in this industry. The actual plan can be tailored or mapped to the County’s project management methodology if needed. Milestones, responsibilities, deliverables, and work products will be agreed upon during the initial phase of the engagement. The flows below depict the high-level tasks involved in a typical transition project.

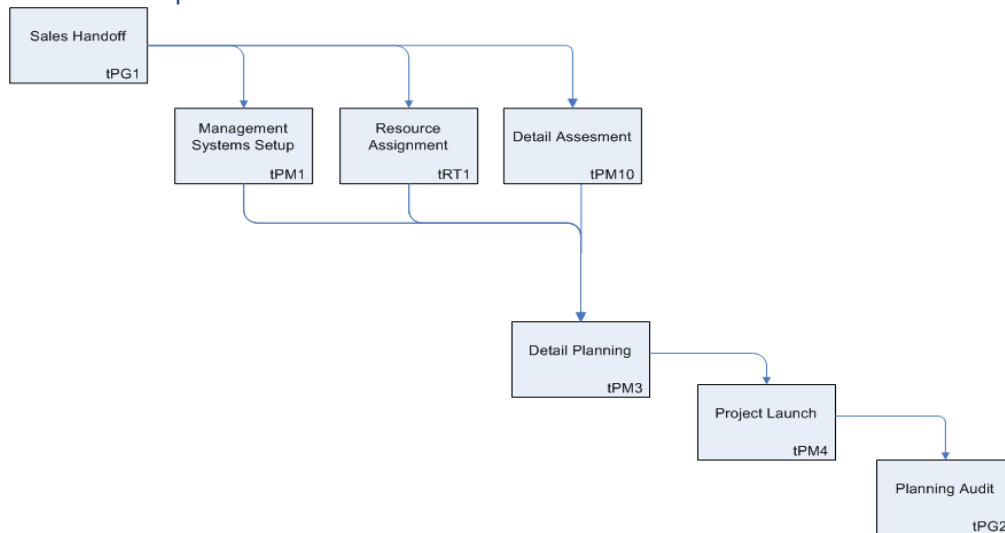
Services Transition:



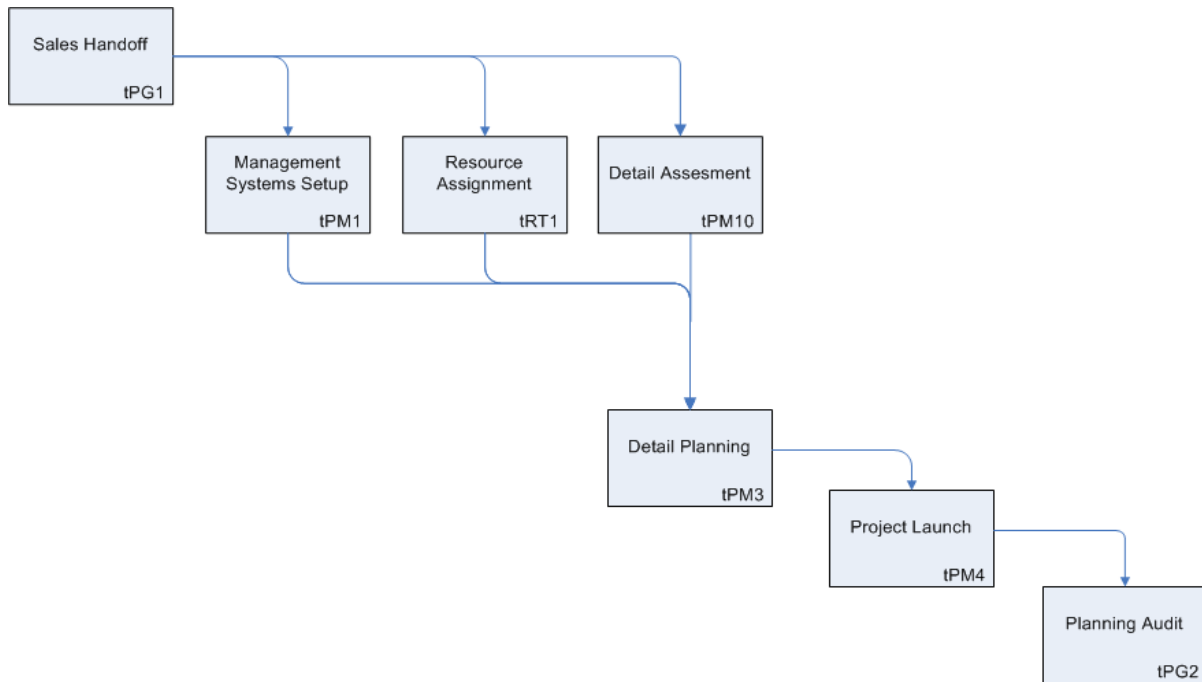
Transition Planning:



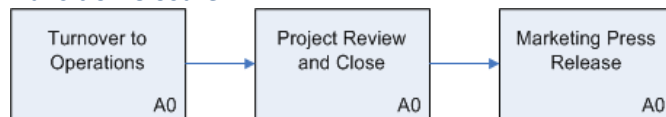
Transition Preparation



Transition Execution:



Transition Closure:



The flows above characterize the projects required to implement each of the components of service, including the high-level timing and sequencing of them,

Please see attachment D3-1 of this document for tables specific to the transition & transformation projects.

OneNeck’s overall approach to managing the transition/transformation projects is led by our Service Transition team as follows:

Projects – OneNeck leverages a Project Manager-led Service Transition team for every customer implementation (not just new customers). The PM is responsible for managing timelines and is primarily responsible for status reviews, facilitating project meetings, and owning all project-related documentation.

Service transition is staffed with certified project managers and engineers certified in each of their respective disciplines (storage, virtualization, management, and compute). OneNeck does not leverage third parties in order to provide resources to

be deployed (e.g., hardware, software, services) as part of service transition & transformation.

Quality assurance is realized through testing of any installed applications and a customer test and acceptance phase. ReliaCloud standards are enforced (supported operating systems, virtual machine versions, etc.).

Once customers accept a project as complete, service transition hands off to the appropriate team (hosting operations, network operations, application support, et al) and we move to a “steady-state” service delivery model that is overseen by the Service Account Manager.

Once in the steady state service delivery phase, reporting to the County is driven by the Service Account Manager and starts at a high level with the Monthly Status Review (MSR) call.

Knowledge Transfer.

OneNeck will work to gather information on current services from the incumbent through an assessment process, the output of which will be validated by the incumbent. Knowledge transfer will be carried out in a similar manner for all components of service: First, OneNeck will conduct an assessment of the current state, secondly the incumbent service actor will validate OneNeck’s assessment results & understanding of the current state.

Because most applications will be refreshed on to more current technology hardware and operating systems, the impact on existing County operations will be specific to application management.

Continuity of Service/OneNeck Transition Approaches.

OneNeck leverages four methods of service transition (listed below), each of which may have a different impact upon continuity of service. Through the assessment process, OneNeck will determine the best course of action for service transition & transformation on a case-by-case, application-centric basis. This approach provides superior alignment to the County’s needs by focusing on applications rather than servers. This approach also minimizes the amount of involvement required of the incumbent service delivery actor.

Technology Refresh Transition Methodology

- Replacement systems are acquired and installed at the OneNeck Data Center in advance of the transition.
- A logical data transfer then moves the processing to the OneNeck facility

Lift & Shift Transition Methodology

- The production environment is secured, shut down, shipped to the OneNeck Data Center

- The environment is set up and re-activated in a one-move process.

Standby Transition System Methodology

- A standby system (usually a test and development system) is transitioned to OneNeck in advance of the transition, and set up as a production standby environment.
- During transition, the standby system is updated with then-current data as a contingency against production system loss or damage during shipment.
- The production system is shipped, set up and re-activated as the production environment.

Live Transition System Methodology

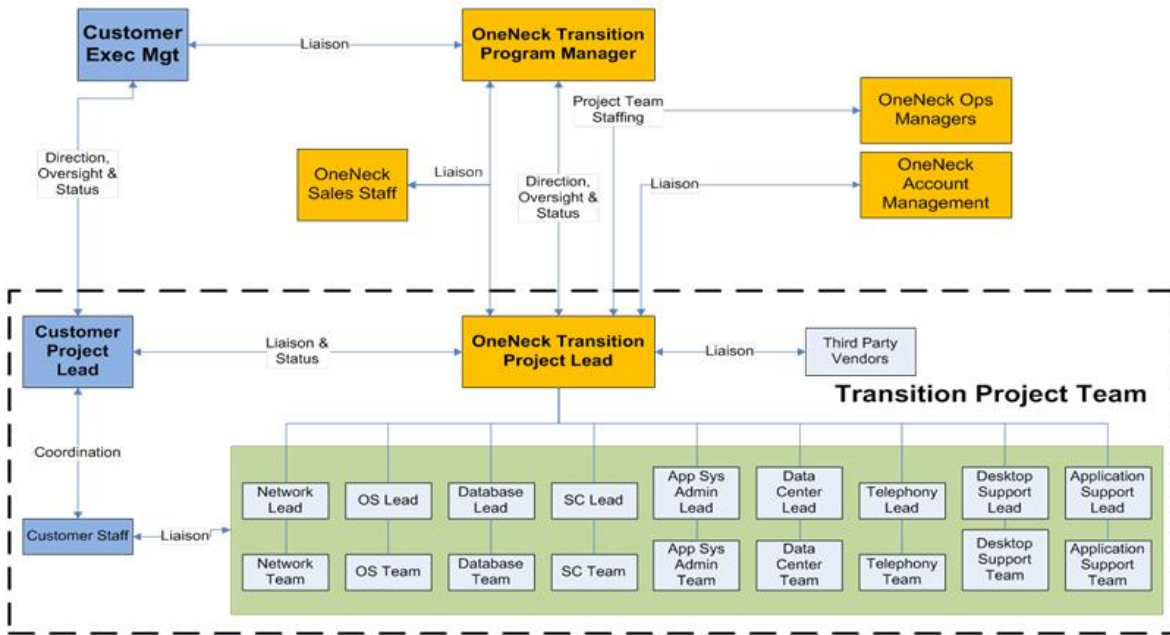
- A live system (usually a test and development system) is transitioned to OneNeck in advance of the transition, and set up as a production environment.
- The Production data and processing is transitioned to this system during an initial transition milestone.
- Subsequently, the production environment is transitioned and set up, and the production data and processing is transitioned to this system as a second transition milestone.

Supplier's Transition/Transformation Team. OneNeck's Service Transition Team is constructed of a team of certified project managers and engineers who are focused on onboarding of customers and new builds of virtual and physical IT infrastructure within our existing ReliaCloud framework. Details around the OneNeck service transition team include:

Service transition team is comprised of four Project Managers, two Network Engineers, two Virtualization/Systems Engineers, and two Storage Engineers. This team would be expanded in the event OneNeck is awarded the County of Milwaukee RFP.

The service transition PM and the Service Delivery Manager (SDM) are jointly responsible for transition team-to-operations handoffs. The SDM and PM work to ensure that Service Operations has documented procedures in place for every customer's Service Desk, Asset Management, Event Management, Incident Management, Problem Management, and Access Management. OneNeck has moved hundreds of customers of varying sizes and scopes of service through this process.

The chart below shows OneNeck's approach to service transition team roles. It is expected that this structure and team will be in place until the transition is completed and the new environment is validated. The customer will be responsible for providing an Executive Sponsor, Project Lead and various Subject Matter Experts (SMEs) primarily focused on technical areas.



County-Provided Resources.

OneNeck will require the following full-time employees (or 3rd party) from the County as part of Transition & Transformation: Application Architect, Network Lead, OS Lead, Database Lead, and Project Lead (in charge of coordination, controls and oversight). These roles will be required for up to one year’s transition time. Detailed transition planning such as project definition will take place and a custom program & project plan will be built.

OneNeck will primarily providing services out of our MSN data center facility and will therefore not require the use of County resources or facilities to perform managed services activities. At the County’s request on-site meetings with the OneNeck managed services team could be conducted at any of the County’s locations at their specific direction. Otherwise OneNeck has locations within the Madison area that can accommodate these face-to-face meetings. Limited use of resources at the County data center\facilities may be requested, however this is not expected to exceed that which is already needed.

Solutionary Transition/Transformation Activities

Approach. Provide a thorough description of Supplier’s approach to:

Assuming responsibility for the Services and building/readying the operations to perform as described in its solution as it pertains to each of the relevant factors of production (e.g., people, process, facilities, technology, training, knowledge); and

At the onset of the Solutionary Managed Security Service engagement, Solutionary and the County will embark on an Onboarding and Account Governance process to implement or optimize any hardware required for the solution and establish the guidelines, policies, processes that will govern the MSS relationship between Solutionary and the County. A Governance Document that details service definitions, communication channels/protocols, account review cadence/requirements, account reporting cadence/requirements, maintenance schedule, event monitoring and notification, incident response procedures, etc. will be developed, reviewed, and finalized by Solutionary and the County.

Taking over the services from the incumbent delivery actor(s).

If necessary and possible, Solutionary will hold meetings and interviews with the incumbent to understand the managed services currently provided to the County of Milwaukee and formulate a plan of action to transition such services from the incumbent to Solutionary with the goal of transforming the incumbent solution to Solutionary's proposed solution.

Projects. Provide a thorough description of the activities Supplier will perform to enact the transition/transformation, including:

A graphical roadmap that describes the projects required to implement each of the components of service, including the:

Overall duration of the Transition and Transformation stages;

Start and stop dates for each project within the Transition and Transformation stages; and

Sequencing of the projects relative to one another; and

Please reference the MSS Onboarding Project Timeline PDF

For each project shown in the roadmap, and using the template set forth in Attachment D3-1 of this document, a table that provides textual information regarding each of the following items:

Project Name. A short, but descriptive name for the project;

Project Type. Identify whether the project is a Transition project or Transformation project (it cannot be both);

Begin/End Dates. The dates on which the project will begin and end;

Scope. A synopsis of the scope of work for the project, including a list of the major activities;

Deliverables. A list of the major deliverables of the project;

Key Milestones. A list of the major operational milestones for the project;

Project Dependencies (Supplier). A list of Supplier's other projects on which performance of the project in question are dependent upon;

Project Dependencies (non-Supplier). A list of the project's dependencies, if any, outside of Supplier's control; and

Risk Mitigation. A list of the major risks inherent in the project and Supplier's plans of mitigating, measuring and reporting on each to County.

Additional scoping will be required upon the County's selection of Solutionary as their new managed security services provider in order to provide requested project details, including start and stop dates, dependencies, and strategies for mitigating risk during transition/transformation.

A description of Supplier's overall approach to managing the transition/transformation, including the underlying:

Projects;

Personnel;

Third parties involved in providing resources to be deployed (e.g., hardware, software, services);

Testing and other quality assurance methods;

Acceptance of the changes by County; and

Reporting to County.

Service onboarding activities entail 3 phases.

- 1) Governance documentation – This phase typically takes 2-4 weeks to document the processes, organizational escalation paths, change control, etc. A designated service delivery coordinator will schedule the proper resources necessary for gathering proper governance documentation. Please see the response located in the Governance section of this document 2.3 (c) for additional governance documentation detail.
- 2) Baseline and Optimization – Initial tuning and configuration activities to properly identify security events of interest typically takes 4-6 weeks. This establishes the necessary baselines and anomaly detection configurations to provide relevant security event data for SOC investigation, alerting, and remediation activities.

Personnel from each relevant practice will be involved throughout the onboarding period. Solutionary and OneNeck, are the only parties involved in managed security services delivery. The Solutionary governance document will outline agreed processes for QA and change control approval. Reporting is delivered during regular meetings to review status, gather approvals, and coordinate required information.

Knowledge Transfer. Provide a thorough description of:

How the transfer of knowledge from the incumbent delivery actors to Supplier will occur for each component of service; and

The impact on the existing operations (e.g., County's incumbent supplier, County, other County suppliers) to participate in Supplier's knowledge transfer activities, including a list of the number of resources by skill set and, for each such resource, the amount of elapsed and active time required.

Delivery personnel have integrated processes and configuration standards to involve SOC resources for operations activities once proper communications are established. There is no anticipated impact to County resources or other suppliers to facilitate knowledge transfer between delivery and SOC personnel.

Continuity of Service. Provide a thorough description of how continuity will be preserved during the Transition/Transformation for each component of service.

The comprehensive and detailed description of process and deployment activities will be further expanded and detailed out upon the down selection of this proposal where additional scoping activities are able to take place. All of the net new services being stood up as a portion of the managed security services will be stood up in parallel environment leveraging all of the new services. The components include Firewall Hardware with inclusive Intrusion Prevention technology which will be put into the new architecture and all rulesets from the existing environment will be reviewed for validity and migrated into the new services component. The malware analysis component will like the FW/IPS be deployed with some inline functionality which will be in place prior to cutting business services to the new infrastructure and will be thoroughly tested and vetted to ensure minimal impedance on any business processes. For the other components including Security Information and Event Management and Vulnerability Management are passive secondary technologies which do not interfere with primary infrastructure, so those components will be fully stood up and enabled within the new infrastructure prior to beginning to migrate business processes to the new parallel infrastructure. This buildout of the new security management/monitoring infrastructure in the new overall infrastructure, will

facilitate a smooth cutover of business processes in the new environment making it as seamless as possible to the business. This will be in full coordination with the other service providers to ensure that the process is done holistically to ensure full design and security functionality enablement in the new infrastructure.

Supplier's Transition/Transformation Team. Provide a thorough explanation of the team(s) of resources Supplier will deploy to perform the Transition/Transformation, including:

A list of the number of Supplier's personnel by function that will perform the Transition/Transformation;

An organization chart describing Supplier's overall team of Transition/Transformation personnel; and

A description of how this team will interact with Supplier's delivery team providing support for operations during the Transition/Transformation.

A designated service delivery coordinator will be assigned at the transition/transformation stage and will remain designated throughout the contract term. Additional scoping will be required to provide specific numbers of personnel involved. This team has integrated processes to involve SOC resources for operations once technologies have proper connectivity.

County-Provided Resources. Provide a thorough accounting of the:

Number of County personnel by skill set and time commitment (elapsed and active) requested by Supplier for each such skill set to perform specified non-knowledge transfer type activities (e.g., advisory, review, decision-making) during the Transition/Transformation; and

Resources (e.g., desks, hardware, network connectivity, physical storage space, system access) requested to be provided by County to Supplier to enable Supplier's performance of its Transition/Transformation.

Solutionary transition/transformation services will be performed remotely. Any requirements for network connectivity or remote hands will be requested from OneNeck.

Transition/Transformation Project Description Template

TRANSITION PROJECTS

Where the “E+x” convention is used in the tables below (e.g., in the Due Date column), “E” means the Effective Date and “x” means the number of months after the Effective Date. For example, “E+2” means that the defined event will occur within (i.e., on or before the last day of) the second month following the Effective Date

Transition Project #1 – Primary Data Center Compute Infrastructure Managed Services Enrollment

Transition Project #1 – Primary Data Center Transition			
Migrate data center services from County facility to OneNeck “MSN.”	Migrate data center colocation & IaaS services. Tech refresh primarily onto OneNeck’s “ReliaCloud” IaaS platform. Physically move equipment that shouldn’t/cannot be migrated into ReliaCloud.		
Key Activities	Milestone?	Due Date	Proposed Acceptance Criteria (if any)
<i>Team Assembly – identification of lead OneNeck participants</i>	No	<i>E+.75</i>	Team assembled named and submitted to County. Client kickoff meeting scheduled.
<i>Client kickoff meeting</i>	Yes	<i>E+1</i>	
<i>Inventory existing data center</i>	Yes	<i>E+3</i>	Detailed inventory and assessment of all compute infrastructure assets. Audit and remediation list.
<i>Identification of systems</i>	Yes	<i>E+4</i>	Inventory of systems to be migrated “as-is” vs. systems that will be “forklift migrated” (rebuilt on new OSE within ReliaCloud). Migration plan submitted to County from OneNeck Professional Services.
<i>Remediation of devices</i>	Yes	<i>E+4</i>	“As-is” devices that are out of spec are now compliant to OneNeck standards. Audit / Remediation validated checklist.
<i>Physical migration plan complete</i>	Yes	<i>E+5</i>	Test migration(s) validated. Migration plan finalized (timing).
<i>WAN links turned up, connections live & tested</i>	Yes	<i>E+6</i>	Successful virtual migration(s). Migration of systems to commence.

Transition Project #1 – Primary Data Center Transition	
Project Start Date	<i>30 days from contract execution</i>
Project Completion Date	E+11
Assumptions, Dependencies, Supplier Requirements of County	<p>Assumptions:</p> <ul style="list-style-type: none"> • Transport provider delivers robust connectivity to MSN <p>Dependencies:</p> <ul style="list-style-type: none"> • CenturyLink <p>Supplier Requirements of County:</p> <ul style="list-style-type: none"> • Access to Eagan facility
Risk Mitigation	<p>Risk #1: Loss of connectivity</p> <p>Mitigation for Risk #1: Multiple carriers</p>

Transition Project #2 – County Data Center Managed Services Enrollment

Transition Project #2 Title – County Data Center Managed Services Enrollment			
Project Description and Scope	OneNeck to assume management of compute-network-storage at the County data center. All operating system environments, network nodes and storage arrays to be monitored, patched and remediated by OneNeck Managed Services team.		
Key Activities	Milestone?	Due Date	Proposed Acceptance Criteria (if any)
<i>Team Assembly – identification of lead OneNeck participants</i>	No	<i>E+.75</i>	Team assembled named and submitted to County. Client kickoff meeting scheduled.
<i>Client kickoff meeting</i>	Yes	<i>E+1</i>	
<i>Environment(s) assessment and audit: general inventory</i>	No	<i>E+2</i>	Detailed inventory and assessment of all network County Hall data center compute and storage assets. Audit and remediation list.
<i>Remediation of devices</i>	Yes	<i>E+4</i>	All devices that are out of spec are now compliant to OneNeck standards. Audit / Remediation validated checklist.
<i>Migration design document</i>	Yes	<i>E+5</i>	Strategic plan document for migration and planned change windows.

Transition Project #2 Title – County Data Center Managed Services Enrollment			
<i>Compute services enrollment</i>	Yes	<i>E+7</i>	All Compute infrastructure endpoints enrolled under OneNeck monitoring and Management
<i>Storage enrollment</i>	Yes	<i>E+9</i>	All storage infrastructure endpoints enrolled under OneNeck monitoring and Management
<i>Alert Tuning, Documentation and Reporting Portals Complete</i>	Yes	<i>E+12</i>	All devices have been tuned for alerts and performance thresholds. Client presentation layer is complete.
Project Start Date	<i>30 days from contract execution</i>		
Project Completion Date	E+11		
Assumptions, Dependencies, Supplier Requirements of County	<p>Assumptions:</p> <ul style="list-style-type: none"> County network devices can be remediated to OneNeck management standards Existing provider will allow administrative level access to devices in a timely fashion <p>Dependencies:</p> <ul style="list-style-type: none"> Transformation is completed for end of life and service support equipment <p>Supplier Requirements of County:</p> <ul style="list-style-type: none"> Administrative and physical access to the devices Logical diagrams of the infrastructure 		
Risk Mitigation	<p>Risk #1: Completion of project is dependent upon the transformation of the end of life end of support equipment, being configured and in place.</p> <p>Mitigation for Risk #1: [Tech refresh/retirement of non-compliant systems]</p>		

Transition Project #3, Network Managed Services Enrollment

Transition Project #3, Network Managed Services Enrollment			
Project Description and Scope	<p>This project will transition the Network service infrastructure for the components of :</p> <ul style="list-style-type: none"> Network Access / WAN / LAN LAN Transport Services Public Works (SCADA) <p>To the OneNeck Managed services team.</p>		
Key Activities	Milestone?	Due Date	Proposed Acceptance Criteria (if any)

Transition Project #3, Network Managed Services Enrollment			
<i>Team Assembly – identification of lead OneNeck participants</i>	No	<i>E+.75</i>	Team assembled named and submitted to County. Client kickoff meeting scheduled.
<i>Client kickoff meeting</i>	Yes	<i>E+1</i>	
<i>Environment(s) assessment and audit: general inventory</i>	No	<i>E+2</i>	Detailed inventory and assessment of all network infrastructure assets. Audit and remediation list.
<i>Remediation of devices</i>	Yes	<i>E+4</i>	All devices that are out of spec are now compliant to OneNeck standards. Audit / Remediation validated checklist.
<i>Migration design document</i>	Yes	<i>E+5</i>	Strategic plan document for migration and planned change windows.
<i>WAN services enrollment</i>	Yes	<i>E+7</i>	All WAN infrastructure endpoints enrolled under OneNeck monitoring and Management
<i>LAN core/edge/wireless enrollment</i>	Yes	<i>E+9</i>	All LAN services infrastructure endpoints enrolled under OneNeck monitoring and Management
<i>Alert Tuning, Documentation and Reporting Portals Complete</i>	Yes	<i>E+12</i>	All devices have been tuned for alerts and performance thresholds. Client presentation layer is complete.
Project Start Date	<i>E+1</i>		
Project Completion Date	<i>E+12</i>		
Assumptions, Dependencies, Supplier Requirements of County	<p>Assumptions:</p> <ul style="list-style-type: none"> County network devices can be remediated to OneNeck management standards Existing provider will allow administrative level access to devices in a time fashion <p>Dependencies:</p> <ul style="list-style-type: none"> Transformation is completed for end of life and end service support equipment <p>Supplier Requirements of County:</p> <ul style="list-style-type: none"> Administrative and physical access of the devices County resource availability to provide access to equipment locations 		
Risk Mitigation	<p>Risk #1: Completion of project is dependent upon the transformation of the end of life end of support equipment being configured and in place.</p> <p>Mitigation for Risk #1: This will be addressed with project management.</p>		

Transition Project #4, Network Equipment Refresh

Transition Project #4 Title <i>Network Equipment Refresh</i>			
Project Description and Scope	Equipment transformation to newer model equipment for the network components of: <ul style="list-style-type: none"> • Network Access / WAN / LAN • LAN • Transport Services • Public Works (SCADA) 		
Key Activities	Milestone?	Due Date	Proposed Acceptance Criteria (if any)
<i>Team Assembly – identification of lead OneNeck participants</i>	No	<i>E+.75</i>	Team assembled named and submitted to County. Client kickoff meeting scheduled.
<i>Client kickoff meeting</i>	Yes	<i>E+1</i>	
<i>Confirmation of Equipment and Approach. Equipment Ordering</i>	Yes	<i>E+2</i>	Equipment or order. Order ETA
<i>Development of Migration Strategy</i>	Yes	<i>E+2</i>	Migration Strategy Doc
<i>Staging / Burn-in / Deployment</i>	Yes	<i>E+6</i>	All equipment racked in designated locations
<i>Managed Services Commissioning</i>	Yes	<i>E+12</i>	All devices have been tuned for alerts and performance thresholds. Client presentation layer is complete.
<i>End of Life, End of Sale Equipment decommissioning</i>	Yes	<i>E+12</i>	All EoL / EoS Devices are transitioned to their new use, or removed from County inventory.
Project Start Date	<i>E+1</i>		
Project Completion Date	<i>E+12</i>		
Assumptions, Dependencies, Supplier Requirements of County	Assumptions: <ul style="list-style-type: none"> • County has available equipment space to support the transition process (New + Old) equipment coexistence. Dependencies: <ul style="list-style-type: none"> • Availability of Cisco inventory 		

Transition Project #4 Title <i>Network Equipment Refresh</i>	
	<ul style="list-style-type: none"> Availability of power and equipment space at County locations to house the existing equipment plus the new infrastructure for replacement. <p>Supplier Requirements of County:</p> <ul style="list-style-type: none"> Availability of power and equipment space at County locations to house the existing equipment plus the new infrastructure for replacement.
Risk Mitigation	<p>Risk #1: Cisco equipment lead times</p> <p>Mitigation for Risk #1: [None] need to develop a strategy with Cisco once inventory is finalized.</p>

Transition Project #5 – Disaster Recovery

Transition Project #5 Title – Disaster Recovery			
Project Description and Scope	OneNeck to assume responsibility for disaster recovery of systems.		
Key Activities	Milestone?	Due Date	Proposed Acceptance Criteria (if any)
<i>Per-system & per-application RPO & RTO defined</i>	Yes	<i>E+2</i>	Mutually agreed-upon RPO & RTO definitions for each application environment’s supporting systems.
<i>Infrastructure for DRaaS components installed</i>	Yes	<i>E+6</i>	ReliaCloud Recovery infrastructure put in place at protected site and recovery site and tested
<i>Test failovers executed</i>	Yes	<i>E+8</i>	Application testing & validation
Project Start Date	<i>30 days from contract execution</i>		
Project Completion Date	E+10		
Assumptions, Dependencies, Supplier Requirements of County	<p>Assumptions:</p> <ul style="list-style-type: none"> Software will be compatible with systems the County wishes to have protected <p>Dependencies:</p> <ul style="list-style-type: none"> Compatibility of systems, availability of storage & management compute resources at the protected and recovery sites 		

Transition Project #5 Title – Disaster Recovery	
	Supplier Requirements of County: <ul style="list-style-type: none"> Facilitate access & authorization on protected systems. Resources to test applications & access during the testing phase.
Risk Mitigation	Risk #1: Legacy system instability Mitigation for Risk #1: Tech refresh

TRANSFORMATION PROJECTS

Where the “T+x” convention is used in the tables below (e.g., in the Due Date column), “T” means the date Transformation commences and “x” means the number of months after the date Transformation commences. For example, “T+2” means that the defined event will occur within (i.e., on or before the last day of) the second month following the date Transformation commences.

Transformation Project #1, ReliaCloud Service Transformation

Transformation Project #1 – ReliaCloud Service Transformation			
Project Description and Scope	County of Milwaukee to run IT workloads in ReliaCloud.		
Key Activities	Milestone?	Due Date	Proposed Acceptance Criteria (if any)
<i>Detailed Solution Scoping</i>	Yes	<i>E+0</i>	Solution Architect to build mutually-acceptable Customer Requirements Worksheet (CRW)
<i>Contract Review and Submission</i>	No	<i>E+1</i>	OneNeck internal process to validate compatibility and service alignment
<i>Customer Engagement Review</i>	Yes	<i>E+3</i>	Mutual acceptance of CRW, scope of project and timing. Technical requirements validation.
<i>Service Delivery & Transition</i>	Yes	<i>E+6</i>	Customer handoff, portal(s) training, test of management access connections.
<i>Service Operations takeover</i>	Yes	<i>E+8</i>	Technical support & services verification (ITIL-guided service operations)
Project Start Date	<i>30 days from contract execution</i>		
Project Completion Date	<i>E+7</i>		
Assumptions, Dependencies, Supplier Requirements of County	Assumptions: <ul style="list-style-type: none"> Compatible workloads to be migrated. Dependencies:		

Transformation Project #1 – ReliaCloud Service Transformation	
	<ul style="list-style-type: none"> • Compatibility of systems & resources provisioned to meet necessary performance levels. Supplier Requirements of County: <ul style="list-style-type: none"> • Facilitate access & authorization
Risk Mitigation	Risk #1: Legacy system instability Mitigation for Risk #1: Tech refresh

- Key planning assumptions
OneNeck’s assumptions are included in our high-level project plan above.
- High level transition team resource expectations and roles and responsibilities for Milwaukee County and the service provider
Please see this information in our high-level project plan above.
- Onboarding of service provider resources including background checks and qualifications
OneNeck IT Solutions takes seriously the security of both our customers and employees. As such, it is our policy to conduct pre-employment background checks and drug screens using the Company’s approved vendors. All background checks include verification of an applicant’s highest level of education, employment verification of the last 7 years, criminal (national and county) checks for all places the applicant resided in the past 7 years and SSN check. All offers of employment are contingent upon clear results of a thorough background check, consistent with both company policy and the law.

Data center access is 24/7/365 unescorted access for customers who are authorized/have on-boarded and have their access card with aligned iris scan.

Access to OneNeck’s data centers is highly secure and controlled. Customers who have gone through the authorization process/on-boarded with us access the data center via two-factor authentication: Proximity Card (badge) and biometric iris scan. Before entering the secure data center, there is an access badge scan into a “people-trap,” and then an access badge scan and a biometric iris scan prior to entry into the data center. All of the access activity is recorded by digital video surveillance. Additionally, there is an anti-tailgate sensor which records how many individuals entered the facility with one person’s credentials, which will sound an alarm as appropriate. Once in the data center, there is yet another badge scan and biometric iris scanner before entering a specific data room.

OneNeck offers various options for access control to a customer’s rack/cage: a combination lock is the standard approach; additional options (with an additional associated cost) include card access and biometric touch-point access.

- Onboarding of Milwaukee County employees the vendor chooses to retain, even though the County is not requiring the service provider onboard any of the County’s existing staff.
OneNeck is responsible for escorted access control (for visitors, vendors, etc.) to a customer’s cabinet/cage.

OneNeck will allow 24/7/365 unescorted access for customers who have completed the authorization/on-boarding process and have a valid access card and iris scan.

Requirements Matrix

Appendix C – Requirements Matrix is a spreadsheet that lists all of the requirements for the in scope support services and hardware. Each of the tabs in the spreadsheet represent a different area of requirements as outlined above.

For each tab and requirement in Appendix C – Requirements Matrix (excluding Performance Standards tab0, the service provider should indicate if its proposed solution exceeds, meets, partially meets, or does not meet the requirement. The service provider should add comments to qualify its response, especially for those requirements marked as “exceeds” or “partially meets.”

Please find our responses to Appendix C – Requirements Matrix included in the embedded Excel spreadsheet below.



Appendix C -
Requirements Matri:

Experience Matrix

The service provider should complete the Excel spreadsheet titled “Appendix D – Service Provider Experience Matrix.” This spreadsheet captures the service provider’s experience in the key technologies outlined in this RFP.

Please find our responses to your Experience Matrix request included in the Excel spreadsheet embedded below.



Appendix D -
Milwaukee County E

Proposed Pricing

The service provider should include its proposed pricing information using a spreadsheet format. The service provider is allowed to structure the pricing information based on its own pricing mechanisms, assuming the pricing follows the following pricing guidelines:

- One-time transition costs should be identified and separated from other on-going service costs
- On-going service costs should be quoted as annual costs and provide separately for each of the following areas:
 - Data Center Facility services
 - Mainframe support services
 - Server support services
 - Storage and backup support services
 - Network support services
 - Security support services
 - Data circuits related to service provider's data center
 - Disaster recovery services
 - Any additional usage based costs that would be in addition to those costs outlined above
- Pricing mechanisms should be provided to allow for increases and decreases in the volume of support services over time (i.e. ARC/RRC mechanisms).
- Include representative hourly rates for potential out of scope, project related services in the categories appropriate to cover the in scope technologies.

Please find our pricing information included in your Pricing Template spreadsheet embedded below.



Appendix B.7 -
Milwaukee County F

Exhibit 1 – Intent to Respond Form



8.0 Exhibits for Execution

All exhibits require completion and execution as a component of the RFP process. Unless otherwise noted, the exhibits are due and are to be included with your response.

8.1 Exhibit 1 - Intent to Respond Form

Please sign, scan, and email this form indicating your intent to respond to this RFP. The deadline for returning this form is November 25th by 12:00 PM CST. Electronic signatures are acceptable.

To: Meghan Niven (mniven@excipio.net)
 Date: January 8, 2016
 Primary Contact: Brian Osterhaus
 Company: OneNeck IT Solutions LLC
 Phone: (608) 204-8668
 Fax: (608) 664-8309
 E-mail address: Brian.Osterhaus@OneNeck.com

Please indicate whether or not you intend to respond to this RFP by checking Yes or No.

RFP Component	Bidding (Y or N)
Data Center	Yes
Mainframe	No
x86 Servers	Yes
Cloud Infrastructure	Yes
Storage and Backup	Yes
Network	Yes
Security	Yes
Disaster Recovery	Yes

Our anticipated submission date is: January 8, 2016


Contact Signature: 
 Title: District Sales Manager

Exhibit 2 – Vendor Information



By signing the above I certify, that I have authorization from the Company named above, to respond to this solicitation.

8.2 Exhibit 2 – Vendor Information Form

This form must be completed and submitted with bid response. It is intended to provide the County with information on the vendor's name and address and the specific persons who were responsible for preparation of the vendor's response. Each vendor must also designate a specific contact person who will be responsible for responding to the County if any clarification of the vendor's response should become necessary.

Vendor Name: OneNeck IT Solutions LLC

Vendor Address: Office: 525 Junction Road, Madison, WI 53717

Data Center: 5515 Nobel Drive, Fitchburg, WI 53711

Phone Number: (608) 204-8668 FAX: (608) 664-8309

E-mail: Brian.Osterhaus@OneNeck.com

Vendor Response Prepared By: Brian Osterhaus, Terry Sielaff, John, Hein, James Brown, Bob Chaplin, and Rebecca Mittelsteadt


Signature: 

Exhibit 3 – Milwaukee County’s Minimum Wage Provision

8.3 Exhibit 3 – Milwaukee County’s Minimum Wage Provision

**Declaration of Commitment to Compliance with
Milwaukee County’s Minimum Wage Provision**

Bid/RFP #: Milwaukee County Data Center Operations Professional Services

In accordance with Chapter 111 of the Milwaukee County Code of General Ordinances, it is the policy of Milwaukee County that certain contractors, subcontractors, lessees and recipients of financial assistance doing business with the county shall pay employees performing part or full time work for the county a minimum wage rate. The current required minimum wage rate is as follows:

Effective Date	Base Wage Required (\$ per hour)
June 1, 2015	\$11.66

Milwaukee County’s Minimum Wage Ordinance generally applies to employers with more than 20 employees that entered into one of the following types of contracts or agreements as of June 1, 2014:

- Service Contracts under Chapter 32 of the Milwaukee County Code of General Ordinances
- Certain Personal Care/Supportive Home Care Services provided by agencies that contract exclusively with Milwaukee County
- Concession Contracts
- Lease Agreements
- Economic Development Financial Assistance Agreements

Exemptions to the policy are listed in section 111.03(2), Milwaukee County Ordinances.

In order to be considered responsive to the Bid/RFP, you must submit this form.

The undersigned hereby agrees to the following:

- To pay all workers employed by the Contractor in the performance of this contract, whether on a full time or part time basis, a base wage of not less than the minimum wage rate as determined annually by Milwaukee County.
- New rates that go into effect (annually on the last business day of February) will be adhered to promptly.
- To provide the Milwaukee County Office of the Comptroller-Audit Services Division a Declaration of Compliance and supporting payroll data every three (3) months during the contract term and within 10 days following the completion of the contract.
- To procure and submit a like Declaration and supporting payroll data from every subcontractor employed by the contractor.

I believe that I am exempt from Chapter 111 for the following reasons:

Please attach documentation to substantiate your claim of an exemption. Milwaukee County will review the documentation you provide; if your exemption is not substantiated, your proposal/bid will be deemed unresponsive, and will be removed from further consideration.

I declare under penalty of perjury that the forgoing is true and correct. I have read and understand Chapter 111 of the Milwaukee County Ordinances. I have executed this Declaration on January 8, 2016 (date).

Company Name: OneNeck IT Solutions LLC

Authorized Signature: 

Printed Name: Brian Osterhaus

Exhibit 4 – Insurance and Indemnity Acknowledgement Form

Addendum A

8.4 Exhibit 4 – Insurance and Indemnity Acknowledgement Form

Vendor must at the time of the contract award provide to the County proof of all Liability clauses listed below:

Indemnity:

~~Contractor~~The parties agrees to the fullest extent permitted by law, to indemnify, defend and hold harmless, the ~~County~~other party and its agents, officers and employees, from and against ~~all loss or expenses~~any third party claim including ~~cost and attorney's fees by reason of liability for damages including suits at law or in equity, caused by any wrongful, intentional, or negligent act or omission of the indemnifying party, or its (their) agent(s) which may arise out of or are connected with the activities covered by this Agreement~~to the extent based on: (i) the services provided by Contractor or Contractor's software used to provide the Services are alleged to infringe upon any United States patent, copyright, United States trademark, or other proprietary right of a third party; provided, however, that Contractor shall not be obligated to indemnify County, if such claim is caused by or arises out of (A) any intellectual property or materials provided by County; (B) any designs, or directions provided by County; (C) any software provided by an OEM or other third party; (D) County's use of the services or software other than in accordance with applicable documentation or instructions supplied by Contractor; (E) any combination, alteration, modification or revision of the services or software not expressly authorized in writing by Contractor; or (F) County's failure to use or implement corrections or enhancements to the services or software made available free of charge to County by Contractor; (ii) a violation by Contractor or its Affiliates of Federal, state, or other laws or regulations; (iii) work-related injury or death caused by Contractor or its affiliates, subcontractors or service providers, or any of their employees or agents, while performing activities in connection with this agreement; and (iv) tangible personal or real property damage caused by Contractor or its affiliates, subcontractors or service providers, or any of their employees or agents, while performing activities in connection with this agreement. Contractor shall be responsible for any costs and expenses incurred by County in connection with the enforcement of this Section, including, but not limited to, reasonable attorneys' fees. The Contractor's liability shall be subject to the limit of liability as stated in the services agreement between the parties.

The County agrees to the fullest extent permitted by law, to indemnify, defend, and hold harmless, the Contractor and its agents, officers and employees from and against any third party claim caused by any wrongful, intentional or negligent act or omission of the indemnifying party, or its agent(s) which may arise out of or are connected with the activities covered by this Agreement. The County's liability shall be limited by Wis. Stat. Section 893.80 for general liability.

The foregoing obligations are conditioned upon: (a) prompt written notice by the indemnified party to the indemnifying party of any claim, action or demand for which indemnity is claimed, provided however that the failure to give such notice shall not relieve the indemnifying party of its obligations hereunder except to the extent that such indemnifying party is materially prejudiced by such failure; (b) complete control of the defense and settlement thereof by the indemnifying party, provided that no settlement of an indemnified claim shall be made without the written consent of the indemnified party, which consent shall not be unreasonably withheld or delayed; and (c) reasonable cooperation by the indemnified party

in the defense as the indemnifying party may request. The indemnified party shall have the right to participate in the defense against the indemnified claims with counsel of its choice at its own expense.

Insurance:

Contractor shall purchase and maintain policies of insurance and proof of financial responsibility to cover costs as may arise from claims of tort, statutes, and benefits under Workers' Compensation laws, as respects damage to persons or property and third parties in such coverages and amounts as required and approved by the County Director of Risk Management and Insurance. Acceptable proof of such coverages shall be furnished to the Director of Risk Management and Insurance prior to services commenced under this professional service Contract.

It is understood and agreed that Contractor shall obtain information on the professional liability coverages of all sub-consultants and/or sub-contractors in the same form as specified above for review of the County.

Type of Coverage Minimum Limits

Statutory (Waiver of Subrogation for Workers Comp by Endorsement)

Employer's Liability \$100,000/\$500,000/\$100,000

Commercial Or Comprehensive General Liability

- General Aggregate \$1,000,000 Per Occurrence
- Bodily Injury & Property Damage \$1,000,000 Aggregate
- Personal Injury \$1,000,000 Per Person
- Contractual Liability \$1,000,000 Per Occurrence
- Fire Legal Liability \$50,000 Per Occurrence

Professional Liability

- Errors & Omissions \$1,000,000 Per Occurrence

Automobile Liability

- Bodily Injury & Property Damage \$1,000,000 Per Accident
- All Autos-Owned, non-owned
- Uninsured Motorists Per Wisconsin Requirements

Milwaukee County, as its interests may appear, shall be named as an additional insured for general, automobile, as respects the services provided in this Contract. Disclosure must be made of any non-

standard or restrictive additional insured endorsement, and any use of non-standard or restrictive additional insured endorsement will not be acceptable. Notice of cancellation, nonrenewal, or material change shall be afforded to the county in accordance with the provisions of the policies.

The insurance specified above shall be placed with at least an A-/VIII rated carrier per Best's Rating Guide approved to do business in the State of Wisconsin. Any deviations or waiver of required coverages or minimums shall be submitted in writing and approved by the County Director of Risk Management and Insurance as a condition of this Contract. Waivers may be granted when surplus lines and specialty carriers are used.

A Certificate of Insurance shall be submitted for review to the County for each successive period of coverage for the duration of this Contract.

Except for Worker's Compensation and Employers Liability, Milwaukee County shall be named as and Additional Insured in the general and automobile liability policies as its interests may appear as respects the services provided in this agreement. A waiver of subrogation shall be afforded to Milwaukee County on the Workers' Compensation policy. ~~A thirty (30) day written notice of cancellation or non-renewal shall be afforded to Milwaukee County~~ Notice of cancellation, nonrenewal, or material change shall be afforded to the county in accordance with the provisions of the policies.

The insurance specified above shall be placed with an A rated carrier per Best's Rating Guide approved to do business in the State of Wisconsin. Any deviations or waiver of required coverages or minimums shall be submitted in writing and approved by Milwaukee County's Risk Manager as a condition of this agreement.

A certificate of insurance shall be submitted for review to Milwaukee County for each successive period of coverage for the duration of this agreement.

Insurance and Indemnity Acknowledgement Form

The undersigned certifies and represents an understanding of Milwaukee County's Insurance and Indemnification requirements. The undersigned acknowledges that Milwaukee County is, in part, relying on the information contained in this proposal in order to evaluate and compare the response to the RFP.

Vendor: OneNeck IT Solutions LLC

Name Brian Osterhaus

Title District Sales Manager

Signature 

Date January 8, 2016

Exhibit 5 – Conflict of Interest Stipulation



8.5 Exhibit 5 – CONFLICT OF INTEREST STIPULATION

For purposes of determining any possible conflict of interest, all vendors submitting a proposal in response to this RFP must disclose if any Milwaukee County employee, agent or representative or an immediate family member is also an owner, corporate officer, employee, agent or representative of the business submitting the bid. This completed form must be submitted with the proposal. Furthermore, according to the Milwaukee County Code of Ethics, no person may offer to give to any County officer or employee or immediate family member, may solicit or receive anything of value pursuant to an understanding that such County representative's vote, official actions or judgment would be influenced thereby.

Please answer below either YES or NO to the question of whether any MC employee, agent or representative or immediate family member is involved with your company in any way:

YES _____

NO - We are not aware of any such relationship with a MC employee.

IF THE ANSWER TO THE QUESTION ABOVE IS YES, THEN IDENTIFY THE NAME OF THE INDIVIDUAL, THE POSITION WITH MC, AND THE RELATIONSHIP TO YOUR BUSINESS:

NAME _____

COUNTY POSITION

BUSINESS RELATIONSHIP

THE APPROPRIATE CORPORATE REPRESENTATIVE MUST SIGN AND DATE BELOW:

PRINTED NAME Brian Osterhaus

AUTHORIZED SIGNATURE 

TITLE District Sales Manager

DATE January 8, 2016

Exhibit 6 – Sworn Statement of Bidder

8.6 Exhibit 6 – SWORN STATEMENT OF BIDDER

I, being first duly sworn at Madison, WI,

City, State

On oath, depose and say I am the District Sales Manager

Official Title

Of the Bidder, OneNeck IT Solutions, LLC,

Name of Company

Do state the following: that I have fully and carefully examined the terms and conditions of this Request for Proposal, and prepared this submission directly and only from the RFP and including all accessory data. I attest to the facts that:

- I have reviewed the RFP, all related exhibits and attachments, questions and answers, addenda, and information provided through MC, in detail before submitting this proposal.
- I have indicated review, understanding and acceptance of the RFP (or relevant service component being bid upon). subject to the Exceptions provided in Bidder's Proposal
- I certify that all statements within this proposal are made on behalf of the Bidder identified above.
- I have full authority to make such statements and to submit this proposal as the duly recognized representative of the Bidder.
- I further stipulate that the said statements contained within this proposal are true and correct and this sworn statement is hereby made a part of the foregoing RFP response.



Signature

Office: 525 Junction Road, Madison, WI 53717

Legal Address

Subscribed and sworn to before me

This 6th day of January, 2016

Notary Public, Black Hawk County

State of Iowa

My commission expires March 3, 2018 - Commission #721136



Exhibit 7 – Cover Sheet for Technical Proposal



8.7 Exhibit 7 – Cover Sheet for Technical Proposal

In submitting and signing this proposal, we also certify that we have not, either directly or indirectly, entered into any agreement or participated in any collusion or otherwise taken any action in restraint of free trade or competition; that no attempt has been made to induce any other person or firm to submit or not to submit a proposal; that this proposal has been independently arrived at without collusion with any other vendor, competitor, or potential competitor; that this proposal has not knowingly been disclosed prior to the opening of the proposals to any other vendor or competitor; that the above statement is accurate under penalty of perjury.

In submitting and signing this proposal, we represent that we have thoroughly read and reviewed this Request for Proposal and are submitting this response in good faith. We understand the requirements of the program and have provided the required information listed within the Request for Proposal.

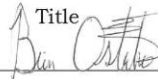
The undersigned certifies and represents that all data, pricing, representations, and other information of any sort or type, contained in this response, is true, complete, accurate, and correct. Further, the undersigned acknowledges that Milwaukee County is, in part, relying on the information contained in this proposal in order to evaluate and compare the responses to the RFP for Professional Services.

OneNeck IT Solutions LLC

Vendor's Name

Brian Osterhaus, District Sales Manager

Title



Signature

January 8, 2016

Date

Exhibit 8 – Cover sheet for Pricing Proposal



8.8 Exhibit 8 – Cover Sheet for Pricing Proposal

In submitting and signing this proposal, we also certify that we have not, either directly or indirectly, entered into any agreement or participated in any collusion or otherwise taken any action in restraint of free trade or competition; that no attempt has been made to induce any other person or firm to submit or not to submit a proposal; that this proposal has been independently arrived at without collusion with any other vendor, competitor, or potential competitor; that this proposal has not knowingly been disclosed prior to the opening of the proposals to any other vendor or competitor; that the above statement is accurate under penalty of perjury.

In submitting and signing this proposal, we represent that we have thoroughly read and reviewed this Request for Proposal and are submitting this response in good faith. We understand the requirements of the program and have provided the required information listed within the Request for Proposal.

The undersigned certifies and represents that all data, pricing, representations, and other information, of any sort or type, contained in this response, is true, complete, accurate, and correct. Further, the undersigned acknowledges that Milwaukee County is, in part, relying on the information contained in this proposal in order to evaluate and compare the response to the RFP for Professional Services.

OneNeck IT Solutions LLC

Vendor's Name

Brian Osterhaus, District Sales Manager

Title

Signature

January 8, 2016

Date

Exhibit 9 – EEOC Compliance



8.9 Exhibit 9 – EEOC Compliance

YEAR 2014 EQUAL EMPLOYMENT OPPORTUNITY CERTIFICATE FOR MILWAUKEE COUNTY CONTRACTS TO BE COMPLETED AND SIGNED BY ALL APPLICANTS

In accordance with Section 56.17 of the Milwaukee County General Ordinances and Title 41 of the Code of Federal Regulations, Chapter 60, SELLER or SUCCESSFUL PROPOSER or CONTRACTOR or LESSEE or (Other-specify), (Hence forth referred to as CONTRACTOR) certifies to Milwaukee County as to the following and agrees that the terms of this certificate are hereby incorporated by reference into any contract awarded.

Non-Discrimination

CONTRACTOR certifies that it will not discriminate against any employee or applicant for employment because of race, color, national origin, sex, age or handicap which includes but is not limited to the following: employment, upgrading, demotion or transfer, recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training including apprenticeship.

CONTRACTOR will post in conspicuous places, available to its employees, notices to be provided by the County setting forth the provision of the non-discriminatory clause.

A violation of this provision shall be sufficient cause for the County to terminate the contract without liability for the uncompleted portion or for any materials or services purchased or paid for by the contractor for use in completing the contract.

Affirmative Action Program

CONTRACTOR certifies that it will strive to implement the principles of equal employment opportunity through an effective affirmative action program, which shall have as its objective to increase the utilization of women, minorities, and handicapped persons and other protected groups, at all levels of employment in all divisions of the seller's work force, where these groups may have been previously under-utilized and under-represented.

CONTRACTOR also agrees that in the event of any dispute as to compliance with the foretasted requirements, it shall be his responsibility to show that he has met all such requirements.

Non-Segregated Facilities

CONTRACTOR certifies that it does not and will not maintain or provide for its employees any segregated facilities at any of its establishments, and that it does not permit its employees to perform their services at any location under its control, where segregated facilities are maintained.

Subcontractors

CONTRACTOR certifies that it has obtained or will obtain certifications regarding non-discrimination, affirmative action program and non-segregated facilities from proposed subcontractors that are directly related to any contracts with Milwaukee County, if any, prior to the award of any subcontracts, and that it will retain such certifications in its files.

Reporting Requirement

Where applicable, CONTRACTOR certifies that it will comply with all reporting requirements and procedures established in Title 41 Code of Federal Regulations, Chapter 60.

Affirmative Action Plan

Milwaukee County RFP for Data Center Operational Professional Services.docx

Page 41 of 44

© 2015 Excipio Consulting, LLC. All Rights Reserved. This document is PROPRIETARY and CONFIDENTIAL and may not be duplicated, redistributed, or displayed to any other party without the expressed written permission of Excipio.



CONTRACTOR certifies that, if it has 50 or more employees, it will develop and/or update and submit (within 120 days of contract award) an Affirmative Action Plan to: Audit Compliance Manager, Milwaukee County Department of Audit, 2711 West Wells Street, Milwaukee, WI 53208 [Telephone No.: (414) 278-4206]. CONTRACTOR certifies that, if it has 50 or more employees, it has filed or will develop and submit (within 120 days of contract award) for each of its establishments a written affirmative action plan. Current Affirmative Action plans, if required, must be filed with any of the following:

The Office of Federal Contract Compliance Programs or the State of Wisconsin, or the Milwaukee County Department of Audit, 2711 West Wells Street, Milwaukee, WI 53208 [Telephone No.: (414) 278-4206].

If a current plan, has been filed indicate where filed No plan currently on file - will meet and the year covered _____ obligation if awarded.

CONTRACTOR will also require its lower-tier subcontractors who have 50 or more employees to establish similar written affirmative action plans.

Employees

CONTRACTOR certifies that it has (No. of Employees) 1 employees in the Standard Metropolitan Statistical Area (Counties of Milwaukee, Waukesha, Ozaukee and Washington, Wisconsin) and (No. of Employees) 540 employees in total.

Compliance

CONTRACTOR certifies that it is not currently in receipt of any outstanding letters of deficiencies, show cause, probable cause, or other notification of noncompliance with EEOC regulations.

Executed this 8th day of January, 2016 by: Firm

Name OneNeck IT Solutions LLC

By Brian Osterhaus Address

525 Junction Road, Madison, WI 53717

(Signature)

OneNeck WI Employee Count	City	County
1	Delavan (WAH)	Walworth
10	Fitchburg	Dane
23	Madison	Dane
1	Oconomowoc (WAH)	Waukesha

Title District Sales Manager City/State/Zip Madison, WI 53717

Exhibit 10 – Certification Regarding Debarment and Suspension



8.10 Exhibit 10 – Certification Regarding Debarment and Suspension

The applicant certifies to the best of its knowledge and belief, that its' principals, owners, officers, shareholders, key employees, directors and member partners: (1) are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal department or agency; (2) have not within a three-year period preceding this proposal been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property; (3) are not presently indicted for or otherwise criminally charged by a governmental entity (Federal, State or local) with commission of any of the offenses enumerated in (2) of this certification; and, (4) have not within a three-year period preceding this proposal had one or more public transactions (Federal, State or local) terminated for cause or default.

Authorized Signature:  Date: January 8, 2016

Printed Name: Brian Osterhaus Title: District Sales Manager

Company: OneNeck IT Solutions LLC

Exhibit 11 – Proprietary Information Disclosure Form



8.11 Exhibit 11 – Proprietary Information Disclosure Form

The attached material submitted in response to the Request for Proposal includes proprietary and confidential information, which qualifies as a trade secret, as provided in s. 19.36(5), Wis. Stats. or is otherwise material that can be kept confidential under the Wisconsin Open Records Law. As such, we ask that certain pages, as indicated below, of this proposal response be treated as confidential material and not be released without our written approval.

Prices always become public information and therefore cannot be kept confidential.

Other information cannot be kept confidential unless it is a trade secret. Trade secret is defined in s. 134.90(1)(c). Wis. Stats. as follows: "Trade Secret" means information, including a formula, pattern, compilation, program, device, method, technique or process to which all of the following apply:


- The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.
- The information is the subject of efforts to maintain its secrecy that are reasonable under the circumstances.

We request that the following pages not be released:

Section	Page #	Topic
None		

IN THE EVENT THE DESIGNATION OF CONFIDENTIALITY OF THIS INFORMATION IS CHALLENGED, THE UNDERSIGNED HERBY AGREES TO PROVIDE LEGAL COUNSEL OR OTHER NECESSARY ASSISTANCE TO DEFEND THE DESIGNATION OF CONFIDENTIALITY AND AGREES TO HOLD MILWAUKEE COUNTY HARMLESS FOR ANY COSTS OR DAMAGES ARISING OUT OF MILWAUKEE COUNTY'S AGREEMENT TO WITHHOLD THE MATERIALS.

Failure to include this form in the Request for Proposal may mean that all information provided as part of the proposal response will be open to examination and copying. Milwaukee County considers other markings of confidential in the proposal document to be insufficient. The undersigned agrees to hold Milwaukee County harmless for any damages arising out of the release of any materials unless they are specifically identified above.

Company Name OneNeck IT Solutions LLC
 Authorized Representative (Signature) 
 Authorized Representative (Print) Brian Osterhaus, District Sales Manager
 Date January 8, 2016

Attachment 1 – OneNeck Legal Exceptions

EXCEPTIONS TO MILWAUKEE COUNTY REQUEST FOR PROPOSAL

The following modifications to Milwaukee County’s Request for Proposal for Data Center Operations Professional Services dated November 2015 (“Exceptions”) to the above stated Request for Proposals are incorporated fully in to the attached proposal from OneNeck IT Solutions LLC (“Vendor”). Any conflict between these Exceptions and the terms of the Request for Proposal shall be controlled by these Exceptions.

Section 8.4. Exhibit 4 – INSURANCE AND INDEMNITY ACKNOWLEDGMENT FORM shall be revised as stated in the attached Addendum A.

Section 8.6 Exhibit 6 – SWORN STATEMENT OF BIDDER shall be revised as stated in the attached Addendum B.

Section 7.1.4 CONTRACT TERMINATION shall be revised as follows:

Milwaukee County ~~in its sole discretion may shall~~, in the case of a termination for breach or default, allow the Contractor 30 days in which to cure a defect. In such case, the notice of termination will state the time period in which cure is permitted and other appropriate conditions. ~~Milwaukee County, by written notice, may terminate this contract, in whole or in part, when it is in the Government’s interest.~~ If this contract is terminated, Milwaukee County shall be liable only for payment under the payment provisions of this contract ~~for services rendered before the effective date of termination.~~

In the event the contractor terminates the contract, such termination will require written notice to that effect to be delivered by the contractor to the County not less than ninety (90) days prior to said termination and shall assist and provide for an orderly transition of services as provided in a statement or work and at Contractor’s then current hourly rates.

7.1.13 INFORMATION RELEASE

All materials submitted become the property of Milwaukee County. Any restriction on the use of data contained within a request must be clearly stated in the bid itself. Proprietary information submitted in response to a request will be handled in accordance with applicable Milwaukee County Ordinances, State of Wisconsin procurement regulations, and the Wisconsin public records law. Proprietary restrictions normally are not accepted. However, when accepted, it is the vendor’s responsibility to defend the determination in the event of an appeal or litigation. Data contained in a Request for Proposal, all documentation provided therein, and innovations developed as a ~~result~~defined deliverable of the contracted commodities or services cannot be copyrighted or patented. All data, documentation and innovations that are specified as deliverables in a written contract between Contractor and Milwaukee County become the property of Milwaukee County.

Milwaukee County may, at any time during the procurement process, request and/or require additional disclosures, acknowledgments, and/or warranties, relating to, without limitation, confidentiality, EEOC compliance, collusion, disbarment, and/or conflict of interest. Such additional terms or requirements shall only apply to Contractor if accepted by Contractor in writing.

Any materials submitted by the applicant in response to this Request for Proposal that the applicant considers confidential and proprietary information and which proposer believes qualifies as a trade secret, as provided in s. 19.36(5), Wis. Stats, or material which can be kept confidential under the Wisconsin public record law, must be identified on the Designation of Confidential and Proprietary Information form (Exhibit 11 – Proprietary Information Disclosure). Confidential information must be labeled as such. Costs (pricing) always becomes public information and therefore cannot be kept confidential. Any other requests for confidentiality MUST be justified in writing on the form provided and included in the bid submitted. Milwaukee County has the sole right to determine whether designations made by a proposer qualify as trade secrets under the Wisconsin public records law.

Section 7.1.15 LIMIT OF LIABILITY shall be added to any contract for services between the parties:

IN NO EVENT SHALL CONTRACTOR, ITS AFFILIATES, OR THEIR RESPECTIVE DIRECTORS, OFFICERS, AGENTS OR EMPLOYEES, BE LIABLE TO COUNTY OR ANY OTHER PARTY FOR ANY REASON, WHETHER IN CONTRACT OR IN TORT, FOR ANY DAMAGES ARISING OUT OF OR BASED UPON PERFORMANCE OF, OR DAMAGES CAUSED BY PRODUCTS (INCLUDING THOSE RELATED TO

CLAIMS OF INFRINGEMENT UPON A PROPRIETARY RIGHT OF A THIRD PARTY) RESOLD UNDER THIS AGREEMENT. FOR THE AVOIDANCE OF DOUBT, COUNTY ACKNOWLEDGES THAT ITS SOLE RECOURSE FOR ANY DAMAGES ARISING OUT OF OR BASED UPON PERFORMANCE OF, OR DAMAGES CAUSED BY PRODUCTS RESOLD UNDER THIS AGREEMENT SHALL BE AGAINST THE ORIGINAL EQUIPMENT MANUFACTURER OF THE APPLICABLE PRODUCT. IN NO EVENT SHALL CONTRACTOR, ITS AFFILIATES, OR THEIR RESPECTIVE DIRECTORS, OFFICERS, AGENTS OR EMPLOYEES, BE LIABLE TO COUNTY FOR ANY OTHER REASON, WHETHER IN CONTRACT OR IN TORT, FOR ANY DAMAGES ARISING OUT OF OR BASED UPON CONTRACTOR'S ACTS OR OMISSIONS RELATED TO THIS AGREEMENT IN AN AMOUNT EXCEEDING THE FEES PAID DURING THE PRECEDING TWELVE MONTHS BY COUNTY TO CONTRACTOR UNDER THE EXECUTED ORDER PURSUANT TO WHICH SUCH CLAIM AROSE REGARDLESS OF THE FORM IN WHICH ANY LEGAL OR EQUITABLE ACTION MAY BE BROUGHT.

Attachment 2 – Sample Colocation SLA and AUP



TERMS AND CONDITIONS



SERVICE DESCRIPTIONS

Upon execution of this Statement of Work ("SOW") by Kohl's Corporation ("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.



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.

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.
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.

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.



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.

Attachment 1 Colocation Acceptable Use Policy

1. Restrictions

1.1 Lawful Purposes. Client may use the Services only in compliance with all applicable laws and regulations, and shall not directly or indirectly use the Services for unlawful purposes or otherwise in violation of this Section 1. Client may not use the Services: (a) to disseminate or transmit bots, spiders, crawlers, or other repetitive information collection or distribution devices; (b) to create a false identity or otherwise attempt to mislead any party as to the identity of the sender or the origin of any communication, information or other material; (c) to attempt to discover, use, copy or modify the information or materials of others or in any way violate their privacy or security; or (d) to use Company's networks to access or monitor other computation, information or communication devices or resources of Company or any third party without that party's express written consent, including but not limited to, engaging in any unauthorized security probing activities or other attempts to evaluate Company's networks or host system.

1.2 Security. Client will comply with all Company security policies related to the Services, including, but not limited to, requirements set forth in any Service Order. Company will provide such security policies to Client in conjunction with the signed Service Order.

1.3 E-mail. Client shall comply with the CAN-SPAM Act of 2003, and shall not use the Services to engage in activities that are likely to cause IP addresses assigned to Client to become blocked or listed as likely sources of unsolicited bulk email (a/k/a *spam*) by anti-spam organizations such as SpamHaus (<http://www.spamhaus.org>) due to violations of the anti-spam organization's policy for acceptance of inbound email.

1.4 Client Data. Client will ensure that any materials and information transmitted through, or stored on, Client's servers or equipment located in Company's facilities, or derived from or in any way related to use of the Services ("Client Data"): (a) will not contain any illegal or otherwise inappropriate material, including material that is threatening, abusive, harassing, defamatory, libelous, fraudulent, obscene, invasive of another's privacy, violates or infringes the intellectual property or privacy rights of any person or entity; and (b) will not include or utilize any "Self-Help Code" or "Unauthorized Code" as defined in this section. "Self-Help Code" means any back door, time bomb, drop dead device, or other routine, algorithm, routine or code designed or used to: (i) disable, erase, alter or harm Company, its Clients, or any of their respective computer systems, programs, databases, data, hardware or communication systems, automatically with the passage of time, or under the control of, or through some affirmative action by, a person other than Company, or (ii) access any computer system, program, database, data, hardware or communication system of Company or its other Clients. "Unauthorized Code" means any virus, Trojan horse, worm, or other routines, code, algorithm or component designed or used to disable, erase, alter, or otherwise harm any computer system, program, database, data, hardware or communication system, or to consume, use, allocate or disrupt any computer resources, in a manner which is malicious or intended to damage or inconvenience.

1.5 Client Compliance. If Company reasonably believes that the Client has violated any of the restrictions set forth in this Section 1, and such violation may cause material harm or interference with Company's rights or property, or the rights or property of others, Company may

suspend the Services affected by Client's violation, provided, where practicable, Company will give Client ten (10) days written notice of a violation and an opportunity for Client to cure such violation within such 10-day window. Notwithstanding the foregoing, if Company reasonably determines that a suspension on shorter or contemporaneous notice is required to prevent damage to Company or its Clients, Company will provide Client prior written notice of any such suspension. Company shall restore suspended Services promptly upon Client's cure of any such violation of this Section 1.

2. Data Center Physical Access

- 2.1 Company reserves the right to exclude or expel from the data center any person who, in Company's sole judgment, is under the influence of alcohol or drugs or who, in Company's sole judgment, poses a risk to persons or property in a data center.
- 2.2 Company may, at its discretion, require any or all authorized persons of Client to have a full face photograph taken at the data center for purposes of secure identification.
- 2.3 All persons entering Company's data centers are classified under *unescorted*, *escorted*, or *visitor*. A valid government-issued photo ID is required for all persons entering a Company data center. Identification information for all persons is kept by Company to log data center access.
 - 2.3.1 Unescorted persons must sign a complete and correct security access request form prior to gaining access to Company facilities, authorized by the proper personnel, and they must follow facility rules as outlined herein.
 - 2.3.2 Escorted persons must be authorized by proper personnel and accompanied at all times by a person with unescorted access privileges. Escorted persons must be at minimum eighteen years of age.
 - 2.3.3 Visitors are accompanied at all times by a person with unescorted access. Individuals on tours are classified as *visitors*.

3. Vendor Access

- 3.1 Company's Vendor Access Policy (as described herein) is to establish the rules for vendor access to Company's data center. Vendors play an important role in the support of hardware and software management, and operations for clients. The Company Vendor Access Policy applies to all clients wishing to allow access to their equipment located in Company's data center for any vendor they currently use.
- 3.2 Any Client granting access to its equipment located in Company's data center to a vendor or subcontractor agrees to the following stipulations in full and without hesitation:
 - 3.2.1 Client accepts responsibility for all actions of the Client-approved vendor while he/she is in the Company data center, whether the ramifications are financial or otherwise.

- 3.2.2 Client agrees that Company shall be held harmless for any loss to Client data or equipment whether financial or otherwise, due to the actions of the Client-approved vendor.
 - 3.2.3 Client agrees that the Client-approved vendor shall be held to the same standards as the Company in regard to safety and security policies and procedures while they are in the data center. It is the responsibility of the Client to educate the vendor of the above-mentioned safety and security policies and procedures.
 - 3.2.4 Client agrees that it will be Client's responsibility to notify Company if and when a Client-approved vendor's access should be revoked. Notifications of this kind shall be made via the Company ticket system. Company reserves the right to take up to forty-eight (48) hours to process the vendor access removal request.
- 3.3 Client-approved vendor must provide a valid government issued identification in exchange for access to the data center.
- 3.4 For those vendors who have multiple representatives that could be dispatched to the Company data center to work on Client equipment, Client must select one of the following three ways of confirming the employment status of the individual accessing the data center:
- 3.4.1 Provide a list of vendor employees that are authorized to do work on the specified Client equipment.
 - 3.4.2 Provide a 24x7 phone number for a vendor representative which can be utilized by the Company security personnel to confirm that the vendor employee trying to gain access to the data center is authorized to do work on the specified Client equipment.
 - 3.4.3 Create a ticket that provides the vendor name and mentions this Company Vendor Access Policy within the ticket. Additionally, the vendor employee needing access will need to reference the ticket number at the time they are requesting access. Each ticket will provide access for up to twenty-four (24) hours from the time it is created.
 - 3.4.4 Using Company's Security Access Request Form(s), Client may designate (with appropriate signatures) one or more NAMED vendor employees as agents of the Client, and Company will issue access badges as if they were Client's employees.

4. Power, Cooling and Space Utilization

- 4.1 All installations or modifications to a Client's cabinets, private cage, or room, equipment and cross connects must be reviewed and pre-approved in writing by Company. Clients are allowed to deploy or redeploy equipment within an allocated cabinet only to the extent that power deployed to the cabinet can support such equipment.
- 4.2 Client shall submit to Company equipment power utilization information for review to ensure power and cooling delivery is adequate for each space. A review will be performed by Company during initial cabinet or cage planning, and for subsequent SOWs for additional power in an existing space.

- 4.3 Power utilization guidelines are hereby defined for each deployed circuit, whereby 80% utilization of a primary circuit (or 80% of the aggregate of a primary/redundant circuit pair) is considered within an acceptable limit for power delivery. Utilization is calculated based on observed ampere utilization, and represents Company's method for monitoring power delivery and utilization to Client. Client will be advised to review power consumption if Client is exceeding the 80% circuit utilization guideline. Company will notify Client to either A) normalize power consumption or B) notify Company that additional power is necessary to maintain acceptable power delivery levels per cabinet, row or cage.
- 4.4 Company will monitor power utilization and consult with Client in such cases where power consumption per cabinet, row or cage exceeds acceptable limits, or where modifications to Client's cabinet or cage utilization is recommended to ensure consistent power delivery.
- 4.5 Company requires Client to utilize a primary/redundant power delivery service within the data center, where available.
- 4.6 Company requires that Client fills all unused portions of a cabinet with blanking panels to assure that an adequate flow of cooling air passes through active components within that same cabinet, and to assure that energy costs to cool are not inappropriately higher than required.

5. Cable Trays and Cabling

- 5.1 Company cable trays are reserved for Company use only. These trays are typically the highest in a room or also under the floor in data centers with raised floors.
- 5.2 Clients with private cage or suite space may install Company approved cable trays within their space for their own exclusive use with prior approval of Company.
- 5.3 Clients with cross connect requirements between cabinets in shared space may submit SOWs with Company's service center and/or Company's account representative.
 - 5.3.1 Clients may place cables between adjacent and same row contiguous cabinets currently leased by the same Client by placing cables through cable openings located on the top of the cabinet without an Executed Order.
- 5.4 Service orders for cross connects between Client spaces and authorized ISP/carrier demarcation points must be ordered from Company's service center and/or Company account representative.

6. Network

- 6.1 Company shall have final design approval on any network installations and integrations which interface directly with the Company's network.

- 6.2 Clients may directly connect, or peer, with any Company-approved carrier or other Client within the data center. Clients and carriers must submit their Executed Orders for cross-connects to Company for these connections.

7. Data Center Tours

- 7.1 Tours must be scheduled no later than 5:00 p.m. on the business day before the requested tour. The following data must be provided
- 7.1.1 visitor's organization name
 - 7.1.2 purpose of tour
 - 7.1.3 date/time of tour
 - 7.1.4 names of visitors
 - 7.1.5 special requests associated with the tour
- 7.2 Company may reject or require rescheduling of a tour at its discretion should the requested tour time conflict with any maintenance, safety, or other operational issue.
- 7.3 Tour size is limited to a maximum of five guests and one (or more) authorized tour guide(s) on all tours unless Company agrees to accommodate more guests.
- 7.4 Any tour requesting access to restricted areas in the data center must obtain special clearance from Company. A Company representative must obtain prior tour approval for restricted Client or stakeholder areas. Tours in these rooms require that a Company employee and tour guide are present with no more than 5 guests in the area at once per guide.
- 7.5 Client personnel with "unescorted" privileges are responsible for the registration of tour visitors and ensuring that visitors comply with posted policies and procedures.
- 7.6 Company reserves the right to exclude any area of a data center from tours at any time without advanced notice.
- 7.7 Unescorted personnel access privileges will be revoked either due to notification from authorized personnel with Client for any reason or by Company due to non-compliance.
- 7.8 Restricted Areas
- 7.8.1 Access by all non-Company personnel is prohibited to the telecommunications areas, power rooms and other critical areas defined by Company. If access is required to such areas by non-Company personnel, they must be escorted by a Company employee with "unescorted" privileges.
 - 7.8.2 Access by all non-Company personnel is prohibited to the shipping/receiving area. If access is required to this area by non-Company personnel, they must be escorted by a Company employee with "unescorted" privileges. At his or her

discretion, the facility manager may assign "unescorted" privileges for this area to non-Company personnel on a case by case basis.

7.8.3 Escorted access in non-emergency situations to telecommunications areas, power rooms and other critical areas defined by Company for non-Company personnel may be requested under the following criteria:

7.8.3.1 The request for access must be submitted a minimum of 5 business days before access is needed.

7.8.3.2 Company may reject or require rescheduling of an access request at its discretion should the requested date and time conflict with any maintenance, safety, or other operational issue.

8. Client Guidelines

8.1 Client will

- 8.1.1 ensure that when entering the data center they do not allow other, non-authorized individuals to enter secure areas with them.
- 8.1.2 follow security measures that do not allow for others to enter the data center by holding open a door or allowing a door to be held open.
- 8.1.3 notify Company of the addition or removal of personnel allowed to access the data center on behalf of Client.
- 8.1.4 notify Company of vendor visitors to the data center to authorize access to their respective cabinet(s), cage or suite a minimum of 5 business days prior to the visit if a Company escort is needed.
- 8.1.5 ensure registration of tour guests, and Client is solely responsible for ensuring that all guests comply with Company policies.
- 8.1.6 immediately notify Company of all risk and security concerns and security breaches of Client, vendor or Company equipment or Company's facility.
- 8.1.7 immediately notify Company of all damage to Client, vendor, or Company equipment or Company's facility.
- 8.1.8 deposit unwanted materials in designated trash receptacles or in appropriate locations outside Company's facility.
- 8.1.9 be responsible for security within their cabinet(s), cage or suite. Company will lock all un-attended cabinets if found un-secured and notify Client.
- 8.1.10 maintain their cabinet(s) in an orderly and clean manner.
- 8.1.11 dual cord all equipment to primary and redundant power circuits.
- 8.1.12 ensure all equipment and cabling is located inside of the cabinet(s) only and not in aisles or other areas of Company's facility.
- 8.1.13 follow all posted guidelines and rules.
- 8.1.14 maintain all equipment colocated at Company. Such maintenance is the sole responsibility of Client. All equipment colocated at Company must be within weight, size and power limitations established by Company. All such equipment, furnishings and supplies also must meet all applicable codes and zoning ordinances.

8.2 Client will not

- 8.2.1 attempt to gain or allow fraudulent access to Company's data center or any Company equipment.
- 8.2.2 bring materials, devices, or products that are explosive, volatile, compressed, poisonous, radioactive, caustic, corrosive, irritant, oxidant, create electromagnetic interference, sparks, or cause any other danger to others or equipment within Company's data center areas unless approved in advance by Company's change advisory board.
- 8.2.3 alter, tamper with, interfere with, breach the security of, adjust, or repair any equipment or property not belonging to Client.
- 8.2.4 store flammable materials in their cabinets, or in the data room (e.g. cardboard).
- 8.2.5 leave litter, cartons, packaging or other unnecessary items in or around Company's facility.
- 8.2.6 eat, drink, or use tobacco products within the data center.
- 8.2.7 take pictures or recordings without prior permission from Company.
- 8.2.8 block any exit route or aisle way or create a fire hazard.
- 8.2.9 impair or block the minimum setback distances (required by prevailing laws and codes) for electrical distribution and high voltage power cabinets.

8.3 Client must notify Company if they

- 8.3.1 will be conducting a tour.
- 8.3.2 require the use of Company's conference room.
- 8.3.3 require Company to provide an escort inside Company's data center.
- 8.3.4 require photos or videos within Company's data center.
- 8.3.5 require the addition or removal of personnel authorized to access the Company data center on behalf of Client.

9. Enforcement

- 9.1 Violation of this policy may result in suspended or revoked unescorted access to Company's data center, voiding of Company's Service Level Agreement obligations, or an alternate action deemed appropriate by Company and within the terms and conditions of the Master Services Agreement.
- 9.2 Company employs measures to safe guard data center doors from being held or propped open. Client agrees not to hold open or prop open a door. Any door that is held or propped open for a period of time will signal an alarm and initiate an investigation of the cause. Client personnel who are found to have held or propped doors open will be removed from the site, and further access denied. Clients responsible for holding or propping doors open, may, at the discretion of Company, have their contract terminated.

10. Shipping/Delivery

- 10.1 Company facility personnel will accept delivery of and store Client's equipment in accordance with the guidelines set forth below. Due to limited storage space, Company, at its sole discretion, has the right to deny or limit the amount of storage space and storage time to Clients.
- 10.2 Delivery Scheduling
- 10.2.1 Due to building requirements, all Client deliveries must be scheduled in advance with Company's Network Operations Center (NOC). Client shall notify the Company NOC of the scheduled delivery date and if any of the items will require the use of the freight elevator. In the event a loading dock is required for the delivery of the equipment, Client shall be responsible for any applicable charges imposed by the landlord or building manager, if any. If Company has not been notified of equipment arrival, Company will deny acceptance of shipment.
- 10.2.2 Shipments will only be accepted between the hours of 8:00 A.M. to 5:00 P.M. Monday through Friday, unless other arrangements have been made between the Client and Company's NOC.
- 10.3 Return of Client Equipment - Clients wishing to receive equipment shipped back to them must include a prepaid shipping label, including the cost of pickup, and Company will return the item in the packaging it was originally sent in. Alternatively, Clients may arrange for a courier to pick up their equipment at their own expense. Professional service charges may apply.
- 10.4 Third Party Equipment Delivery - If the equipment is delivered by a third party, Company facility personnel will receive it on behalf of Client, provided that Client pre-scheduled the delivery with Company's NOC. If any such delivery to Company has not been so scheduled, Company will not accept delivery of the shipment.
- 10.5 Include the following packing and shipping information:
Client Name
c/o Company
Data Center Address
Special Instructions
- 10.6 Client shall prepay all shipments, freight, packages, etc. Company will not accept shipments that require any payment, whatsoever. Client is responsible for all shipping and/or freight claims.
- 10.7 Large shipments that require specialized handling to enter Company's data center are the responsibility of the Client to contract special handling or have a Client representative(s) onsite to bring the equipment into the data center from the building loading dock.
- 10.8 Upon receipt of Client's equipment, Company will make commercially reasonable efforts to do the following:

- 10.8.1 Verify that the shipment is for the correct colocation facility.
 - 10.8.2 Place the equipment in a secured area until Client's space is ready or available.
 - 10.8.3 Notify Client via email of receipt of all shipments or shortages, if any.
- 10.9 Company facility personnel will not open or verify the contents of any shipment; nor will they be responsible for any equipment difficulties due to shipping or other actions. While Company facility personnel will not inspect each package for damage, in the event of extremely obvious damaged external packaging, Company will accept the package and indicate, "**damaged shipment/freight**" on the shipping receipt and request the delivery driver to countersign acknowledging delivery of "damaged shipment/freight." In the event of any other discrepancy identified by delivery personnel, Company will accept the shipment and indicate "**short shipment/freight**" on the shipping receipt and request the delivery driver to countersign acknowledging delivery of "short shipment/freight."
- 10.10 To the extent that the Client equipment is received by Company and Client does not pick it up the same day, Company will temporarily store Client's equipment in a secure storage area if there is space to do so at the discretion of the Company facility personnel and the Company NOC. To the extent that the Client fails to place or install their equipment in the services area designated by Company when available, Client will have ten (10) business days from the date that the equipment was first delivered in which to collect its equipment from the Company temporary storage area, after which Company shall charge Client a storage fee of \$10 per cubic foot per day, with a one cubic foot minimum. All equipment left in a Company storage area for more than forty-five (45) days will be shipped to the Client's billing address, unless an alternative address has been identified, at Client's sole cost and expense.

Company is not responsible for loss or damage to Client equipment occurring in route to the Company data center, stored in Company facilities or in transit if returned to Client.

11. Safety

- 11.1 Client will follow all safety and emergency exit procedures posted in Company's data center.
- 11.2 First aid kits are located at designated locations in the facility. All injuries should be reported to a Company employee.
- 11.3 In the event of an emergency situation (e.g., fire, building evacuation, medical emergency, etc.), or drill, Clients present at Company's data center will be required to follow instructions given by on-site Company employees. Clients must leave the data center if an alarm is triggered.

Milwaukee County Addendum 3 – Disadvantaged Business Enterprise Utilization

The award of this contract is conditioned upon your good faith efforts in achieving this project’s proposed Disadvantaged Business Enterprise (DBE) goal of 17%, and you must document those efforts. Your Proposal must state how you will meet the goal, including identifying the DBE firm(s) by name, the scope(s) of work/service(s) to be provided, the dollar amount(s) of such work, and the percentage of the DBE goal to be met. Failure to document the utilization will result in a determination of non-responsiveness, and rejection of your Proposal may occur.

A necessary step in the good faith efforts process is contacting Community Business Development Partners (CBDP) at 414-278-4747 or <mailto:cbdp@milwaukeecountywi.gov> for assistance in identifying DBEs and understanding the County’s DBE Program procedures. The official directory of eligible DBE firms can be accessed by the following link:

<https://app.mylcm.com/wisdot/Reports/WisDotUCPDirectory.aspx>

Although the Milwaukee County RFP was released November 18 we were sent this new Addendum 3 on December 30th at 8:21pm with a due date of January 8th. For this initial response we have aligned out partnerships for this response with companies that we have done business with and feel confident will add value to our solution. We are certainly willing to utilize a DBE as long as they add value to the solution for Milwaukee County. TDS Telecommunications Corp. is headquartered in Madison, WI and is well known for their community efforts. Given some time to vet some of the DBE’s listed on the web site, we will certainly make every effort to include a DBE approved company.