OneNeck IT Solutions LLC (“Company”) - Acceptable Use Policy

1. Restrictions

1.1 Lawful Purpose
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 four 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:

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

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 Facilities Command Center (FCC). Client shall notify the Company FCC 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 FCC.

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 FCC. 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 FCC. 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.