Key Issues in Cloud Contracts

Presented By:
Kemal Hawa and Emily Naughton of Greenberg Traurig, LLP and Amber Lester of CyrusOne, Inc.

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

PART I

CLOUD SERVICES 101

CLOUD PROCUREMENT

- Cloud technology is central to most business operations today
- Cloud contracts are first and foremost about procuring performance at specified levels
  - Of course, the standard legal protections are also addressed
- To ensure performance, one must have a basic understanding of Cloud technology
  - Different types of agreements can be used depending on the services provided
  - Pricing, performance metrics and remedies for failure to meet performance standards vary depending on the services provided and the customer's business needs

CLOUD-BASED SERVICES

- IaaS (Infrastructure as a Service)
  - Storage and retrieval, disaster recovery, virtual equipment, firewalls, etc.
- SaaS (Software as a Service)
  - Delivery of software centrally hosted on the Cloud, *e.g.*, O365, Salesforce, security software
- PaaS (Platform as a Service)
  - Provision of networks, servers, storage, applications, and other services that are required to support or host the user's application
  - The user creates customized software using the Cloud platform

TYPES OF CLOUD OFFERINGS

- Public Cloud
  - Involves shared servers owned and operated by a third party
  - Primary benefits are scalability and the ability to pay only for servers utilized
- Private Cloud
  - Involves dedicated servers typically housed in a data center, but can also be hosted on premises
  - Primary benefits are control, customization and security
- Hybrid Cloud
  - Simply a combination of the features of public and private Cloud, *e.g.*, the utilization of public Cloud for non-sensitive applications, and private Cloud for mission critical and sensitive items

PART II

AN OVERVIEW OF CLOUD INFRASTRUCTURE

WHAT IS THE CLOUD?

- The “Cloud” consists of a physical network of data centers, equipment, fiber optic cable infrastructure, and submarine cable systems, interconnected globally

- Data centers are the heart of the Cloud
  - Data centers are secure buildings containing racks/cabinets of servers for data storage
  - Data centers can be large hub sites, or can be smaller edge sites located closer to the end user

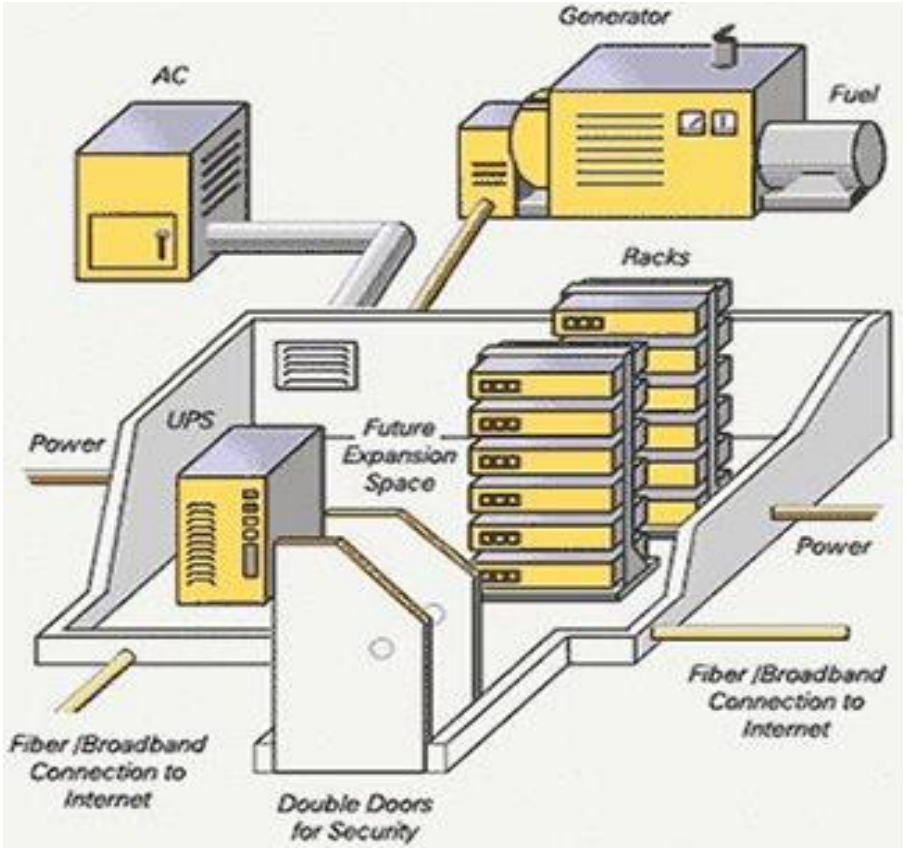
- Data centers are connected by telecommunications and broadband networks

DATA CENTERS

- Power is central to a data center's operations and its pricing
  - Uninterruptible power supply (UPS) and power redundancy
  - Back-up power/generators to minimize outages
  - Massive cooling capability
- As more mission critical data is stored in data centers, redundancy is critical
  - "N" refers to a non-redundant data center (i.e. no additional infrastructure to supply power in the event of a single failure)
  - "N + 1" refers to a facility that has additional power supply to ensure that essential facilities remain operational in the event of a single failure
  - "2N" refers to a fully redundant facility

DATA CENTER

DATA CENTER INFRASTRUCTURE



BASIC NETWORK ARCHITECTURE

- Last-mile transport facilities connect end users to edge sites
  - These facilities can be dedicated or common
- Backhaul facilities connect edge sites to the core of the network (data centers)
  - Edge sites are typically connected to data centers via high-capacity transport facilities
    - These connections may be direct, or there may be intermediate connections with other colocation sites
- Backhaul facilities also connect data centers to submarine cable landing stations
- Submarine cables connect countries and continents

THE EDGE

- Edge sites are located closer to the end user and serve as traffic aggregation points
  - Edge sites are selected based on availability of high-density connections, the number of providers interconnected at the edge site, and space and power availability, among other factors
    - The proliferation of big data analytics, the Internet of Things and artificial intelligence are changing network architectures, resulting in smaller data centers being built closer to the edge of the network
- In locations where it is not economic to deploy a data center or edge site, caching nodes are often used
  - Caching node servers reduce reliance on backhaul and increase network efficiency

PART III

CLOUD CONTRACTS AND PROCUREMENT

DATA CENTER CAPACITY PROCUREMENT

- End users enter into data center leases, licenses, and services agreements directly with data center operators
  - For space and power (retail colocation)
  - For managed services (essentially retail colocation plus managed services)
- End users procure data center capacity from Cloud providers (such as Microsoft, AWS, and Google)
- End users enter into agreements with OTTs (over-the-top) providers (such as Netflix, Hulu, Apple TV/iTunes) to procure services such as streaming video and other content
  - OTTs, in turn, lease capacity from data center operators
  - Many OTTs partner with Cloud providers; many Cloud providers are OTTs

NETWORK PROCUREMENT: DEDICATED ACCESS CONTRACTS

- End users, particularly large enterprise customers, often purchase dedicated access to connect their premises to a data center, edge location, etc.
  - Historically, a private line purchased from a telecommunications carrier
  - Can be purchased on a tariffed or commercial basis
- Internet service providers, content providers and OTTs are now offering access bundled with other services

NETWORK PROCUREMENT: FIBER CONTRACTS

- Dark Fiber is unused fiber laid by carriers or fiber providers
  - Carriers may only light a portion of the fiber for their own use, and the rest remains unused or “dark”
  - Dark fiber is purchased on high capacity routes (between data centers)
  - Dark fiber typically conveyed as an indefeasible right of use or “IRU”
    - Many of the benefits of ownership, without passing legal title
- Lit Fiber is fiber laid by carriers or fiber providers that has been activated
  - Unlike dark fiber, these are common facilities, shared by multiple content providers, carriers and end users
  - Carrier provides end-to-end service on lit fiber

PEERING AND INTERNET EXCHANGES

- The Internet is a collection of separate and distinct networks
  - No individual network provider touches even a fraction of all routes/end points
- Peering arrangements are agreements between providers for the exchange of on-net internet traffic
  - Settlements-free (no payments)
- IP Transit arrangements (involve payment)
- Internet exchanges
  - Typically carrier-neutral sites that allow providers to exchange Internet traffic with multiple other providers

CONTENT DELIVERY NETWORK SERVICES CONTRACTS

- CDN is used to distribute content to edge servers close to the end user
- CDN operates by utilizing a system of mapping and caching
  - Increases network efficiency and speed
- Content providers are building their own CDNs
- Few CDN providers offer CDN as a stand alone business model

SUBMARINE CABLE SYSTEMS

- High-capacity fiber optic cables that lie on the ocean floor, connecting continents and countries
  - The majority of global Internet traffic traverses submarine cables
- Three primary contracting schemes:
  - Consortium cable systems
    - A group of carriers and content providers join together to construct a new cable system in which they have a joint ownership interest
  - Investments in private cable systems
    - A provider buys substantial capacity in a private system as an anchor tenant
  - Rights of use on subsea systems
    - IRUs in or leases of submarine cable capacity on new and existing systems

PART IV

KEY LEGAL ISSUES IN CLOUD CONTRACTS

QUESTIONS TO CONSIDER BEFORE NEGOTIATING A CLOUD CONTRACT

- What goods and services are being provided?
- How will the goods and services be used?
- How critical are the goods and services to your business?
- What data is implicated?
  - Data Security and Compliance
  - Data Loss Tolerance
- Are there any downstream considerations or contingencies?
  - Internal Use Only
  - Integration into an External Product or Service
- Who is the Provider?
  - A well written contract is no substitute for adequate diligence

WHOLESALE AND RETAIL DATA CENTER CONTRACTS

- Data center contracts are priced based on power (in kilowatts)
  - Retail customers generally pay for power on a per-circuit basis, irrespective of utilization
  - Wholesale customers typically have separately metered power
- Service level agreements (SLAs) are most critical
  - Power, temperature, humidity and security are most common
- The line between wholesale and retail is blurring, with end users requiring many things wholesale purchasers require
  - Specific levels of network connectivity
  - Redundancy
  - On-site support

DATA CENTER LEASES AND SERVICES AGREEMENTS

- Cost and Timing
  - Early access for installation and testing
  - Energy/Power costs (PUE factor)
  - CPI adjustments
- Billing
  - Timely billing; time bar for billing errors/unbilled amounts
- Reporting
  - Regular reports on maintenance and service level compliance
- Audit rights
  - Right to audit invoices and test facilities and systems to ensure compliance and accuracy

DATA CENTER LEASES AND SERVICES AGREEMENTS (CONT.)

- Connectivity
  - Interconnection rights
  - Cross-connects
- Expansion options, such as rights of first refusal/offer or reservations of space and electrical capacity
- Renewal rights
  - It is difficult and costly to relocate once deployed
  - Strong renewal and expansion rights should be negotiated to control future costs and price increases
- Transition services
- Early termination rights

DATA CENTER LEASES AND SERVICES AGREEMENTS (CONT.)

- Personnel requirements
  - Limitations on subcontractors, *e.g.*, consent requirements, background checks, union issues
- Non-disturbance
  - Master landlord/owner or mortgagees will not remove the operator or the tenant/content provider in the event of default
- Liability for damage
  - Owner/operator liability for damage caused to tenant/content provider's equipment
  - Insurance requirements for customer and provider
- Assignment or sale by operator
  - Restrictions on operator's ability to assign a services agreement or lease to an unqualified operator
- Assignment and sublease rights of tenant/customer

DATA CENTER SALE LEASEBACKS

- Large enterprise customers with cumbersome IT infrastructure footprints are increasingly selling their data centers to data center operators and leasing back space within those data centers

- Key benefits to seller:
  - Seller can remain in the data center and continue its operations without interruption
  - Opportunity for seller to gradually reduce its footprint at the property
  - Allows seller to pass operational responsibility for the data center to a buyer that is in the business of operating data centers
  - Access to cash from the sale of the property, which can then be used to improve seller's balance sheet or invest in new business

- Key benefit to buyer:
  - Acquires an asset that has a long-term lease with steady revenue

RETAIL CLOUD CONTRACTS

- Many of the same legal issues that apply to data center leases and services agreements also apply to retail Cloud contracts
- Intellectual property issues are often more prevalent
- Scope of license grant relevant
  - Is license perpetual, exclusive, terminable, transferable?
- IP non-assert clauses may be embedded in contract
  - This is a provision stating that customer will not assert any IP infringement claim against a service provider globally with respect to any services at issue

RETAIL CLOUD CONTRACTS (CONT.)

- In addition to their own use, enterprise customers utilize Cloud/data center capacity in the provision of services to their own customers
  - SLAs given to such customers must be reconciled with SLAs received from the Cloud provider/data center operator
- Resale restrictions
  - Customers often intend to utilize Cloud services as an integral part of their own service offerings, and if so the agreement must allow such use
  - Ability of customer to utilize data center operators and outsource rights to third parties
- Take-or-pay provisions/minimum spend commitments

RETAIL CLOUD CONTRACTS (CONT.)

- Enrollment agreements
  - Initial agreements establishing relationship between the parties sometimes supersede other contracts (e.g. vendor policies)
- Acceptable use policies
  - Providers typically reserve the right to unilaterally modify
  - Changes may be inconsistent with an customer's standard operations, and thus customer may unknowingly be in breach
- Reporting requirements
  - Customers may have to keep certain records and report usage on a monthly and quarterly basis
  - Compliance audit rights

RETAIL CLOUD CONTRACTS (CONT.)

- Privacy/data security
  - Financial services and health care industries have specific requirements
  - Certifications
    - SOC (Service Organizational Control) regarding internal controls over financial reporting
      - SSAE (Statement on Standards for Attestation Engagements)
    - ISO (International Standards Organization) for security
    - HIPAA for health care compliance
    - PCI (Payment Card Industry) security standards for credit card processing
- Liability for data breaches - allocation of risk between Cloud/data center provider and enterprise customer
  - Indemnification: typically limited to Cloud/data center provider breach of security obligations
  - Limitations on liability: damage caps vary depending upon customer leverage

RETAIL CLOUD CONTRACTS (CONT.)

- Data protection
  - Cloud/data center provider compliance with data protection laws
- Data sovereignty
  - Geographic limitations on the storage and transmission of data
- Law enforcement disclosure obligations
  - Whether a subpoena is required and whether end users have a right to protest disclosure
- Regulator access to vendor personnel and data center facilities, *e.g.*, in financial services, insurance and health care industries
- Disaster recovery
  - Processes and charges for back-up and recovery of mission critical applications

NETWORK AGREEMENTS

- Price protection for large investments
  - Bankruptcy protection for IRUs
  - Separation of IRU and O&M (operation and maintenance) agreements into executory and non-executory contracts
- Continuity of service
  - Step-in rights in case of default by carrier
  - Non-disturbance in case of foreclosure by lender
- Service levels
  - Delivery and availability SLAs
  - Termination in case of chronic failure

NETWORK AGREEMENTS (CONT.)

- Network planning flexibility
  - Early termination options
  - Swaps and exchanges
  - Portability
- Off-net risks
  - Terms and SLAs vary for off-net portions of network
- Anti-monitoring
  - Prohibitions on access to content by carrier and third parties, except in case of government warrants and subpoenas
  - Carrier to provide notice of access and opportunity to object

EQUIPMENT PROCUREMENT CONTRACTS

- Access to Equipment (located in a data center)
  - Routine access for maintenance
  - Access/removal rights for lien holder in the event of default (if financed)
  - Data center operator should not have a lien over equipment
- Assignment/Change of Control
  - Many equipment contracts restrict assignment/COC
  - There are often significant hidden fees associated with transfer of intellectual property underlying equipment's operation
- Compatibility with law enforcement standards
  - CALEA (Communications Assistance for Law Enforcement Act)
- Warranties
- Specifications

PRIVACY AND DATA SECURITY

- Compliance and allocation of risk associated with privacy and data security breaches is a critical issue
- The new European GDPR regime stringently regulates a company's ability to transfer data between countries
  - The penalties for non-compliance are severe
- Numerous other countries – most notably China - have even stricter rules
- Virtually every Cloud contract contains specific provisions governing liability for privacy and data security breaches and non-compliance with applicable privacy and data security laws
- Increasingly, purchasers of Cloud services are insisting on contractual protections addressing privacy and data security
  - Special indemnities for breaches
  - Termination rights for chronic breaches

PART V

CLOUD CONTRACT CHECKLIST

CLOUD CONTRACT CHECKLIST

- What goods and services are being provided?
  - What applications/programs are being purchased or supported? Is training or ongoing support needed? Will the services be dedicated or shared?
    - Hardware component (buying or leasing hardware)
    - Software component (licensing of software)
    - Service component (engineering, installation, on-going support, maintenance, etc.)
- Where will the services be provided?
  - Will services be provided at multiple sites under a single contract?
  - Have there been issues relating to security or availability of services (including network connections) at the site?

CLOUD CONTRACT CHECKLIST (CONT.)

- Who is providing the services?
  - Will any part of the service be provided by any subcontractors or any affiliates? If so, what services will be provided and where are such subcontractors and affiliates located?
  - Are employees/ contractors entering the data center or otherwise accessing critical equipment required to sign confidentiality agreements? Are they subject to background checks?
  - Is there a mandatory training and awareness program in place for employees to make them aware of the company's security policies, standards and security practices?

CLOUD CONTRACT CHECKLIST (CONT.)

- What are the performance standards for the service?
  - What service levels are provided?
  - What are the customer's remedies in the event of a service level failure?
    - When are credits provided and in what amounts?
    - Will customer have a right to terminate in the event of repeated service level failures?

CLOUD CONTRACT CHECKLIST (CONT.)

- What data is implicated?
  - What data will be stored or generated (flag sensitive or confidential information)?
  - Will the vendor have logical or physical access to data?
    - If the provider will have access to data, does it have a documented information security program? If so, what security precautions and plans are in place to ensure confidentiality, integrity and availability of customer's network, hardware, informational assets, and confidential data?
  - Does the service include data back-up? What is the business impact if all data is lost?
  - Who owns the data? Is there any customization or development anticipated?

CLOUD CONTRACT CHECKLIST (CONT.)

- How critical is the service to the customer's business?
  - What is the impact to the customer's business if the service is unavailable for a period of time?
  - What is the work around if the service is unavailable?
  - Does the service/product include any disaster recovery component?
    - If so, what is the process for risk identification/mitigation, what are the recovery time objectives and what are the applications that will support the services?

CLOUD CONTRACT CHECKLIST (CONT.)

- What compliance obligations does the provider have?
  - What certifications will the provider have received for any national or international security or quality standards (e.g. ISO 27001, SOC2, SSAE, ITIL, etc.)?
  - What is the scope and frequency of permissible customer audits? What is the cost associated with such audits and who will bear the cost?

APPENDIX

SAMPLE PROVISIONS

SERVICE LEVEL AGREEMENT (POWER)

Section 1. Service Levels and Service Credits. In the event Supplier fails to achieve a Service Level set forth below in any given calendar month during the applicable Service Term (but in all cases subject to the exclusions set forth in **Section 2 (Exclusions)** below), Customer may claim the Service Credit corresponding to the applicable failure (as set forth in the table below) by providing Supplier with a written request for such Service Credit within thirty (30) days after receipt of an invoice from Supplier for the period in which the Service Level was not achieved. Supplier's records and data shall be the basis for all Service Level calculations and determinations. Service Credits are Customer's sole and exclusive remedy and Supplier's sole and exclusive liability under the Agreement with respect to any deficiencies, interruptions or failures with respect to the Services. Service Credits shall not have any cash value at the end of the Service Term or otherwise. Unless otherwise stated in the table below, Service Credits are calculated based on the total MRC paid by Customer that is (a) attributed to use of the Colocation Space with respect to which the Service Level failure occurred and (b) the calendar month in which such Service Level failure occurred ("**SLA Credit Baseline**"). Notwithstanding anything to the contrary, the maximum amount of Service Credits in any calendar month under the SLA shall not exceed fifteen percent (15%) of the SLA Credit Baseline. If Customer is in multiple Colocation Spaces, Service Credits are calculated on a space-by-space basis such that a Service Credit shall be given only for a failure in the particular Colocation Space that is the subject of the Service Level failure. For any multiple Service Level event with the same root cause, only the Service Level with the highest Service Credit available shall apply (*i.e.*, multiple Service Credits for the same event will not be given).

Section 2. Exclusions. For purposes of determining the percentage of availability, stability or other measure for any Service Level under this SLA, the following causes will be excluded from the calculation (*e.g.*, if unavailability or instability are due to any of the causes listed below, such unavailable or unstable time shall be included as "available" or "stable" for purposes of calculating the percentage of availability or stability):

(a) Customer not utilizing or implementing the redundancy components of the infrastructure provided by Supplier including without limitation Customer's failure to purchase or properly utilize an "A" and "B" power whip to the Power Demarc;

(b) scheduled maintenance during a maintenance window communicated to Customer;

(c) acts or omissions of Customer or its employees, agents, customers, contractors, representatives, or a third party acting at the direction of Customer;

(d) Supplier following or implementing instructions or procedures issued by Customer;

(e) a Force Majeure Event; and

(f) any other exclusions set forth in the Agreement.

SERVICE LEVEL AGREEMENT (POWER) (CONT.)

Service Level	Description	Percentage	Service Credit
Power Availability	The power availability SLA shall become effective only once Customer has purchased and is properly utilizing an "A" and "B" power whip to the Power Demarc. The "Power Demarc" is the receptacle at the end of the power whip attached to each Customer power distribution unit or power strip. Supplier will provide power to the Power Demarc ("Power Availability"). Power shall be deemed unavailable if the electricity feeds in both power whips "A" and "B" fail simultaneously, for any amount of time, on the Supplier side of the Power Demarc. Power Availability shall be provided by Supplier to Customer at 100% uptime per month ("Power Availability Service Level"). For purposes of determining whether the Power Availability Service Level has been achieved, the percentage of availability shall be calculated each month during the Service Term as follows: (Total minutes of Power Availability per month) / (Total minutes per month). Customer shall be entitled to a Service Credit as set forth in this Section in the event the Power Availability Service Level is not achieved. The Service Credit is expressed as a percentage of Customer's MRC in a Colocation Space for the month in which the Power Availability Service Level is not achieved.	100%	No Credit
		<100% ≥99.5%	3% of SLA Credit Baseline
		<99.5% ≥99.0%	5% of SLA Credit Baseline
		<99.0 % ≥98.5%	10% of SLA Credit Baseline
		<98.5%	15% of SLA Credit Baseline

SERVICE LEVEL AGREEMENT (SERVICE DOWNTIME)

Downtime: Any period of time when [service] applications are put into reduced functionality mode due to an issue with the [service] activation.

> "**Downtime**" is defined for each Service in the Services Specific Terms below. Downtime does not include Scheduled Downtime. Downtime does not include unavailability of a Service due to limitations described below and in the Services Specific Terms.

> "**Scheduled Downtime**" means periods of Downtime related to network, hardware, or Service maintenance or upgrades. We will publish notice or notify you at least five (5) days prior to the commencement of such Downtime.

Monthly Uptime Percentage: The Monthly Uptime Percentage is calculated using the following formula:

$$\frac{User\ Minutes\ -Downtime}{User\ Minutes}\ x\ 100$$

where Downtime is measured in user-minutes; that is, for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

Monthly Uptime Percentage	Service Credit
<99.9%	25%
<90%	50%

DATA SECURITY

If Supplier and/or its subcontractors and/or Affiliates collects, receives, accesses, analyzes, processes, transfers, transmits, stores, disposes, uses or discloses ("Processed and Transferred") any Customer Data, such party shall implement and maintain, or shall cause the subject subcontractors and/or Affiliates to have, a written information security program (the "Security Program") with reasonable administrative, physical and technical safeguards designed for the security, confidentiality and integrity of Customer Data that complies with applicable data protection and privacy laws and meet or exceed accepted industry practices.

Except as expressly provided in this Agreement, in no instance may any personnel or employee of Supplier (i) access and/or use any Customer Data, unless such access is to enable performance of any specific Services hereunder or (ii) release, transfer, store, disclose, disseminate, copy or download any Customer Data. In the event Supplier knows, or reasonably believes, that there has been any breach of any terms of this Section and/or any unauthorized acquisition, disclosure, use of and/or access to Customer Data (a "Breach"), Supplier shall take the following actions: (i) notify Customer of such Breach within 72 hours; (ii) identify for, and disclose to Customer at no cost to Customer, the specific data, by Permitted User and/or account number, which has or may have been compromised by the Breach; (iii) monitor any affected accounts for any unusual activity (if reasonable and appropriate in the circumstances); and (iv) to the extent such Breach is caused by Supplier, its Affiliates and/or their contractors and/or employees or is a result of an act or omission by Supplier, its Affiliates and/or their contractors and/or employees: (A) take prompt measures designed to contain and control the incident and prevent further unauthorized access, (B) implement a plan designed to remedy the circumstances that permitted such Breach to occur, and (C) cooperate with Customer as reasonably necessary to facilitate Customer's compliance with any applicable federal or state law regarding unauthorized access of Customer Data.

LIMITATION OF LIABILITY

- **Example 1:**

Limitation of Liability. IN NO EVENT SHALL THE AGGREGATE LIABILITY OF EACH PARTY TOGETHER WITH ALL OF ITS AFFILIATES ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER AND ITS AFFILIATES HEREUNDER FOR THE SERVICES GIVING RISE TO THE LIABILITY IN THE TWELVE MONTHS PRECEDING THE FIRST INCIDENT OUT OF WHICH THE LIABILITY AROSE. THE FOREGOING LIMITATION WILL APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, BUT WILL NOT LIMIT CUSTOMER'S AND ITS AFFILIATES' PAYMENT OBLIGATIONS UNDER THE "FEES AND PAYMENT" SECTION ABOVE.

Exclusion of Consequential and Related Damages. IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY LOST PROFITS, REVENUES, GOODWILL, OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER, BUSINESS INTERRUPTION OR PUNITIVE DAMAGES, WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF A PARTY OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR IF A PARTY'S OR ITS AFFILIATES' REMEDY OTHERWISE FAILS OF ITS ESSENTIAL PURPOSE. THE FOREGOING DISCLAIMER WILL NOT APPLY TO THE EXTENT PROHIBITED BY LAW.

LIMITATION OF LIABILITY

- **Example 2:**

  Limitation on Indirect Liability. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY, NOR VENDOR'S SUPPLIERS, WILL BE LIABLE UNDER THIS AGREEMENT FOR LOST REVENUES OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES, EVEN IF THE PARTY KNEW OR SHOULD HAVE KNOWN THAT SUCH DAMAGES WERE POSSIBLE AND EVEN IF DIRECT DAMAGES DO NOT SATISFY A REMEDY.

  Limitation on Amount of Liability. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY, NOR VENDOR'S SUPPLIERS, MAY BE HELD LIABLE UNDER THIS AGREEMENT FOR MORE THAN THE AMOUNT PAID BY CUSTOMER TO VENDOR UNDER THIS AGREEMENT DURING THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO LIABILITY.

  Exceptions to Limitations. These limitations of liability do not apply to violations of a party's Intellectual Property Rights by the other party, indemnification obligations, or Customer's payment obligations.

AUDITS

> **Example 1: Compliance and Supplier Audits**

During the Service Term, Supplier shall maintain (or, if the applicable Facility is a new Facility, implement controls at the Facility necessary to obtain) the industry-standard information technology security assessments or their equivalents for the Facility listed below; provided, that certification for new Facilities will not be maintained until after the first audit cycle for the applicable Facility. Upon request, Supplier shall make available for Customer's review (e.g., onsite at the applicable Facility or via web conference) reasonable documentation demonstrating its assessments and certifications. Subject to Customer's obligations of confidentiality hereunder, Customer may provide such documentation to its End Users, so long as any such End Users are required to sign a Customer confidentiality agreement which contains confidentiality provisions at least as protective as those contained herein:

(a) SSAE 18 SOC 1, Type II or equivalent;

(b) AT 101/SOC 2, Type II or equivalent;

(c) ISO27001 certification;

(d) PCI DSS assessment as Level 1 Supplier validating controls of Section 9 and 12

(e) HIPAA/HITECH assessed as required by colocation providers with regard to physical infrastructure and control to protect electronic protected health information (ePHI);

(f) Federal Information Security Management Act (FISMA) assessed to ensure compliance with the applicable controls from NIST 800-53;

(g) Federal Financial Institutions Examination Council (FFIEC);

(h) CSA Security, Trust and Assurance Registry (CSA STAR); and

(i) The Health Information Trust Alliance (HITRUST) Common Security Framework (CSF).

AUDITS

> **Example 2: Customer Audits**

During the applicable Service Term, Customer, Customer's internal and external auditors and any government authority or regulatory agency having jurisdiction over Customer's business (collectively, "**Auditors**") may conduct onsite audits of Supplier's operations, books and records, procedures and practices as reasonably necessary for Customer to verify Supplier's compliance with the Agreement and, in each case, to the extent applicable to the Services and the Colocation Space at which the Services are delivered. Each such audit shall be conducted during Supplier's regular business hours for its headquarters office, for a reasonable duration and upon reasonable advance written notice to Supplier. Customer shall not conduct more than one (1) audit per 12-month period, unless Customer's request is required by a government authority or regulatory agency. Supplier will be responsible for Supplier's own costs to support audits, while Customer will be responsible for audit expenses incurred by Customer and any Auditors provided, however, that if Customer exceeds one (1) voluntary audit per year (the "**Audit Cap**"), then Customer will reimburse Supplier for reasonable costs associated with any voluntary audits in excess of the Audit Cap as follows: [_____]. Supplier shall have no obligation to participate in more than [___] audits per year. For clarity, audits conducted in response to a breach of the Agreement and any audit to follow up on issues identified in a previous Audit shall not count toward the Audit Cap. All audits shall be conducted in accordance with Supplier Policies, including its physical access policy and audit policy, and shall be subject to the confidentiality obligations set forth in the Agreement. In no event shall an Auditor include a Supplier competitor nor shall an Auditor have the right to audit any areas or systems used by customers of Supplier (other than Customer), any of the internal cost information comprising Supplier pricing nor any fees that are charged on a fixed-cost basis. "All audits shall be conducted in accordance with Supplier Policies, including its physical access policy and audit policy, and shall be subject to the confidentiality obligations set forth in the Agreement. In no event shall an Auditor include a Supplier competitor nor shall an Auditor have the right to audit any areas or systems used by customers of Supplier (other than Customer), any of the internal cost information comprising Supplier pricing nor any fees that are charged on a fixed-cost basis. If an operational audit reveals that Supplier is not in material non-compliance with Applicable Law or any term of the Agreement, Supplier shall be responsible for and liable for, at its sole cost and expense, taking all necessary actions necessary to comply with such Applicable Law or term of the Agreement. In addition, if any such audit reveals an overcharge of more than five percent (5%) of the audited Charges in any Charges category, Supplier shall promptly reimburse Customer for the actual cost of such audit.

TERMINATION EXTENSION AND ASSISTANCE

> **Example 1: Termination Extension**

Prior to the expiration or termination of an Order Form, and separate from and in addition to any other extension rights or options provided for herein, Customer may extend the effective date of expiration or termination of such Order Form up to [two (2)] times each for a period of [ninety (90)] days (unless otherwise stated in the applicable Order Form) and, upon at least [sixty (60)] days' advance written notice to Supplier, provided that the total of all such extensions under this Section [XX] shall be no more than [one hundred eighty (180)] additional days from the effective date of termination of such Order Form. Notwithstanding the foregoing, the rights set forth in this Section do not apply in the event of a termination by Supplier for Customer's [breach/default] pursuant to Section [XX].

> **Example 2: Termination Assistance**

(a) During the Termination Assistance Period (defined below) and regardless of the basis for termination, Supplier shall provide, in accordance with the provisions of this Section [__], reasonable assistance to Customer and any third parties reasonably designated by Customer with regard to the winding down of the Services and the transition from Supplier to Customer or another provider. Upon Customer's written request prior to the effective date of termination and subject to subsection (b) below and Customer's continuing payment of the fees for the terminated Services, such assistance includes continuation of the Services during the Termination Assistance Period. The "Termination Assistance Period" is the period of twelve (12) months following the effective date of termination of the affected Services, provided such period does not extend beyond the Service Term then in effect with respect to such terminated Services. Customer may terminate the Termination Assistance Period early upon no less than ninety (90) calendar days' written notice to Supplier.

(b) Any resources that Supplier is required to expend in providing such cooperation or assistance and that are in addition to those resources otherwise provided under the Agreement for the terminated Services shall be chargeable to Customer at Supplier's then-current rates. If Supplier has terminated the Services for Customer's failure to pay undisputed amounts owed to Supplier, Supplier may condition the provision of the termination assistance on (i) payment in full of all outstanding undisputed amounts owed to Supplier and (ii) payment of fees in advance of each month for the provision of assistance during the Termination Assistance Period. Under no circumstances shall Supplier be required to (nor shall Customer) share Confidential Information of Supplier with, nor provide access to a Facility to, any third party that competes with Supplier.

FOR ADDITIONAL INFORMATION:

Kemal Hawa **Shareholder (Partner)** **Greenberg Traurig, LLP** **E-mail: hawak@gtlaw.com** **Phone: 703-749-1379**	**Amber Lester** **Assistant General Counsel** **CyrusOne, Inc.** **E-mail: alester@cyrusone.com** **Phone: 859-468-9803**
Emily Naughton **Shareholder (Partner)** **Greenberg Traurig, LLP** **E-mail: naughtone@gtlaw.com** **Phone: 703-749-1390**	