Service Description

Cloud Hosting and Disaster Recovery as a Service

1. Hosting of Client-Owned Equipment

a. Services outlined in the Service Order Form (SOF) (or defined under a separate SOW) such as monitoring, management, support and professional services (the "Services") will be supplied by CDI for Client's computer system located at CDI's facility (the Facility). The Facility will provide a safe and secure computing environment (electricity, temperature control, 24-hour security, UPS, generators, etc.) Any task not identified as a CDI responsibility shall be the responsibility of Client.

b. Client provided services include but are not limited to: a) configuration and support of all applications and software b) any and all application customization, troubleshooting and errors c) all end-user related support issues (user error, software bugs, local system issues, etc.) d) Internet connectivity issues that are outside the Facility

c. CDI will make available its online trouble ticketing system for Client's access to log and track issues. CDI will assign a Solution's Advisor (SA) who will serve as CDI's central point for management coordination, customer satisfaction and to provide periodic strategy and reviews to discuss high impact situations, (problems, changes and trends) with Client's designated representative.

d. CDI will provide Transition Services specifically listed in a separate Statement of Work to coordinate with Client either a new system installation or the move of Client's existing servers to the Facility. CDI will supply these transition services, including technical support, operations support and network support until installation and testing is completed and the software and hardware systems covered by this Statement of Work are operational at the Facility.

e. CDI will perform physical power-on/off or resets for equipment located in the Facility; place service calls to hardware vendors for equipment located in the Facility and monitor through resolution; and respond to requests from Client's central point of contact concerning system operational services as outlined in the SOF or under separate SOW.

f. Client will provide and deliver to CDI any Client-owned hardware to be located in the Facility. Client will be responsible for maintaining current manufacturer maintenance agreements (i.e. onsite break-fix warranty) on Hardware provided by Client. CDI will coordinate the move or delivery of Client's hardware to the Facility. Client will be responsible for all moving and insurance costs necessary to move the hardware. Client will provide hazard insurance for any Client-owned hardware while it is located at the Facility.

g. Client Supplied Software - Client will provide and deliver to CDI any software not listed on the SOF, together with all maintenance and upgrades or updates thereof. Client will be responsible for any maintenance, transfer or upgrade fees from software vendors. Client will be responsible for tracking and providing (at Client's expense) all required licensing and CALs on Client provided software.

h. Client will be responsible for providing any and all miscellaneous supplies, parts or ancillary items that may become necessary in the course of hosting servers. Client acknowledges that additional billings may be incurred to configure, install and maintain any additional hardware and software added to systems at the Facility that require CDI's involvement. Printing will be done remotely at Client's location using Client's printers and supplies, all of which are the responsibility of Client. All other hardware, laptops, workstations, etc not located at the Facility are the sole responsibility of Client.

2. Hosting on CDI-Owned Infrastructure (IaaS/DRaaS)

a. CDI will provide Infrastructure as a Service (IaaS) and Disaster Recovery as Service (DRaaS) as defined on the related Service Order Form

b. CDI's Cloud Hosting Platform Consists of the Following:

    i. Compute/Virtualization – CDI's compute platform is based on best of breed blade server and hyper-converged platforms. The systems are built with "full grid redundant power" (which means the system could survive the failure of two power supplies), redundant network and storage connections throughout while leveraging a central point of management. VMware vSphere and vCloud Director technologies provide the virtualization and multi-tenancy layer, and provides advanced features such as; Clustering with High Availability, Distributed Resource Scheduling, Distributed Switches, and Storage vMotion.

ii. Storage – The storage component consists of a highly reliable shared SAN infrastructure with five 9's of availability. Included are the latest Flash memory and SAS/NL-SAS disk technologies with redundant storage processors. The SAN is Flash-optimized with auto-tiering and virtual storage pool provisioning supporting multiple file and block storage protocols. Disk-based backups to a separate storage array are also included.

iii. Networking – The networking component consists of redundant blade server infrastructure fabric interconnects, access switches, core switches, uplink switches, routers, and firewalls. Our Internet access architecture consists of redundant Internet uplinks.

iv. Data Center

1. The Facility - The structure is made up of a combination of concrete block, brick, and steel. There are no windows located in the data-center areas.
2. Power Systems – The power system is built with N+1 redundancy. This provides a power system configuration in which multiple components (N) have at least one independent backup component to ensure system functionality continues in the event of a system failure. To be at a level of N+1, the overall system integrity is designed to withstand the failure of any one component, and is designed to continue to function at acceptable performance levels after the loss of any component.
3. Cooling systems - The HVAC systems at our data center are built with multiple technologies together to provide a very redundant, efficient and scalable solution. In use is a central HVAC room or Cell technology that utilizes innovative hot air recovery technology. This technology employs a common return plenum that is extended to the cabinet and is attached directly to the top of each cabinet. This technology enables the ability to host very high densities while eliminating data center hotspots. The HVAC network has been engineered with a minimum N+1 level of redundancy throughout the system.

v. Data Backup Service - CDI will provide the following data backup service for Client's data located at the Facility unless otherwise outlined in a SOF. Server images will be stored on a disk-based data backup repository located within the Facility. This standard data backup service includes full backup with 21 days retention/history. Additional retention/history or offsite options are optional and would be listed on a SOF.

vi. Uptime SLA - CDI will use commercially reasonable efforts to make the IaaS Cloud Services available with a Monthly Uptime Percentage of at least 99.95% in each case during any monthly billing cycle. In the event CDI does not meet the Service Commitment, Client will be eligible to receive a Service Credit as described below.

1. Definitions

a. "Monthly Uptime Percentage" is calculated by subtracting from 100% the percentage of minutes during the month in which CDI IaaS Cloud Services were unavailable. "Unavailable" shall be defined such that all running (always-on) CDI IaaS Cloud instances have no external connectivity.

b. Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any CDI IaaS Cloud Service Exclusion (defined below).

c. Exclusions - The Service Commitment does not apply to any unavailability, suspension, or termination of CDI IaaS Cloud Services, or performance issues of CDI IaaS Cloud Services: (i) that result from a suspension for non-payment, (ii) caused by factors outside of our reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of CDI's IaaS Cloud Services, or (iii) that result from any actions or inactions of Client or any third party; (iv) that result from Client's equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within our direct control); (v) that result from failures of individual instances or volumes not attributable to Unavailability; (vi) that result from any maintenance as provided for pursuant to the CDI Master Service Agreement; or (vii) arising from our suspension and termination of Client's right to use CDI IaaS Cloud Services in accordance with the CDI Master Service Agreement. If availability is impacted by factors other than those used in our Monthly Uptime Percentage calculation, then we may issue a Service Credit considering such factors at our discretion.

3. CLOUD BASED DISASTER RECOVERY SERVICES

a. If selected on the SOF, CDI will provide cloud-based disaster recovery services. CDI will implement replication technologies to enable replication of Client's servers to CDI's data center for the purpose of restoring the protected servers and making them available over a secure Internet connection.

b. CDI Cloud Disaster Recovery is a recovery-as-a-service (RaaS) solution that introduces native cloud-based disaster recovery capabilities for VMware vSphere® virtual environments. Replication is built on Zerto Virtual Replication and vCloud Director – a hybrid cloud platform for infrastructure-as-a-service (IaaS). Together, these components form a straightforward service- oriented approach to extending disaster recovery capabilities and protection coverage to any business or mission- critical application running in a vSphere virtual environment. CDI's Disaster Recovery Service leverages Zerto Virtual Replication to provide robust, asynchronous replication capabilities at the hypervisor layer. This approach to replication allows for virtual machines in vSphere to be easily configured for disaster recovery without the traditional dependencies on underlying infrastructure hardware or data center mirroring. Per-virtual-machine replication and restore granularity further provide the ability to meet dynamic recovery objectives without overshooting actual business requirements for disaster recovery as they change over time.

c. Key Service Attributes
   - i. Reserved Compute and Memory on CDI's Cloud to be used for DR Testing or Disaster Recovery Failover
   - ii. Storage of replicas of Client's protected virtual servers
   - iii. Replication software (Zerto)
   - iv. Colocation for legacy and other hardware as needed
   - v. Multiple network configurations available
   - vi. Comprehensive Disaster Recovery Operational Guide
   - vii. Retention of multiple recovery points – customized point-in-time instances
   - viii. Flexible failover testing

d. Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
   - i. The Recovery Time Objective (RTO) refers to the point in time in the future, after a declared disaster, that Client's protected servers and desktops will be up and running again. CDI's RTO is 4 hours or less.
   - ii. The Recovery Point Objective (RPO) refers to the point in time in the past to which data will be recovered by CDI. CDI's RPO is 1 hour or less.

e. Disaster Declaration: If the Client declares a disaster, CDI Managed Services will convert the client's protected servers into Virtual Machines in CDI's cloud environment, and make them accessible through the internet. The related service order form includes the fee structure for DR testing, Disaster Declaration, and Failover/Failback.