

Addendum
Desktop as a Service
June 2020

Contour Data Solutions
4259 West Swamp Road, Suite 301
Doylestown, PA 18902

This Desktop as a Service Addendum (this “Addendum”) is subject to and part of the Contour Master Cloud and Managed Services Agreement (the “Agreement”) between Contour Data Solutions LLC (“Contour”) and Customer. Any capitalized terms that are not defined in this Addendum shall have the meanings set forth in the Agreement entered by the parties.

1. Description of Services

- a. Contour provides Desktop as a Service (“DaaS”), that enables the delivery of virtual desktops, applications, and desktop disaster recovery capabilities to Customer. “Virtual Desktop” means a virtual computing environment hosting an end-user (non-server) operating system. “Virtual Server” means a virtual computing environment hosting a server operating system. “Virtual Machine” means a Virtual Desktop and/or a Virtual Server, as applicable.

2. Service Model Levels

- a. Customer must use Customer’s operating system volume license(s) purchased through a Microsoft licensing re-seller. At Customer’s request Contour can, subject to additional terms and conditions, provide licenses as a re-seller.
- b. The following are recommendations only. Please verify licensing requirements and restrictions with Customer Microsoft licensing distributor and/or reseller.
- c. All necessary Microsoft licenses for operating VMware Horizon desktops are available from Customer’s preferred Microsoft licensing distributor.
- d. Microsoft Windows 10 operating system licensed guest Virtual Desktops require Microsoft Virtual Desktop Access (“VDA”) subscription licenses or enrollment in Microsoft Software Assurance for Windows.
- e. Virtual Servers running Microsoft Windows must use Windows Server operating system licenses. Contour can provide Windows Server Datacenter Edition, subject to additional terms and conditions, as a re-seller.
- f. Because VMware Horizon desktop hardware requirements and Microsoft licensing policy change over time, Customer should check with its Contour Account Manager for the latest recommendations.

3. Service Objects

- a. All Service Offerings include the capability to access these objects/systems:
 - (1) Available Active Directory (“AD”) deployment and integration, including administrative roles, permissions, and end user groups.
 - (2) Virtual machine templates may also be managed through the Contour Virtual Desktop Administration Console and or though the Change Management Process and are used as the base image from which Virtual Machines are cloned.
 - (3) Remote Desktop Session Host (“RDSH”) published apps are the applications make available on hosted RDSH servers that are accessed by an end user.
 - (4) Desktop pools are groups of Virtual Machines, Remote Desktop Session Host (RDSH) published desktops, and Remote Desktop Session published applications that can be accessed by an end user. Pools specify which desktop model, image, desktop type, and other policies to apply when creating Virtual Machines. Virtual Desktops can only be

created as part of a pool.

- (5) Reserved Capacity, which may be selected and configured through the Cinch Portal.
Microsoft Federated Services

4. Support Services

- a. Incident and Problem Management
 - (1) As further provided in the Service Level Addendum, Contour will provide incident and problem management services with respect to:
- b. Infrastructure and software used by Contour to provide the DaaS environment, such as servers, storage and network devices, and supervisory software.
- c. Contour-provided operating system templates to the extent that:
 - (1) Published templates cannot be accessed.
 - (2) Published templates cannot be used for provisioning without modification.
 - (3) Published templates cause errors at first run time.
 - (4) There are substantial hangs or excessive delays in the retrieval of a template.
 - (5) The configuration of a published template affects the Virtual Machine's interaction with the hypervisor; and
 - (6) Time synchronization issues (NTP) exist
- d. Customer is responsible for incident and problem management (such as detection, severity classification, recording, escalation, and return to service) with respect to:
 - (1) User-management within Customer's Active Directory environment.
 - (2) Customer deployed and configured assets, such as custom-developed or third-party applications, custom or user-deployed operating systems, network configuration settings, and user accounts.
 - (3) VPN integration and configuration on Customer's firewall.
 - (4) Performance of Customer-deployed or custom or third-party applications, Customer databases, and operating systems imported or customized by Customer, or other assets deployed and administered by Customer that are not provided by Contour or otherwise unrelated to the Contour Cloud or DaaS
 - (5) Anything else not under the direct control and administration of Contour.
- e. Change Management

5. Contour will provide the following change management elements:

- a. Processes and procedures to maintain the health and availability of the Contour service components.
- b. Processes and procedures to release new patches, updates, hot fixes, and service packs related to providing and administering the DaaS environment and infrastructure.
- c. **Customer is responsible for:**
 - (1) Management of changes to Customer's operating systems, custom or third-party applications, and administration of any components within Customer's control.
 - (2) Cooperating with Contour when planned and emergency maintenance is required.

6. Security

- a. "Contour Area" means the areas of the Contour infrastructure and systems for which Contour has sole administrative control. "Customer Area" means the portions of the systems where Customer assumes full or partial control, permission, or access to modify an

environment.

b. Contour will use commercially reasonable technical and organizational measures designed to provide the following:

- (1) Physical security measures intended to protect Contour’s data centers from physical security breaches;
- (2) Information security measures intended to protect the Contour Area.
- (3) Network security measures intended to protect the Contour Area.
- (4) Monitoring for potential security events in the Contour Area.
- (5) Patching and vulnerability management of the systems Contour uses to deliver the DaaS environment, including the application of patches it deems critical for the target systems. Contour will perform routine vulnerability scans of the Contour Area to identify critical risk areas for the systems it uses to deliver the DaaS service. Critical vulnerabilities will be addressed in a commercially reasonable manner.

c. Customer is responsible for:

- (1) Information security measures to protect the networks, information systems, data, content or applications in the Customer Area, including without limitation any patching, security fixes, encryption, access controls, roles and permissions granted to Customer’s internal, external, or third-party users;
- (2) Network security measures to protect the networks, including software defined networks, within the Customer Area, including measures such as maintaining effective firewall rules, exposing communication ports only as necessary to conduct business, preventing and promiscuous access.
- (3) Monitoring for potential security events in the Customer Area.
- (4) Security monitoring and response for the Customer Area, including detecting, classifying, and remediating all security events in the Customer Area, through the use of such measures as vulnerability scanning tools or monitoring tools, or that are required for Customer’s compliance or certification program; and
- (5) Identifying and remediating compromised desktops within the Customer Area and resolving all related issues. Contour reserves the right to suspend desktops, or all or any portion of the Service Offerings if compromised environments are detected by Contour to protect Contour’s infrastructure and business operations.
- (6) Customer is required to utilize on each desktop a reputable anti-virus program, which must be running, up to date, and properly configured.

7. Usage and Other Restrictions

- a. Virtual Desktops are intended for use with desktop applications only. However, with Contour’s prior written authorization, Customer may use a Virtual Desktop instance as a utility server, such as a domain controller, active directory server, DHCP relay or file server.
- b. Any use of applications intended for use on servers or transactional applications is not supported and may interfere with performance and user experience. Encrypted hard disks are not allowed within the DaaS environment.
- c. Contour is not responsible for issues arising from inadequate bandwidth at Customer locations, whether on-site or remote.

d. Monitoring & Management with Service Levels

- (1) **Monitoring System:** Contour will use system monitoring tools (the “Monitoring Systems”) to monitor the Managed Systems. Contour will use an incident management system to automatically create incident tickets and track the management of those incidents.
 - (2) **Monitoring Dashboard/Portal and Business Views:** Contour will provide Customer with access to a dashboard and management portal (“Customer Portal”) through which Customer may access incident ticketing information, reports, and trending data with respect to Managed Systems.
 - (3) **Monitoring Services:** Contour’s proactive Monitoring Systems and Customer Portal will be available as set forth in this Exhibit. The Monitoring Systems collect and evaluate availability and performance statistics from Managed Systems and present those statistics to Customer via the Customer Portal. In addition to monitoring up/down status of each device with a Managed System, the Monitoring System monitors the critical application attributes that are identified in cooperation with Customer and set forth a Service Order.
 - (4) **Incident Management:** Contour will manage the collection, communication, and escalation of incidents arising as a result of alerts received from the Monitoring System, in accordance with the written standard operating procedures (the “SOPs”) agreed upon with Customer in writing and the terms and conditions defined in this document.
- e. **Proactive Management:** Contour will provide the Infrastructure Management Services identified in the applicable Service Order, for the Managed Systems specified in the applicable Service Order.

(1) The Infrastructure Management Services may include:

- (i) **Preventative Maintenances:** Contour will perform appropriate preventative maintenance tasks on Managed Systems. The tasks may include services such as log review, job monitoring, and replication job monitoring, disk defragmentation, virtualization configuration analysis and adjustments, each as further defined in an SOP.
- (ii) **Health Checks:** Health checks are a technical assessment of Customer’s existing physical and virtual Managed Systems to ensure that you continue to achieve optimal levels of performance and efficiency. Health checks maximize the return on your investments and provide a proactive, in-depth understanding of the performance level across your network, servers, storage systems, and backup systems. Contour staff will provide daily health checks in accordance with the applicable SOP to ensure that all critical components of your environment are physically inspected and affirmed operational by one of its team members.

f. **Performance Tracking/Reporting:** Contour will regularly monitor and analyze the performance and utilization data from Managed Systems, to identify trends and tuning opportunities with respect to Managed Systems. That data will be shared with Customer on

an ad hoc basis, and on a monthly management report, which reviews the service level status and service support delivery of Managed Systems. As reasonably requested by Customer, Contour will provide reports regarding the performance, capacity, availability, and incidents for of all Managed Systems. Contour and Customer will also meet as reasonably requested by Customer to review the status of the account.

g. Remediation Services: For incidents that have been detected and reported to Contour by the Monitoring Systems (“Incidents”), Contour will provide the first level response. Contour will provide this response in accordance with a Customer-provided run book, which has been reviewed and accepted by Contour (not to be unreasonably withheld, conditioned, or delayed). Customer hereby authorizes Contour to open support tickets for Customer with Customer’s internal escalation resources and/or third parties required for resolution (including, but not limited to, manufacturers, service providers, and telecommunications carriers). Contour will work to remediate Incidents, as set forth in the applicable Service Order and the SOPs. Customer may engage Contour to manage the troubleshooting and resolution of other issues, on a time and materials basis or as part of an established retainer-based Service, in either case as set forth in one or more SOWs.

h. Standard Operating Procedures: The SOPs will contain prioritization levels associated with specific events, business requirements, and other management and support criteria designated by Customer. The SOPs will specify the prioritization definitions outlined in Help Desk Procedures, the SOPs will govern the escalation and issue management process.

i. Periodic Review Meetings: The Contour employee that is dedicated to managing Customer’s account (“Account Manager”) may from time to time meet with stakeholders from Customer and other members of the Contour support team to review reports, identify meaningful trends, and to discuss the priorities and concerns of all parties. These meetings are designed to last from one to two hours, and may be held at Customer’s location, by telephone, and/or as otherwise mutually agreed by the parties.

j. Infrastructure as a Service: All hardware provided by Contour that is not sold or leased to Customer pursuant to a Service Order, is the sole property of Contour and will remain so for the Term.

k. Equipment Location Use and Repair: If Contour-provided Managed Systems are located other than at a Contour-owned or Contour-managed location (collectively, “Off-Premises Contour Equipment”), then Customer agrees to the terms and conditions herein. Customer will maintain and use Off-Premises Contour Equipment only at the location shown on the applicable Service Order. Customer agrees that it will not move Off-Premises Contour Equipment from that location without the advanced written approval of Contour. Customer is solely responsible for maintaining all Off-Premises Contour Equipment in good repair and proper working order. Customer is solely responsible for maintaining a safe and sufficient operating environment and protecting all Off-Premises Contour Equipment from damage of any kind whatsoever. Customer will continue to make all required payments to Contour in the event of any loss, damage, or destruction of any Off-Premises Contour Equipment, including if such equipment is rendered inoperable or is completely destroyed. Customer will not modify or make alterations or attachments to any Off-Premises Contour Equipment without prior written authorization from Contour. Customer acknowledges and warrants that Contour, or its agents shall have the right to inspect any Off-Premises Contour Equipment during Customer’s normal business hours without notice to Customer at such Off-Premises Contour Equipment’s current location. Customer will cooperate with Contour

or its agents as necessary to complete regular maintenance and repair activities of Off-Premises Contour Equipment. Upon termination or expiration of the applicable Service Order, Customer will return all Off-Premises Contour Equipment to Contour in substantially the same condition as when such equipment was provided to Customer, normal wear and tear expected. Customer acknowledges and agrees that Contour will invoice Customer, and Customer will pay, for all repairs or replacements to Off-Premises Contour Equipment.

I. Insurance: During the Term, Customer will procure and maintain property insurance covering all Off-Premises Contour Equipment at Customer's sole expense, naming Contour or its designee as the sole loss payee, for the full replacement value of the Off-Premises Contour Equipment, and general liability insurance listing Contour or its designee as an additionally insured. Customer will furnish Contour with proof of insurance upon request. If Customer is unwilling or unable to provide proof of insurance, Contour will procure such insurance for the Off-Premises Contour Equipment and add the cost of such insurance to the amounts due from Customer under this agreement. All changes to such insurance must be disclosed in writing to Contour within thirty (30) days of Customer becoming aware of such changes. Customer hereby irrevocably appoints Contour as its attorney-in-fact to make claim for, receive payment of and execute and endorse all documents, checks or drafts for loss or damage under any insurance policy insuring the Off-Premises Contour Equipment.

8. Service Level Agreement

- a. Contour will provide certain aspects of the Infrastructure Management System to Customer in accordance with the following Service Level Agreement (this "SLA").
- b. **System Availability**
 - (1) "Available" or "Availability" means the time (in minutes) that the system being measured could establish a network connection and that its material features and functions are up, running, and operationally functional. "Excluded Downtime" means the time (in minutes) that the system being measured is not Available, to the extent caused by (A) Customer-provided hardware, software, or other equipment not provided by or certified by Contour; (B) Customer-provided or Customer-leased local area networks or ISP connections; (C) modifications made by Customer without Contour's prior written approval; (D) use of the system by Customer, its employees, agents, or contractors, in ways not authorized by this Exhibit; (E) Maintenance Downtime, as defined below; (F) Customer's failure to use sufficient, redundant power sources or Internet connectivity; (G) a Force Majeure event; or (H) any other system outside of Contour's control. "Maintenance Downtime" means scheduled repairs, maintenance, upgrades, or deployments related to Contour's equipment, network, or facility, and other events agreed upon in advance by Contour and Customer. "Total Minutes" shall mean the number of minutes in the applicable calendar month.

"Percent Available" will be calculated as follows: $((\text{Availability} / (\text{Total Minutes} - \text{Excluded Downtime})) \times 100)$.

9. Monitoring System

- a. In each calendar month during the Term, the Percent Available for the Monitoring Systems will

be 99.99%.

b. Ticketing System

(1) In each calendar month during the Term, the Percent Available for the Customer Portal will be 99.99%.

c. Managed Data Center and internal Network Availability

(1) In each calendar month during the Term, the Percent Available for the network within the locations used to store Managed Systems (“Data Center”) will be 99.99%.

d. Redundant Devices

(1) In each calendar month during the Term, the Percent Available for each Redundant Device managed by Contour will be 99.99%.

e. Device Availability

(1) In each calendar month during the Term, the Percent Available for each Non-Redundant Device managed by Contour will be 50.00%.

f. Non-Standard Equipment

(1) Customer may require Contour to manage or support hardware and/or software products for which Contour does not typically provide support as part of the Infrastructure Management Services (collectively, “Non-Standard Equipment”). Contour shall not be responsible under this SLA or this Exhibit for the Availability or functionality of any Non-Standard Equipment, and Customer shall not be eligible for credits under this SLA for the failure of any Non-Standard Equipment.

g. Security

(1) Contour shall use commercially reasonable efforts to secure: (i) the Data Centers and networks contained therein; and (ii) Managed Systems (including testing and deploying security patches and fixes, where appropriate).

h. Failure to Meet SLA

(1) In a calendar month where Contour fails to meet any expressly stated service level commitment in this Section 2, Customer will give Contour written notice thereof no later than ten (10) business days after the end of such calendar month. Contour will investigate such failure promptly after its receipt of notice.

i. Response Time SLA for Remediation Services

(1) Beginning forty-five (45) days after the Acceptance Date and continuing for the Term, Contour will respond to issues relating to the Infrastructure Management Services, in accordance with the tables below and based on the priority of the issue. Contour is not responsible for issues caused by any of the items within the definition of Excluded Downtime (“Excluded Issues”).

j. Initial Response SLA

(1) Contour will initially respond to issues reported by the Monitoring Systems, in accordance with the following table.

SLA	Criteria	Initial Response Commitment Level
Response	Initiate response to monitoring system alert	<15 minutes response

In a calendar month where Contour fails to initially respond to an issue within the Initial Response Commitment Level above, Customer will give Contour written notice thereof no later than ten (10) business days after the end of such calendar month. Contour will investigate such failure promptly after its receipt of notice.

k. Incident Management and Escalation SLA

(1) Contour will acknowledge and escalate issues reported by the Monitoring Systems, in accordance with the following table.

Priority	Status	Action	Time	Escalation
P1 - Critical	Unassigned	Response/Acknowledgement	15 minutes	NOC Tier 1
P1	Assigned	NOC escalates to Tier 2	15 minutes	NOC Tier 2
P1	Assigned	Tier 2 calls Engineer	30 minutes	Engineering
P1	Assigned	Crisis Management Process	1 hour	CRISIS
Priority	Status	Action	Time	Escalation
P2 - High	Unassigned	Response/Acknowledgement	15 minutes	NOC Tier 1
P2	Assigned	NOC escalates to Tier 2	1 hour	NOC Tier 2
P2	Assigned	Tier 2 calls Engineer	4 hours	Engineering
Priority	Status	Action	Time	Escalation
P3 - Low	Unassigned	Response/Acknowledgement	15 minutes	NOC Tier 1
P3	Assigned	NOC escalates to Tier 2	8 hours	NOC Tier 2
P3	Assigned	Tier 2 calls Engineer	24 hours	Engineering

In a calendar month where Contour fails to acknowledge or escalate an issue within the time set forth above, Customer will give Contour written notice thereof no later than ten (10) business days after the end of such calendar month. Contour will investigate such failure promptly after its receipt of notice.

Priority Definitions

Priority Level	Criteria
Priority 3	Managed Systems is not Available, but with minor operational variances (e.g., bugs).
Priority 2	Managed systems are partially unavailable
Priority 1	Managed Systems are completely unavailable

i. Knowledge Management SLA

- (1) For each issue responded to in accordance with this Section m, Contour will record relevant information in its incident management system and provide access to Customer upon request. In addition, for each calendar month, Contour will deliver a report to Customer that summarizes all issues in such month, by no later than seven (7) days after the end of such month.
- (2) In a calendar month where Contour fails to perform its obligations in this subsection, Customer will give Contour written notice thereof no later than ten (10) business days after the end of such calendar month. Contour will investigate such failure promptly after its receipt of notice.

m. Excluded Issues

- (1) Contour is not required to provide support for Excluded Issues. Contour may, in its sole discretion, provide support for Excluded Issues, and Customer will pay for all such support at Contour's then-standard hourly rate. Contour is not responsible for Customer's failure, for any reason, to respond to alerts or incidents escalated by Contour in accordance with this Exhibit.

n. Customer Responsibilities

- (1) **Customer alone is responsible for:**
 - (i) Designating a qualified liaison between itself and Contour;
 - (ii) Providing Contour with the names of persons (and alternates) responsible for technical, administrative and contact matters; Obtaining licenses and complying the terms thereof for all software utilized on Customer's equipment and environments; All communications with Customer's end users, whether for technical support, business relations or any other purpose; and if applicable, providing Contour with a list of end users for service and/or support.

o. Transition Services

- (1) If Customer requests (which must be made before the termination or expiration of the applicable Service Order), then Contour, for a commercially reasonable period of time (not to exceed thirty (30) days) will provide assistance to Customer in the transfer of Customer's Managed Systems to a third party or to a Customer site (the "Transition Services"). Such

Transition Services will be rendered and paid for by Customer on a time and material basis, plus all reasonable and necessary travel and living expenses. Promptly after Customer’s request (which must be made no later than thirty (30) days after the end of the applicable Service Order), Contour will provide Customer with all of Customer’s data in Contour’s possession, at no expense to Customer.

Revision History

Contour Data Solutions Public Information					
Type	Title	Date	Version	Description of Changes	Author
Addendum	Desktop as a Service	05/05/2020	1.0	Initial Draft	Rocco Guerriero
Addendum	Desktop as a Service	06/03/2020	1.0	Final Release	Rocco Guerriero
Addendum	Desktop as a Service	06/08/2020	2.0	Complete review	Rocco Guerriero
Addendum	Desktop as a Service	06/08/2020	2.0	Organizational Format / Layout Changes	Rocco Guerriero