CARBON 60
THE MANAGED CLOUD COMPANY

Service Description:
Managed Cloud for Azure

CONTENTS

1 INTRODUCTION

This Service Description provides detailed information of Carbon60's services. The Customer Order(s) will indicate which services are part of their solution and takes precedence over this document. If you require further clarification of have any questions about the services outlined herein, please contact us.

Carbon60 reserves the right to modify service descriptions as we continually seek to improve the efficiency and effectiveness of our services.

1.1 CONFIDENTIALITY STATEMENT

This document is confidential. Possession, transmitting, or receiving this document requires the consent of Carbon60 and does not expressly license or imply rights to copy, use, sell, design, or develop products or services from this information. Transfer of this document from the custody and control of Carbon60 constitutes a loan for limited purposes. This document must be returned to Carbon60 upon request. Unauthorized reproduction, publication, or disclosure of this information in whole or in part, by any means, is prohibited.

1.2 FAIR USE POLICY

Carbon60 provides various services as outlined in this service description. Through this fair use policy, we seek to ensure an optimal, as well as fair, user experience and support experience for all our customers. Carbon60 is committed to an up-front, published, simple, transparent pricing model. However, Carbon60 needs to ensure that our services are not monopolized by a small subset of customers. Therefore, we monitor the effort spent by our technical team to support customers' environments according to a fair use policy. To ensure that all customers have access to our technical support that is commensurate to the fees in an Order, we may notify a customer that they are consuming more support time or logging more support issues than scoped or that of a typical customer with similar users and a similar subscription and additional fess may apply to provide adequate support.

2 MANAGED CLOUD FOR AZURE

Managed Cloud for Azure is a service that will maximize the availability and accessibility of the Customer's environment(s) in the public cloud, managed by a world class team that responds quickly to issues and sees them to resolution. Carbon60 will provide operational support services of Customer's environments and support resources at a platform level that are controlled by the Cloud Service Provider's (CSP) console or APIs.

2.1 SERVICE SELECTION

Carbon60 provides two service options from which the Customer can choose, *Essentials* and *Enhanced*, designed to meet the level of support the Customer requires for their environments.

2.1.1 MANAGED CLOUD FOR AZURE ESSENTIALS

Managed Cloud for Azure Essentials is a base service focused on monitoring, investigation, and remediation of the infrastructure of our customer's Azure environment. Carbon60 enables Azure monitoring while using best practices for investigation and resolution. Carbon60 utilizes Azure technologies and is monitored and managed by our specialist Cloud Operations teams. With *Managed Cloud for Azure Essentials* you can focus on your application while being assured that Carbon60 is ensuring availability and will escalate with Microsoft on your behalf.

2.1.2 MANAGED CLOUD FOR AZURE ENHANCED

Managed Cloud for Azure Enhanced is an advanced service that expands upon the *Essentials* service to also include *Patching*, *Backups and Restore*, *Managed Security Services*, *Endpoint Protection*, and full *Service Desk Support*. Our team of certified cloud experts will triage and respond to any alerts configured in your environment and actively ensure your solution is following best practices, up-to-date, and secure. We'll take care of the day-to-day operation of your compute and data infrastructure ensuring they are backed up, have data resiliency (where required), and are performing to your expectations.

2.2 ONBOARDING

Once the customer is ready for onboarding, Carbon60 first assigns a project manager to manage the process of onboarding the customer environment into the *Managed Cloud for Azure* service based on the *Essentials* or *Enhanced* package that was selected.

2.2.1 ONBOARDING TERMS

During the initial phase of onboarding, Carbon60 assesses the time needed to onboard the customer based on the complexity and intricacies involved with deployment and to plan and track the progress to readiness.

It's important to note that by default Carbon60 performs onboarding of Customer environments into the service during Business Hours.

2.2.2 DEPLOYMENT

Carbon60 will require access to the Customer's Azure account(s) where the to-be-managed environments reside. This includes Azure Resource Manager Portal and API access, as well as network or VPN access that may be required to access systems. This enables Carbon60's operational teams to provide the contracted management services within the Customer's environment where configuration, maintenance, troubleshooting, and service desk support are required.

The level of access required by Carbon60 is determined by the contracted level of service, *Essentials* or *Enhanced*. For example, *Managed Cloud for Azure Essentials* access is limited mostly to a read-only role for the purposes of our monitoring tools to capture platform metrics, with additional permissions required for Azure VM, SQL Database, and Azure Database for MySQL instances to enable Carbon60 engineers to troubleshoot incidents.

During the onboarding process, Carbon60 requires access information for the Customer's chosen public cloud platform such as network address(es), accounts/subscriptions and logins, authentication, and permissions. This is a prerequisite for Carbon60 to deliver *Managed Cloud for Azure Essentials* or *Enhanced* to the Customer. The necessary documentation will be made available at the time of onboarding the environments.

The statement of work (SOW) details the policies that the Customer needs to comply with for the duration of the contract.

2.3 MANAGED CLOUD FOR AZURE ESSENTIALS

Monitoring as a Service: The service will monitor the availability and accessibility of the Customer's environments. Carbon60 will monitor IaaS and PaaS services at the Platform Level by ingesting Azure monitor metrics. Carbon60 will define alerting for these metrics based on best practices and Customer requirements. The performance metrics will also be collected to detect trends with defined thresholds for alerting and per-incident performance analysis.

An optional service can be purchased for automated monitoring and notification of any public websites (HTTP/S endpoints) so that Carbon60 can respond to, and notify a customer, if a website becomes unavailable. Carbon60 will carry out an HTTP check on the specified public endpoints identified during onboarding to detect bad response codes (e.g. 404).

Remediation: Carbon60 will provide hands on intervention and resolution of incidents captured through Monitoring. Carbon60 will assist Customers with resolving issues with the service or resource at Platform level based on Carbon60's standard Incident and Request Management Service Level Objectives, with the focus of providing availability and accessibility of the resource and service within Customer environments.

2.3.1 SERVICE LEVELS

Service	Service Level Hours
Onboarding	Business Hours (9x5)
Platform Availability Management	24x7
Support (Critical)	
Support (Normal, High)	

2.3.2 OPERATING SYSTEMS SUPPORTED

Carbon60 supports all operating systems currently supported by Azure Monitor. A full list of operating systems can be found on the following webpage: https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview

Carbon60 tools may require updating and may need to be tested to ensure they work as expected with new versions of operating systems. For that reason, at times, Carbon60 may not be able to support new LTS versions of operating systems as soon as they are released.

In the case of OS vendors making changes that require Carbon60 to adjust the tooling, Carbon60 reserves to determine the time required to make all necessary changes to support new LTS releases.

Versions not supported by Azure are supported on a commercially reasonable effort basis and are subject to limitations based on deprecated vendor support.

2.3.3 PLATFORM AVAILABILITY MANAGEMENT

Carbon60 will monitor the health of cloud resources for each mutually agreed Azure subscription and can raise an alert based on the event conditions defined in our preconfigured thresholds. Carbon60 defined Azure health check metrics are based on a subset of available Azure Monitor metrics.

In the event an alert is raised, Carbon60 will provide Incident Notification and Incident Resolution in accordance with the Incident Management Process.

Data Residency: All monitoring data collected by Carbon60 will be stored on servers hosted in Canada.

Data Collection: For CSP native monitoring services (eg. Azure Monitor), data will be collected from an external 3rd party tooling provider via API requests to the appropriate service. As part of the onboarding process, a service account role with required permissions will need to be created in the Customer's environments to allow this collection. Frequency of collection is configurable, with default being every **5** minutes. Over time, older metrics data might be aggregated for performance reasons.

Data Retention: Monitoring data will be retained for **six (6) months**.

During onboarding, Carbon60 will apply a baseline of monitoring metrics to effectively monitor the Cloud environment. Carbon60 can configure custom platform alerting on a case-by-case basis as agreed during the solutioning and sales process. Carbon60 will configure the monitoring alerts to the needs of the

Customer environment(s), focusing on monitoring key components which indicate that the platform is available and accessible. Carbon60 will only perform monitoring of the services which are critical for the health and availability of the environment.

2.3.4 'SUPPORTED' AND 'MONITORED' SCOPE

Best Practices: Carbon60 holds expert level knowledge of this service and leverages this to provide guidance and advice to Customers. Architects will be able to advise Customer on changes to the service that are in line with the best practice guidelines provided by the vendor and discuss details and intricacies of the service with Customers.

Configuration Management: Where remediation is included, Carbon60 will perform changes to the service at the Platform Level, using the CSP's Management Console or Programmatic API to execute the change. The scope of any changes to be carried out will strictly be to resolve incidents related to the affected resource/service.

Out of Scope Configuration Management: Please note that within the *Managed Cloud for Azure Essentials*, Carbon60 will only perform Platform Level support and will not provide resource level administration.

As an example, for SQL Database, Carbon60 will ensure that the database is running correctly (eg: Azure Monitor metrics) but will not provide any service that interacts with the data inside the database (eg: altering tables, modifying data, creating SQL users).

Service Troubleshooting: Where remediation is included, Carbon60 will assist Customers with troubleshooting issues with the service or Resource at the Platform Level, with the focus of providing availability and accessibility of the resource and service within Customer environments.

Out of Scope Support Boundaries: For services that are not included in the "supported" list below, Carbon60 will endeavor to work with the Customer and CSP Support team, leveraging CSP's in-house skills and documentation to deliver guidance for this service. *Managed Cloud for Azure Essentials* will only support existing resources, provisioning of net new resources is not included unless it's necessary while resolving issues with existing infrastructure.

2.3.5 SUPPORTED AND MONITORED AZURE SERVICES

Carbon60 can monitor any Azure service that produces monitoring and performance metrics through Azure Monitor. The services that will be monitored by Carbon60 are identified by the Customer and reviewed by Carbon60 during the onboarding process to ensure the relevant Azure resources are covered.

Carbon60 will support the following types of Azure resources under this *Managed Cloud for Azure* service, additional services can be included in the monitoring:

**Additional services subject to monitoring may be added at a future date*

Compute

- VM, Disk, Load Balancer, Scale Sets, Functions, App Service

Containers

- Container Instances, Container Registry, Kubernetes Service

Storage

- Azure Blob, Azure Files, StorSimple, Azure Backup

Database

- Relational databases, Cosmos DB, Cache for Redis

Networking & Content Delivery

- Virtual Network, VPN gateway, Content Delivery Network, Traffic Manager, ExpressRoute

Management & Governance

- Monitor, Resource Manager, Activity Log, Application Change Analysis, Automation, Monitor, Advisor

Security, Identity, & Compliance

- Azure AD and RBAC, App Service Certificates, Key Vault, Logic Apps

Application Integration

- Service Bus, Queue Storage

End User Computing

- Azure Virtual Desktop

2.4 MANAGED CLOUD FOR AZURE ENHANCED

Managed Cloud for Azure Enhanced includes all the features of the *Essentials* service, with the following additional features to deliver an effective managed cloud service:

a) **Patching** – Security patches will be applied monthly to Azure VM instances, with the ability to audit and report on the patches applied, while maintaining compliance standards.
b) **Backups and Restore –** Block level backups will be taken for Operating Systems and Database Engines with restore of backups performed via service desk requests.
c) **Endpoint Protection –** as part of managing any virtual machine (VM) in the Customer environment Carbon60 includes endpoint protection software to provide anti-virus and anti-malware protection. The supply, configuration, tuning, and ongoing maintenance are part of the service.
d) **Service Management Support** – The customers public cloud environment(s) will be maintained as part of the service including configuration management and any troubleshooting that may be required to address issues with availability and accessibility of the environment(s). Incidents and Changes will be managed using the standard Carbon60 ticketing tools and procedures. The total hours of Service Management Support available to the customer will be outlined in the Managed Services for Azure SOW.

Carbon60 provides optional services that Customers can add for additional management and oversight of their Azure footprint:

- **Managed Security Services –** As an extension to *Managed Cloud for Azure Enhanced*, Carbon60 can offer additional managed security services focused on threat and vulnerability management. These offerings are purchased at an additional cost and details can be found in the "Carbon60 Service Description – Managed Security Services" document.
- **Cost Management –** designed to address and overcome many of the challenges that enterprises face with public cloud billing, usage insight, financial governances, and cost optimization.

2.4.1 SERVICE LEVELS

Service	Service Level Hours
Onboarding	North American Business Hours (9x5)
Platform Availability Management	24x7
Backup and Restore	
Endpoint Protection	
Service Desk Support (Critical)	
Service Desk Support (Normal, High)	
Patching	24x5
Service Management Support	

2.4.2 VM AGENTS INSTALLED ON COMPUTE RESOURCES

Carbon60, as a part of delivery of the *Managed Cloud for Azure Enhanced* services, may install the following agents onto the compute resources:

Vendor	Agent	Notes
CrowdStrike	Falcon Agent	Endpoint Protection Agent
Azure	Log Analytics	Management Agent used for the purpose of patching
Azure	Monitor	Agent used for monitoring performance and to assist in cost management

Carbon60 reserves the right to change or add agents to the customer VM's. The customer will be notified of any changes made with advance notice. All applicable fees will apply (monthly recurring and non-recurring).

2.4.3 SCOPE OF SUPPORT

Best Practices: Carbon60 holds expert level knowledge of this service and leverages this to provide guidance and advice to Customers. Architects will be able to advise Customer on changes to the service that are in line with the best practice guidelines provided by the vendor and discuss details and intricacies of the service with Customers.

Configuration Management: Where remediation is included, Carbon60 will perform changes to the service at the Platform Level, using the CSP's Management Console or Programmatic API to execute the

change. The scope of any changes to be carried out will be to resolve incidents related to the affected resource/service.

Service Monitoring: Carbon60 will integrate into the native Azure monitoring service to provide monitoring to customers. Carbon60 will use API calls to collect various metrics from Azure Monitor and will ingest those metrics into a monitoring platform, where further analysis will be performed to identify problems and patters within the customer environment.

Carbon60 will investigate events in accordance with the agreed upon monitor alerting thresholds. If necessary Carbon60 will raise a support case to contact the customers primary contact(s) to inform them of the details of the support case. Carbon60 reserves the right to disable or modify a specific monitoring or alerting configuration on notice to the customer, if deemed necessary by Carbon60 for accurate alerting.

Compute Resources: For an additional level of monitoring for compute resources, Carbon60 will require to perform an installation of agent software on every compute resource that is supported.

Out of Scope Support: Customer hosted applications, such as databases, network, and web servers will only be monitoring for performance of the underlying VM infrastructure that they are running on.

2.4.4 PATCHING

Scope: Carbon60 uses Azure Automation along with Azure Monitor to automate the process of patching your managed instances with both security related and other types of updates. Azure Automation uses patch baselines, which can include rules for auto-approving patches within days of their release, and a list of approved and rejected patches.

Carbon60 will perform the following OS patching where patches are made available by the OS provider:

Type	Frequency
Critical and Security Patching	Monthly, within mutually agreed maintenance window with customer during onboarding.
Responsible Disclosures and Zero-day events	Where the risk profile is severe, responsible disclosures and zero-day events will trigger a patching or remediation effort from Carbon60

If a non-marketplace Azure VM is used as a source for the infrastructure deployment, Carbon60 will hold temporary snapshots as a roll-back mechanism if required during critical/security patching.

OS Upgrades: Carbon60 considers this type of activity Service Packs (Windows) or Distribution Upgrades (Linux) as more complex, with higher risk to application stability. For this reason, Carbon60 does not perform this type of upgrade by default, and only by customer request. OS upgrades will be subject to an additional statement of work and will incur one-time professional service charges and will require additional temporary Azure resources for the process.

2.4.5 BACKUP AND RESTORE

Azure VM Compute Backup

Backup of Azure VM instances is performed using the Azure Backup service or by taking a snapshot of Azure Managed Disk volumes based on the schedule, whichever makes the most sense for the Customer's environment.

Carbon60 will perform daily, weekly, and monthly backups of the Azure VM instances based on the following default schedule and retention periods:

Backup	Schedule	Retention
Daily	02:00 AM EST Monday to Sunday	14 days
Weekly	03:00 AM EST Sunday	3 weeks
Monthly	04:00 EST on the first of every month	1 month

Customers may request alternative backup schedule and retention periods at any time but will require the approval of Carbon60. Note that increasing retention periods will result in additional Azure usage costs.

All backup failure alerts will automatically be assigned as an incident request and actioned by the Carbon60 operations team.

Azure VM Compute Restore

When required, Carbon60 will assist with restoring from a backup on an Azure VM instance within the account being supported. The restore will be treated in priority based on the immediate service impact and any potential downtime to be incurred will be communicated to the Customer.

Root Volumes: Carbon60 will create a new volume from a previous Snapshot based on the date requested by the customer. After the volume is recovered, the instance will be stopped, the old volume will be replaced by the new volume, and the instance will be restarted. The old volume will be retained until it is no longer needed. This change will require downtime. Alternative recovery methods are available upon request (eg: launch a new Azure VM instance with the recovered volume).

Additional Drives: Carbon60 will create a volume from a previous Snapshot based on the backup date requested by the customer. Carbon60 will remove the volume and replace with the newly created volume or if requested, attach the new volume at a different mount point. The recovery method will be coordinated between Carbon60 and the Customer prior to recovery.

Azure SQL Database Backup

Azure SQL instance backups are taken using the Automated Backup provided by the CSP. These CSP generated backups are made up of an initial full snapshot of the database, with daily incremental snapshots containing changes since the full snapshot was taken. In addition, Azure captures changes to the transaction logs every 5 to 10 minutes, allowing for point-in-time recovery that is more granular than the backup schedule.

The default automated backup retention period is 7 days and can be increased to 35 days at the customer's request. Carbon60 will provide tooling for automating additional SQL backup requirements beyond 35 days that are common for business compliance, these requirements will be established during the onboarding process and additional Azure consumption fees will apply

Azure SQL Database Restore

As part of the service, Carbon60 can perform a restore of the database. Carbon60 will only perform the restore of the database using the CSP generated backups. Carbon60 will only perform the restore as an emergency action, upon agreement with the customer, when the application has become unavailable due to an issue with the database. Carbon60 reserves the right to first investigate and decide if restore is an appropriate action to take. Carbon60 will always take the quickest path to restoring the database.

Restoring an Azure SQL instance will launch a brand-new instance, there is no way to restore or revert an existing instance to a previous state. Once ready for use, the Customer will be able to use the new instance as required. Typically, when the recovery is intended to replace the current, there will need to be a DNS change to point the application server(s) to the recovered database, Carbon60 will assist with the change. The Customer will typically need to restart the application for the new database to enter use.

During this operation, additional maintenance tasks (eg: update of customer's "Infrastructure-as-Code") may be required if Carbon60 was responsible for the initial infrastructure deployment. If requested by the customer, such tasks may be performed by Carbon60.

2.4.6 ENDPOINT PROTECTION

There are 3 tiers of endpoint protection available: Silver, Gold, and Carbon. Silver is the standard tier included in *Managed Cloud for Azure Enhanced* and delivers the following features:

Feature	Details
Managed Antivirus	Carbon60 deploys software that protects against both malware and malware free attacks. It is third-party tested and certified, ensuring confidence that Carbon60 can replace an existing legacy anti-virus (AV) solution.
Endpoint Detection and Response	Carbon60 delivers continuous and comprehensive endpoint visibility across detection, response and forensics, so nothing is missed, and potential breaches can be stopped.
IT Hygiene	Carbon60 identifies unauthorized systems and applications, and alerts in real time to the use of privileged credentials in your environment, enabling faster remediation.
Threat Intelligence	Carbon60 has Integrated threat intelligence into endpoint protection, automating incident investigations and speeding breach response.

Defense-in-depth Approach	Using leading foundational and modern techniques, Intercept X keeps malware at bay, integrating the industry's top-rated malware detection, exploit, and endpoint detection and response.

2.5 INCIDENT MANAGEMENT PROCESS

All incidents raised by the customer will be logged with Carbon60 and will be prioritized based on the following table:

REQUESTS (SLO)			
Priority	**Criteria**	**Response Time**	**Resolution Time**
1 - Urgent	• Urgent Change Requests involving security issues • Application hot fixes to stabilize environment	15 Minutes	4 Hours

2 - Standard	• Standard Change Requests
	  ○ User / Password / Permission Changes
	  ○ DNS / Firewall / Load Balancer Changes
	  ○ System Upgrades / Patching
	  ○ Performance / Security Testing
		1 Hour	24 Hours

3 - Normal	• A request for technical information or advice about the Company's services or procedures • Sales, Billing Questions	24 Hours	5 Days

INCIDENTS (SLO)			
Priority	**Criteria**	**Response Time**	**Resolution Time**
1 - Critical	▪ Production system is malfunctioning and business transactions are failing or significantly degraded	15 Minutes	4 Hours
2 - High	▪ Complete or partial failure of service on a non-production system	30 Minutes	8 Hours
3 - Normal	▪ Minor disruption to the business if the workload is unavailable for a short period of time	1 Hour	3 Days

Carbon60's service desk can be accessed on a 24/7 basis to assist with high and critical incidents relating to the customer cloud platform.

An incident can be logged by the customer or Carbon60 by sending an email to support@carbon60.com while CC'ing all participants who may need to be kept updated of this ticket's status. Alternatively, you can call 1-888-227-2666, Option 1. Our Service desk monitors voicemail messages 24/7/365 so if there is no answer leave detailed voice message as this will auto-create a new ticket.

2.5.1 CUSTOMER RESPONSIBILITIES

When logging an incident, the customer will provide Carbon60 with the following diagnostic information.

- Detailed description of the issue
- If available and reproducible, step by step instructions to reproduce the reported incident
- If available, date and time (and zone) when incident occurred.

Following the logging of an incident, customers need to be available via email or telephone to answer questions and assist the service desk as appropriate.

2.6 ROLES AND RESPONSIBILITIES MATRIX

This Responsibility Matrix describes responsibilities that are included in your Agreement with Carbon60 with respect to *Managed Cloud for Azure* Services and it identifies which party must perform them.

Each party will perform the responsibilities assigned to it in the applicable sections of this Responsibility Matrix.

The following responsibilities in this Section of the Responsibility Matrix apply exclusively to *Managed Cloud for Azure* Services that are specified in a Statement of Work and/or a Service Order.

In the table below, R = *Responsible* and I = *Informed*.

2.6.1 MANAGED CLOUD FOR AZURE ESSENTIALS

PROVISIONING		
Description	**Carbon60**	**Customer**
Design the monitoring parameters based on the Customer Requirements	R	I
Deploy the agreed upon Configuration	R	I
Execute updates to the policies and configuration when a ticket is submitted to Carbon60	R	I

MONITORING & RESPONSE		
Description	**Carbon60**	**Customer**
Monitor the availability of Azure Resources 24x7x365	R	I
Acknowledge, investigate, and notify Customer of events identified	R	I
Before going live, provide detailed guidelines of the desired monitoring and alerting thresholds and the related notification and response procedures	I	R
Before going live, configure monitoring and alerting tools made available by Carbon60 and purchased by Customer and test them for reliability to ensure that they are working properly. Work collaboratively to achieve mutually agreeable functionality of monitors	R	I
Provide up-to-date contact information via our ticketing system for contact authorization, monitoring, alerting and response procedures, including an up-to-date contact distribution list with specific response and escalation instructions for complex contact protocols with numerous parties	I	R
Notify Carbon60 and other non-Carbon60 authorized contacts of any maintenance or other activities that may result in monitoring alerts, including cloud application downtime	I	R

ADMINISTRATION AND SUPPORT		
Description	**Carbon60**	**Customer**
Provide 24x7x365 Service Desk support, including emergencies (e.g. infrastructure down) via telephone and email	R	I
Support and troubleshooting of the Customer's Infrastructure	R	I

2.6.2 Managed Cloud for Azure Enhanced

PROVISIONING		
Description	**Carbon60**	**Customer**
Fully and accurately disclose to Carbon60 in writing or through discovery meetings – all capacity, performance, security, regulatory, backup, high availability, disaster recovery (e.g. RPO and RTO), scalability and other needs for all applications, Content and other software and data that will be used with, stored on or transmitted to the Configuration (collectively, the "Customer Requirements")	I	R
Collaboratively design the Configuration based on the Customer Requirements	R	I
Verify that the Configuration, as specified, is sufficient to meet all Customer Requirements	I	R
Description	**Carbon60**	**Customer**
Provide user keys and configure permissions for Customer administrative user to access and use the Linked Account	R	I
Securely maintain user keys for Customer's administrative user and any additional users	I	R
Maintain redundancy sufficient to meet all Customer Requirements	I	R

MONITORING & RESPONSE		
Description	**Carbon60**	**Customer**
Before going live, provide an accurate and complete description of all Customer-defined response and failover procedures for High Availability cloud Applications	I	R
Before going live, test failover for all High Availability cloud Applications, including all Customer-defined response procedures, for reliability and to ensure they are working properly	R	I
Provide up-to-date contact information via our ticketing system for contact authorization, monitoring, alerting and response procedures, including an up-to-date contact distribution list with specific response and escalation instructions for complex contact protocols with numerous parties	I	R

SECURITY AND PATCHING OF SERVERS		
Description	**Carbon60**	**Customer**
Test security patches within the customer's infrastructure	I	R
Schedule and apply security patches through planned maintenance	R	I
Apply critical security updates (e.g., patches addressing vulnerabilities that allow remote root or Administrator exploits) through announced emergency maintenance	R	I
Manage security groups and implement access changes as requested by authorized Customer contact in writing	R	I

ADMINISTRATION AND SUPPORT		
Description	**Carbon60**	**Customer**
Provide a dedicated Service Delivery Manager	R	I
Provide systems, network, and security administration, which is limited to the following: (1) operating system deployment, maintenance and upgrading; (2) responding to tickets submitted through Carbon60's ticketing system; (3) performing routine network administration and maintenance; (4) systems database administration for databases that are deployed entirely on managed cloud Resources to assist with high availability; and (5) maintaining the ticketing system	R	I
Support and troubleshooting of the Operating System	R	I
Support and troubleshooting of Customer's application	I	R
Request non-emergency (non-production impacting) maintenance 48 hours in advance	I	R
Develop, maintain, and support all Customer applications and other Content, including application components and all required Configuration parameters that need to be part of the deployment process	I	R
Maintain the compatibility of all Customer applications and other Content with O/S versions and version upgrades	I	R

BACKUPS AND RESTORATION		
Description	**Carbon60**	**Customer**
Implement a daily backup/snapshot policy for Customer-specified Servers	R	I
Define custom backup/snapshot policies per business requirements	I	R
Customize backup/snapshot policies per Customer request	R	I
Perform restores as requested by the Customer from available backups/snapshots	R	I

MANAGED APPLICATION, DATABASE, AND STORAGE SERVICES		
Description	**Carbon60**	**Customer**
Provide the requisite licensing information for all Customer-owned applications, including all applications for which Customer has independently obtained use or ownership rights	I	R
Install desired application on the Servers	I	R
Assist Customer in configuring data replication for High Availability cloud applications	R	I
Specify, in writing all custom failover procedures that Carbon60 will follow if a resource that has one or more redundant resources configured in a high availability relationship with it fails	I	R
Before going live, provide an accurate and complete description of all customer-defined response and failover procedures for High Availability cloud applications	I	R
Before going live, configure automated failovers for all High Availability cloud Applications specified in a Build Order within a Region	R	I
Before going live, test failover for all High Availability cloud Applications, including all Customer-defined response procedures, for reliability and to ensure they are working properly. Work collaboratively to achieve mutually agreeable functionality of failover	R, I	R, I
Before going live, configure automated failovers from the primary Region to the secondary Region for all cloud Applications specified on a Build Order with a Remote Failover Solution	R	I
Before going live, test all automated procedures for failing all HA cloud applications with a remote failover solution to a secondary region. Work collaboratively to achieve mutually agreeable functionality of Region-to-Region failover	R, I	R, I
Before going live, develop and provide Carbon60 with a full and accurate description of all manual failover procedures for High Availability cloud Applications that do not have an automated failover capacity	I	R
Upon written request, assist Customer in developing manual failover procedures for High Availability cloud Applications that do not have an automated failover capacity	R	I
Test written manual failover procedures for High Availability cloud Applications that do not have an automated failover capacity prior to going live (making Customer Applications available to end users)	R	I
Work collaboratively to achieve mutually agreeable functionality	R	I
Before going live, develop and provide Carbon60 with a full and accurate description of all manual failover procedures for Remote Failover Solutions that do not have an automated failover capacity	I	R
Upon receipt of a written request from Customer, aid with the development of specified manual failover procedures for Remote Failover Solutions that do not have an automated failover capacity	R	I
Before going live, test all automated procedures for failing all High Availability cloud Applications with a Remote Failover Solution over to a secondary Region. Work collaboratively to achieve mutually agreeable functionality	R	R
Notify Carbon60 of any changes made by Client to the Configuration (e.g. the addition of a managed disk a new database on a database server)	I	R

Description	Carbon60	Customer
Update and test all failover procedures affected by any change made to the Configuration prior to use of the modified portion of the Configuration in a live production environment. Work collaboratively to achieve mutually agreeable functionality	R	I
Notify Carbon60 of any changes in the architecture of the Configuration that may impact high-availability or monitoring and response within 24 hours of making that change (e.g. changing the Servers on which an application runs or integrating an additional Server into the active hosting architecture)	I	R

Carbon60 assumes no responsibility or obligations with respect to customers use of any unmanaged cloud resources.