Synoptek { Managed Azure

TABLE OF CONTENTS

1 INTRODUCTION

This Service Definition is subject to all terms and conditions of the Service Order to which it was attached. This Service Definition describes and contains additional terms that apply to Synoptek's Managed Azure (the "Service") which optionally may also include the re-sale of Azure ("Azure Services").

The service definitions found herein reflect Synoptek standards at the time the Service Order(s) was issued. Synoptek reserves the right to change any standard herein to reflect Synoptek's best practices or industry standards at its sole discretion with or without notice.

2 SERVICE OFFERINGS

Synoptek Managed Azure Cloud Services are designed to maximize the value of Azure public cloud services through pro-active operational, service management and expertise aligned to Information Technology Infrastructure Library (ITIL) frameworks. Companies today are looking to accelerate into the cloud without incurring the challenges and expense of managing it themselves. Some organizations lack the technical know-how or staff to operate cloud infrastructure, tools and applications while others may have the ability but choose to stay focused on their core business. Many larger businesses are on a multi-phased journey to the cloud, requiring transition and management services that can adapt to an evolving environment.

Synoptek provided Managed Azure Services (herein called the "Service Offering") are designed to keep Azure services operational, bundled with expertise to address rapid changes that affect IT operations lifecycle. The Service Offering is available as single offering only and will focus on providing the following:

- Cloud Management Platform & Governance
- Cloud Managed Services
- Service Management
- Security & Compliance
- PaaS Management
- Application Centric
- Disaster Recovery
- Client Engagement

Synoptek Managed Azure Services are delivered in "Service Blocks" which allow flexible consumption of managed services by type of offering you would need – the very same flexibility afforded by different type of Azure cloud services

Cloud Service Blocks:

- **Basic** – a starting point for enabling Azure cloud with basic operations, monitoring, backup, patching, AV and malware.
- **Core** – includes the basic service and adds additional cloud capabilities with increased reporting, change/configuration/problem management, SSO/MFA, RBAC management and PaaS Administration services.
- **Premium**- includes all the services from Basic and Core and adds application monitoring and DRaaS to enable a more resilient cloud ecosystem.

Please see Appendix C for a comparison chart.

2.1 CLOUD MANAGEMENT PLATFORM & GOVERNANCE

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	SERVICE BLOCK(S)
CLOUD MANAGEMENT PLATFORM (CMP) & GOVERNANCE	Synoptek's Cloud Management Platforms (CMP) enables organizations to manage across multi-cloud services and resources. This includes providing governance, security, cost management and automation.	Basic Core Premium

2.2 CLOUD MANAGED SERVICES

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	SERVICE BLOCK(S)
CONTINUOUS RIGHT-SIZING & COST OPTIMIZATION	Synoptek will provide a monthly cost optimization report. • Consumption less than $5K a month will receive a FinOps report. • Consumption greater than $5k a month will receive a monthly review.	Basic Core Premium
24X7X365 MONITORING	Synoptek provides 24x7x365 monitoring, alerting and remediation of performance and availability issues that arise on virtual machines and network centric services running on/in Azure. Available parameters, thresholds and alerts vary based on the operating systems, applications and services being monitored. Should an alert be triggered, or threshold be exceeded, Synoptek will act to remediate. These thresholds are defaults only and may need to be adjusted based on the requirements of your specific environment to avoid too many false positives or to account for higher resource usage. The Customer can optionally designate a lower threshold value to receive direct email notification. By default, Synoptek will provide the following: • Monitor Server storage, CPU and memory to default thresholds at Synoptek pre-defined intervals. This could include contacting Customer if assistance is needed to determine how to resolve. Resolution could include advising for the purchase of additional cloud consumption if necessary. • Monitor up to five Windows services with customizable actions Monitor up to ten custom ports for a positive ping result to ensure custom services are actively running.	Basic Core Premium

OS ADMINISTRATION AND WINDOWS PATCH MANAGEMENT	Synoptek will apply any “Critical” or “Security” updates with a priority level of “Important” and higher for Windows operating system patches and OS Hot Fixes. Synoptek provides patching support for stable and supported Microsoft Windows versions within 90 days of General Availability (“GA”) release. Synoptek will engage “best efforts” support for versions that have exceeded the “End of extended support” date but makes no guarantees of success with best efforts activities. Synoptek will provide Customer with a choice of patching process during on-boarding: 1. Synoptek’s managed patching process for production Windows systems through a designated patching window. 2. Tailored patching schedule contingent upon agreement between Synoptek operations team and Customer. 3. Opt-out to not have Synoptek apply patches on specified subset of servers. By choosing this, customer agrees to take on additional risk associated with security vulnerabilities and functional problems associated with critical bugs. Only critical and security patches are applied, non-core and/or patches that are not critical security updates are not applied. Customer may choose to skip a monthly window if they provide at least 3 days’ notice to Synoptek via email. Synoptek does not apply service packs during this process, but can apply those if requested, through a separate manual process and may incur additional charges. In the event of an issue with a Managed Server, immediately following and as a suspected result of patching, Synoptek will respond as follows: 1. If the Server does not come back online after the Server reboot, then the EOC will notify the Customer and contact a Synoptek Server Engineer to troubleshoot the issue. 2. The EOC will be notified in the event of a service failure after the reboot. The EOC will contact a Server engineer to troubleshoot any core service failures and will escalate to the Customer in the event of an application service issue. In the event of a core OS service outage the Customer will be notified of the issue and notified again after resolution. 3. Synoptek can rollback patches if required. The Customer will be notified in the event that Synoptek must rollback a patch due to a core OS issue. 4. The Customer may submit a ticket to rollback a patch if required to resolve an application issue.	Basic Core Premium

	There are times when a Software Vendor releases a critical patch to address a vulnerability that represents an immediate threat to our Customer's Servers and/or data. Synoptek will notify the Customer of our intention to perform Emergency Patching of all Automatic approved Servers as far as in advance as possible. The Customer will have the option to respond to the notification to stop the Emergency Patching of these Servers otherwise the patching will proceed as scheduled. Customers that manually approve patching will receive notification of the Emergency Patching release along with details of the vulnerability. The notification will also recommend the creation of a ticket to have affected Servers patched immediately.	
LINUX OS PATCH MANAGEMENT	Synoptek will apply "Linux Critical" and "Security Errata" operating system patches and OS Hot Fixes. Synoptek provides patching support for stable and supported Red Hat Enterprise Linux, SuSE Linux Enterprise Server, Ubuntu LTS, CentOS versions within 90 days of General Availability ("GA") release. Synoptek provides best effort support for versions exceeding End of Service Life (EOSL) or equivalent end of patch support by the vendors. Synoptek provides best effort for Linux operating systems not described above. Synoptek will provide Customer with a choice of patching process during on-boarding: 1. Synoptek's managed patching process for production Linux systems through a designated patching window. 2. Tailored patching schedule contingent upon agreement between Synoptek operations team and Customer. 3. Opt-out to not have Synoptek apply patches on specified subset of servers. By choosing this, customer agrees to take on additional risk associated with security vulnerabilities and functional problems associated with critical bugs. Only critical and security patches are applied, non-core and/or patches that are not critical security updates are not applied. Customer may choose to skip a quarterly window if they provide at least 3 days' notice to Synoptek via email. Synoptek does not apply service packs during this process, but can apply those if requested, through a separate manual process and may incur additional charges.	Basic Core Premium (SuSE, Ubuntu, CentOS) Red Hat Patching Requires Additional Add-On

	Customer must provide Synoptek with local administrative rights on Managed Servers. In the event of an issue with a Managed Server, immediately following and as a suspected result of patching, Synoptek will respond as follows: 1. If the Server does not come back online after the Server reboot, then the EOC will notify the Customer and contact a Synoptek Server Engineer to troubleshoot the issue. 2. The EOC will be notified in the event of a service failure after the reboot. The EOC will contact a Server engineer to troubleshoot any core service failures and will escalate to the Customer in the event of an application service issue. In the event of a core OS service outage the Customer will be notified of the issue and notified again after resolution. 3. Synoptek can rollback patches if required. The Customer will be notified in the event that Synoptek must rollback a patch due to a core OS issue. 4. The Customer may submit a ticket to rollback a patch if required to resolve an application issue. There are times when a Software Vendor releases a critical patch to address a vulnerability that represents an immediate threat to our Customer's Servers and/or data. Synoptek will notify the Customer of our intention to perform Emergency Patching of all Automatic approved Servers as far as in advance as possible. The Customer will have the option to respond to the notification to stop the Emergency Patching of these Servers otherwise the patching will proceed as scheduled. Customers that manually approve patching will receive notification of the Emergency Patching release along with details of the vulnerability. The notification will also recommend the creation of a ticket to have affected Servers patched immediately.	
BACKUP & RECOVERY MANAGEMENT	Synoptek helps the client back up critical information on a regular basis and assists with a timely recovery using our proven methodology. The client defines the backup schedules, frequency, and retention period while Synoptek initiates and monitors all backup jobs.	Basic Core Premium
AZURE UNIFIED SUPPORT	The Client must be under the Synoptek CSP to qualify for these Premium Support Plans. This plan includes expedited response times, escalation management, account management, etc.	Core Premium

CLOUD TRUSTED ADVISOR HOURS ($5K + MO CONSUMPTION)	Synoptek Cloud Trusted Advisor evaluates your account to identify ways to optimize your Azure infrastructure, improve security and performance, reduce costs, and monitor service quotas. You can then follow the recommendations to optimize your services and resources.	Core – 4 hrs Prem. – 8 hrs
PROACTIVE PROGRAMS	Block of hours purchased for one-time or reoccurring operational work for proactive maintenance. • Cloud Dedicated Consulting Engineer (DCE) • Cloud DevOps (DCE) • VCISO • Client Advisor A Cloud DCE is a cloud consultant that helps you follow best practices to optimize your public cloud deployments. Analyzes resource configuration and recommends solutions that can help improve reliability, security, cost effectiveness, performance, and operational excellence of Cloud resources. A Cloud DevOps Engineer is responsible for designing, implementing, and maintaining the systems and processes that support the development, testing, and deployment of software and services in a cloud environment. The specific responsibilities of a Cloud DevOps Engineer may vary depending on the specific needs and goals of the organization, but common tasks may include: • Collaborating with development and operations teams to design and implement processes for building, testing, and deploying applications and services in a cloud environment • Using agile methodologies and tools such as continuous integration and delivery (CI/CD) to automate the build, test, and deployment process • Managing and optimizing the performance and availability of cloud-based systems and applications • Implementing and maintaining infrastructure as code (IaC) using tools such as Terraform or Ansible • Collaborating with development and operations teams to improve the efficiency and reliability of the software development and delivery process The vCISO is a consultant who provides strategy, risk & compliance planning, threat & protection guidance, secure design & architecture review, incident response assessment, and tailored security briefings to deliver a custom cloud security advisory plan.	Available as a standalone Add-On

2.3 SERVICE MANAGEMENT

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	INCLUDED
SERVICE MANAGEMENT (INCIDENT & PROBLEM)	Synoptek uses IT service management (ITSM) incident management best practices to restore service, when needed, as quickly as possible 24/7/365. Synoptek will provide the following Incident and Problem Management (e.g., detection, severity classification, recording, escalation, and return to service). After incidents have been addressed, a support engineer will act on support ticket with customer approval. If there is a false alarm – support team mange the alerts resolved based on support metrics. Final closure would be initiate after three consecutive attempts to communicate with end customer over 72 hours or more.	Basic Core Premium
ADVANCED SERVICE MANAGEMENT (CHANGE, AND CONFIGURATION)	Synoptek will provide the following Change & Configuration Management elements: The Client Delivery team would be the first point of contact on all changes to the end customers Azure environment. 1. All change requests will be managed through a support ticket, preferably through a ticketing system. 2. Synoptek will create a ticket for changes that are owned or initiated by end customer. 3. Customers may also have access to the ticketing system to create support tickets whenever any support is required for any changes owned and initiated by the end customer. 4. In addition, the customer may also call our support line and request that a ticket be created. 5. Synoptek will assign the SME / support engineers and perform the change, keeping the customer fully informed on progress and once the maintenance done, ticket close after final confirmation from end customer	Core Premium
ROOT CAUSE ANALYSIS FOR CRITICAL ISSUES	Root cause analysis (RCA) is the process of discovering the root causes of problems in order to identify appropriate solutions. Synoptek will provide a written summary of the root cause analysis within 72 hours for all Priority 1 incidents.	Core Premium

2.4 SECURITY AND COMPLIANCE

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	INCLUDED
ENDPOINT PROTECTION	Synoptek will provision managed VM's with Anti-Virus and Anti-Malware. Synoptek manages daily virus signature updates and managed to our centralized management platform for control and visibility. Should a virus be detected, Customers will be notified. Synoptek will provide assistance in containment and eradication of malware using the appropriate tools and methods necessary. In some circumstances removal of malware may not be possible and Disaster Recovery may be the recommended path to restore availability ASAP. Malware remediation services may incur additional costs.	Basic Core Premium
ENDPOINT THREAT PREVENTION, DETECTION AND RESPONSE (EDR)	Synoptek will provision managed VM's with the ability to prevent suspicious and malicious activity through a combination of advance threat prevention capabilities: • Simulates the presence of sandbox and analysis tools that are considered "hostile" for malware. • Intercepts attempts to inject malicious code into memory for protection against file-less threats • Terminates weaponized files such as VBA scripts, Excel Macros, and PowerShell scripts • Simulates artifacts of infected devices to deceive the malware to think it's already infected the system. • Cloak sensitive files from malware, even in the event of an infection. After a threat is prevented, it is considered detected, then subsequently analyzed for further response (if necessary). Any response needed will be recommended or advised to the Customer. Malware remediation services may incur additional costs.	Basic Core Premium
TENANT MANAGEMENT	Synoptek will manage existing client tenant or configure new client tenant if required.	Basic Core Premium
IDENTIFY COMMON SECURITY GAPS	Synoptek will identify potential security gaps as part our continuous improvement program.	Basic Core Premium

REVIEW RECOMMENDATIONS AND REMEDIATION (WITH CLIENT APPROVAL)	Synoptek will provide key findings and recommendations and will remediate based off client approval.	Core Premium
NATVIE SINGLE SIGN-ON (SSO) AND MFA AUTHENTICATION MANAGEMENT	Manage existing single sign-on (SSO) and MFA configuration.	Core Premium
RBAC MANAGEMENT	Synoptek will segregate access for all remote users (Synoptek and Client) to ensure that the appropriate individuals have the required access to desired data or systems.	Core Premium

2.5 PaaS ADMINISTRATION

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	INCLUDED

NETWORK, FIREWALL, LOAD BALANCER (WAF, FRONTDOOR, APPGATEWAY)	Synoptek will provide ongoing support and management of the following:
	• Updates, rule changes and tuning, troubleshoot and remediation any 3rd party virtual firewall appliance (i.e., Fortinet).
	• Monitor, Troubleshoot and remediate Azure Native services:
	  • Azure Virtual Network
	  • Azure Web Application Firewall
	  • Load Balancers
	• Ongoing administration of native services (App Services, Lambda, AKS, Managed SQL, MySQL, RDS, etc.).
		Core
		Premium

2.6 APPLICATION CENTRIC

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	INCLUDED
APPLICATION MONITORING (AZURE MONITOR)	Synoptek will collect and analyze system log data from client environments by using Azure Monitor by maximizing the	Premium

	performance and availability of the deployed resources and proactively identify problems.	

2.7 DISASTER RECOVERY (DR)

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	INCLUDED
DRAAS (ASR)	Setup and configure Azure Site Recovery between cross regions to replicate workloads running on physical and virtual machines (VMs) from a primary site to a secondary location that helps protect client data from loss or corruption. Site recovery is a disaster recovery solution that helps recover data and applications if client primary Azure region goes down. This service includes continuous management of resources and replication and pre planned annual test requested by the client. Synoptek requires a 30-day lead-time to coordinate and execute the DR test plan. Once the client declares a disaster, Synoptek will execute the DR runbook to failover the identified systems.	Premium

2.8 CLIENT ENGAGEMENT

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	INCLUDED
ACCOUNT MANAGEMENT (CLIENT DELIVERY MANAGER/LEAD)	Client Delivery Manager / Leads will serve as the single point of communication around the delivery of services, providing the following: • Establish and manage relationship with identified Customer contacts. • Coordinate with other business units as agreed, to ensure a unified Synoptek solution. • Service Management Liaison • Lead Operational Reviews regular cadence	Basic Core Premium

	• Monthly / Quarterly Review (Based off Monthly Revenue)	
QUARTERLY/MONTHLY PATCHING, INCIDENT & SLA REPORTING (CDM REPORT – TBR)	The Client Delivery Manager will provide monthly or quarterly reports for incidents, patching, backup and SLAs.	Core Premium

3 SERVICE DEPLOYMENT

Synoptek's Service Deployment team is responsible for the onboarding (installation / configuration of management tools, monitoring requirements, backup policies, etc.) and offboarding of Managed Azure.

3.1 CUSTOMER ACCESS TO AZURE PLATFORM

Self-Service Portal

Synoptek will not limit access to the Native Azure Self-Service Portal ("Console"); the primary interface for access, consumption and management of cloud resources purchased from Azure.

Synoptek will provide access to the Client Ticketing Portal to review help desk tickets upon request.

Synoptek will provide read only access to the AV Customer portal to review Azure protection upon request.

3.2 NETWORK PROVISIONING

Provisioning of VPN, IPSEC Tunneling, IPS/IDS, Firewalls, Load Balancers, ExpressRoute are all handled as part of professional services and not the managed service.

3.3 AZURE ACCOUNT SUBSCRIPTION

Synoptek will setup the Azure account as either Microsoft CSP or PAL/DPOR which may require additional enrollment steps for the Customer admin. The CSP program enables Synoptek to file tickets to Microsoft on the Customer's behalf. The PAL/DPOR program recognizes Synoptek in situations where Synoptek is not the primary owner of Azure Management, but still a significant contributor (i.e., a migration or the main deployment provider)

3.4 API ACCESS

Synoptek will not limit access to the Azure API for programmatic resource management or workload migration.

4 SERVICE SUPPORT

Synoptek will provide support for problems that the Customer reports to assist with adoption of and related to the Service Offerings 24x7x365.

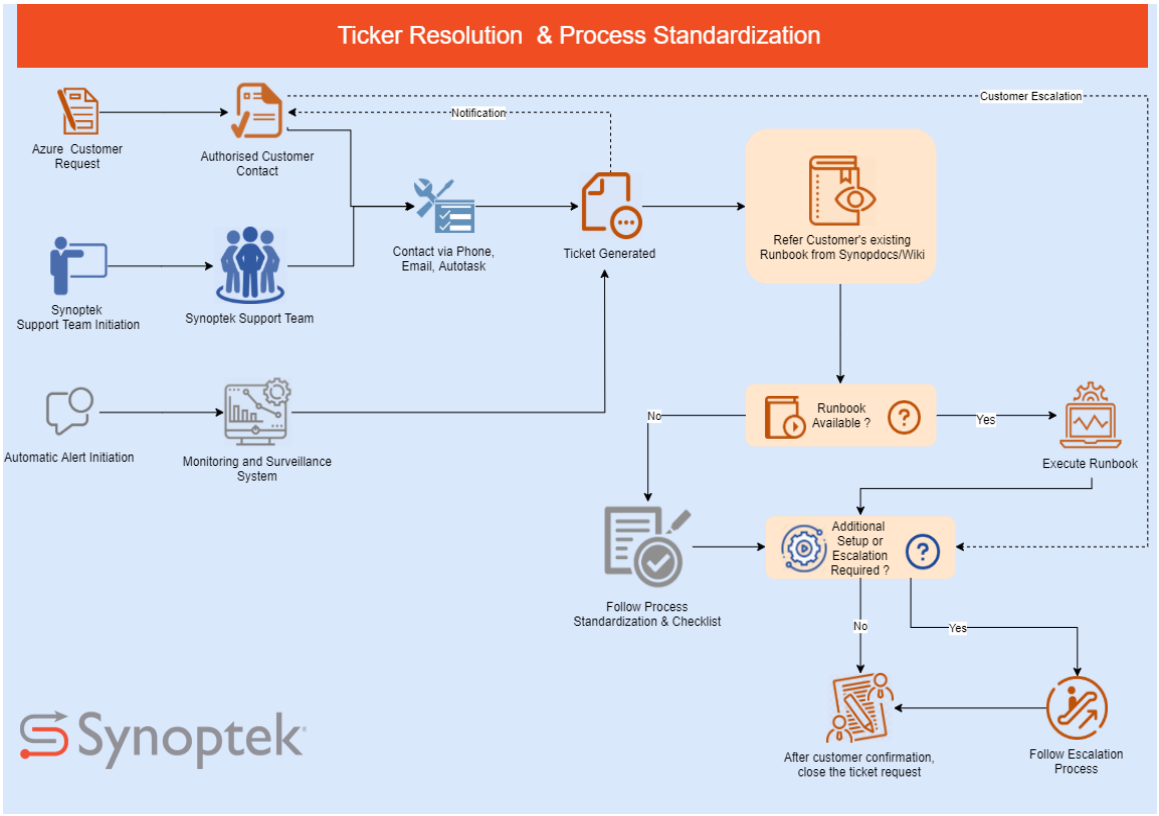
Customer may assign up to 3 named contacts to contact the service desk on behalf of the Customer. The Service Desk is a central point of contact for handling the following Customer issues:

- Email at support@synoptek.com
- Portal at https://wwww.autotask.net/clientportal/

The Service Desk is a central point of contact for handling the following customer issues:

- Incident ownership, initial troubleshooting and escalation of incidents within the defined Service Level Agreement (SLA).
- Respond to “how to” questions such as how to provision or remove cloud instances and migrate data.
- Respond to access issues and requests.
- Access to Azure Certified Solution Architects:
  - Synoptek staffs Azure Certified Solution Architects with the skills and knowledge to provide support to Customers looking for guidance, architectural advice, and best practices where available by opening a ticket or through escalation during normal business hours

Standard Support Request Lifecycle:



4.1 CUSTOMER RESPONSIBILITIES

In order to deliver upon the Services described in this Service Order, the Customer must:

- Mission critical application support is not covered under the Managed Azure agreement, but mission critical support can be provided via a different service offering.
- Procurement of SSL Certifications for website encryption.

SERVICE PROVISIONING	• Provide Azure Admin Portal Account and Virtual Machine Admin login credentials (additional requirements below) • Provide a Letter of Authorization where appropriate • Delegate access to Azure subscriptions and resource groups where Synoptek is not the Azure Admin to the main Azure tenant.
MONITORING, ALERTING & REMEDIATION	• Notify Synoptek of newly created server instances to have the correct monitoring probes setup and configured to deliver the advanced monitoring features. • Notify Synoptek of deleted Service instances to avoid potential false positives. • Provide the necessary credentials with proper access to managed Azure cloud services. • Authorize to purchase additional VM instance and storage to run Synoptek Virtual Edge and monitoring agents. • Authorize to permit SSL/HTTPS outbound connections for Synoptek Virtual Edge and monitoring agents
OS PATCH MANAGEMENT	• Provide local administrative rights to the OS. • Grant necessary support entitlements and genuine licensing for patching. • Approve defined patch schedule.
CIRCUIT & NETWORK MANAGEMENT	• Provide the necessary credentials with proper access. • Provide a Letter of Authorization (for Express Route)
CHANGE MANAGEMENT	• Manage change as it relates to changes to custom or third-party applications, databases, and administration of general network changes within customer control.
SECURITY MANAGEMENT	• Review the predefined security policy • Remediate all failures caused by viruses or malware. Synoptek can assist with locating and removing the virus or malware using the appropriate tools and methods necessary and will do so in a timely manner to minimize all impact to the Customer Service, but these services will incur additional cost
VPN & FIREWALL MANAGEMENT	• Provide the necessary credentials with proper access.

SECURITY BEST PRACTICE CHECK & REMEDIATION	• Provide the necessary credentials with proper access. • Enable or have enabled necessary Azure Service(s) to facilitate information gathering and trending
BACKUP MANAGEMENT	• Purchase any additional Azure storage space to accommodate the necessary snapshots, backups, or data retention requirements.
INCIDENT AND PROBLEM MANAGEMENT	• Manage incident and problems (i.e., detection, severity classification, recording, escalation, and return to service) pertaining to: ○ User-deployed and user-configured assets such custom developed or third-party applications.

4.2 LEGAL TERMS

4.2.1 MICROSOFT AZURE SERVICES AGREEMENT

Customer acknowledges that if Synoptek resells the Azure Services to Customer then Customer's use of those Azure Services is subject to the Microsoft Customer Agreement, a current copy of which is located at: https://docs.microsoft.com/en-us/partner-center/agreements and which shall be effective without signature, and this Agreement. Customer releases Synoptek from any and all liability whatsoever arising out of or in connection with the Azure Services, Microsoft's provision, management or operation of the Azure Services, and Microsoft's exercise of its rights in the Microsoft Customer Agreement or Customer's breach thereof.

4.2.2 RESALE OF MICROSOFT AZURE SERVICES

Azure Services Resale. Synoptek may resell to Customer a subscription for the Azure Services and help Customer to provision Customer's Azure account(s). Settings shall be applied to the Azure account(s) provisioned by Synoptek on Customer's behalf, and Synoptek shall create Customer's Synoptek account. Synoptek shall help Customer provision the Microsoft Azure Services, and such help may include assistance with the following tasks: (i) creating Customer's Microsoft customer account; (ii) verifying Customer's ownership of that account; (iii) provisioning Customer's end user subscriptions on Customer's customer account; and (iv) activating Customer's end user subscriptions

Microsoft Azure Services SLA. The Microsoft Customer Agreement provides a service level agreement from Microsoft to Customer that may be updated periodically by Microsoft. Remedies for service level violations shall be provided by Synoptek for those Azure services Customer purchases directly through Synoptek, provided that Customer must notify Synoptek of any service level requests by the end of the billing cycle in which the service incident occurred. Customer may not go directly to Microsoft with service level inquiries or requests for remedies. Synoptek shall pay any credits owed under the Microsoft Customer Agreement within 60 days of Customer's request to Synoptek for such credits.

4.2.3 SERVICE MANAGEMENT MINIMUM CONSUMPTION

The cloud consumption and managed services fee for Managed Azure services is based on the anticipated quantities, usage, consumption provided by Customer as agreed to in this Service Order. In no event will the anticipated quantities, usage, consumption be reduced by more than twenty percent (20%) of the originally contracted anticipated quantities, usage, consumption during the Term of this Service Order as result of any reduction in scope of Services. In the event Customer's actual quantities, usage, consumption is less than anticipated, Customer agrees to pay at least 80% of the cloud consumption and managed services fee agreed to in this Service Order.

Exceptions to this are Synoptek pre-approved cost optimizations and planned reductions of quantities, usage, consumption, subject to mutually written agreement between the parties.

5 OPTIONAL SERVICES

Synoptek offers a highly complementary Service Portfolio that can augment the value of Azure cloud services. Here is a non-exhaustive highlight of services that pair well with Managed Azure.

FEATURE AND DESCRIPTION:	ADDITIONAL INFO:	INCLUDED
APPLICATION MANAGEMENT - SQL SERVER	Includes monitoring, patching and basic troubleshooting of a Database Server (SQL or MySQL). This includes general server configuration, memory configuration, data and log file management, instant file initialization, temp DB management, database property settings, maintenance job configuration and index job configuration.	Optional – Additional Charges Apply
APPLICATION MANAGEMENT - OFFICE 365	Includes monitoring of the Office 365 tenant, and managing incidents across Exchange Online, Azure ActiveDirectory, and SharePoint Online.	Optional – Additional Charges Apply
DESKTOP AS A SERVICE USING AZURE VIRTUAL DESKTOP	Synoptek will deploy and manage virtual desktops using Azure Virtual Desktop, hosted on Microsoft Azure. Specifically, Synoptek will manage desktop golden images and virtual desktop infrastructure (VDI) in either a Shared Desktop (many users) or Dedicated (single user) model.	Optional – Additional Charges Apply
AZURE MIGRATION	Migration of VMs and data between customer and Azure can be performed using multiple Azure provided methods. • Utilizing Azure Powershell and upload Commands • Azure Site Recovery • Microsoft Virtual Machine Converter • Azure Import / Export Service • MS Azure recommended 3rd Party tools for complex / EOL migration	Optional – Additional Charges Apply

NETWORK ANOMALY DETECTION	Synoptek will manage a network detection appliance with connectors to Azure cloud to monitor all network activity. Synoptek's Network Detection is unique in which it machine learns the network pattern of a company and its users correlating this information in order to detect subtle deviations or anomalies that may indicate potential or active and imminent threats.	Optional – Additional Charges Apply
APPLICATION DEVELOPMENT AND CUSTOM APP SUPPORT	Synoptek will develop, integrate, and manage a Customer's custom application and host it in the Azure cloud (i.e., Azure App Service, or directly on an application platform hosted in Azure IaaS).	Optional – Additional Charges Apply
ANALYTICS AS A SERVICE	Synoptek will provision, integrate, or migrate to a Cloud Data Warehouse to manage a data analytics solution: • PowerBI Dashboards (standalone or on Teams) • Reports • Predictive analytics models • ML/AI models	Optional – Additional Charges Apply
DYNAMICS 365 INTEGRATION, MIGRATION, AND MANAGEMENT	Synoptek will migrate customers from legacy Dynamics CRM/AX to Dynamics 365. Synoptek will integrate application add-ons and modules to Dynamics. Synoptek will manage Dynamics 365 to a custom support scope.	Optional – Additional Charges Apply
VULNERABILITY MANAGEMENT	Synoptek will deploy a scanning agent to subscribed devices that shall, upon scheduled initiation, perform a full vulnerability scan on subscribed device to identify weaknesses inherent in the software or operating system on subscribed device. Customers shall receive a quarterly report of vulnerabilities found. Synoptek will work with Customer admins to ensure that found vulnerabilities are categorized by risk ranking and that vulnerabilities are remediated within the patch management and change management schedule as appropriate.	Cyber Defense Add-On Service
MANAGED DETECTION AND RESPONSE (MDR)	Synoptek's Managed Detection and Response (MDR) provides 24x7 monitoring of security alerts for subscribed cloud servers and networks, as well as proactive security playbook planning and 24x7 containment and mitigation of detected alerts.	Cyber Defense Add-On Service

6 APPENDIX

6.1 Appendix A – Reports

Synoptek can generate reports on-demand for the following at Customer's request.

Reports	Description (examples only)	Pre-generated Report	On Demand Report	Scheduled Report
Instance Inventory Reports	Device details report		X	
	Disk space report		X	
	Virtual Hardware report		X	
	Software report		X	
	Storage report		X	
	Virtualization report		X	
Network Reports	Interface utilization and traffic		X	
Preventive maintenance reports	Azure backup report		X	
	Anti-Virus status report		X	
Service reports (per client)	Application audit report		X	
	Patch Status Report		X	
	Ticket notification and resolution times report		X	
	URL monitoring report (If applicable)		X	

6.2 Appendix C - Comparison Chart: Managed Azure Service Blocks

#	Managed Cloud Services	Basic	Core	Premium
1	**Cloud Management Platform & Governance**	✓	✓	✓
2	**Cloud Managed Services**			
	Continuous right-sizing & cost optimization Report	✓	✓	✓
	24x7x365 Monitoring	✓	✓	✓
	OS Administration, Patch Management, AV & Malware	✓	✓	✓
	Backup and Recovery Management	✓		
	Backup and Recovery Solutions (3rd Party Licenses)		✓	✓
	Unified Support (Azure CSP)		✓	✓
	Cloud Trusted Advisor Hours	-	4	8
3	**Service Management**			
	Service Mgmt. (Incident & Problem)	✓	✓	✓
	Advanced Service Mgmt. (Change & Configuration)	$MAC	✓	✓
	Root cause analysis for critical issues		✓	✓
4	**Security and Compliance**			
	Endpoint Protection and Endpoint Prevention and Response (EDR)	✓	✓	✓
	Subscription/Account Access Management	✓	✓	✓
	Identify common security gaps		✓	✓
	Review, recommendations and remediation	$MAC	✓	✓
	Native Single-Sign-On (SSO) and MFA authentication management		✓	✓
	RBAC management		✓	✓
	Anomaly Detector			✓
5	**PaaS Management**			
	Network, Firewall, Load Balancer		✓	✓
	AppServices, Lambda, AKS, etc.		✓	✓
	Managed SQL, Managed MySQL, RDS		✓	✓
6	**Application Centric**			
	Application Monitoring			✓
	Log Analytics, Application Insights (with client approval)			✓
7	**Disaster Recovery (DR)**			
	DRaaS (ASR)			✓
	Annual DR / Replication Drill			✓
8	**Client Engagement**			
	Account management	✓	✓	✓
	Quarterly/Monthly Patching, incident & SLA Reporting		✓	✓

- $MAC – Additional charge for this item.
- Cloud Migration Service Credits apply to new logos only.