Customer Name:
Date:

Name:

IMSP currently does Provide

IMSP currently does not Provide

Integrated MSP Service Catalog

08/15/2024

Our Services are limited to the following Services

		Service	Includes	Third Party *	Description
		TIER 1 DESKTOP	RMM	NinjaOne or Connectwise	Remote Monitoring Management is used to manage the clients' IT systems, such as servers, desktops, laptops, and software, through locally installed agents.
			Patch management	NinjaOne or Connectwise	Provider will manage Microsoft patches for current Microsoft supported Windows Operating systems. and Microsoft supported Microsoft Office applications. Patches will include security updates, critical updates, definition updates, update roll ups, and service packs. This excludes Microsoft Windows Feature Releases
			Asset Monitoring	NinjaOne or Connectwise	Hardware and software inventories are maintained within the RMM systems. Asset reports are available. Additionally, warranty tracking and reporting for vendors such as Dell and HP can be provided.
			Warranty Status	NinjaOne or Connectwise	Warranty tracking and reporting for vendors such as Dell and HP can be provided when the RMM system is capable of doings so.
		TIER 2 DESKTOP	RMM	NinjaOne or Connectwise	Remote Monitoring Management is used to manage the clients' IT systems, such as servers, desktops, laptops, and software, through locally installed agents.
			Patch management	NinjaOne or Connectwise	Provider will manage Microsoft patches for current Microsoft supported Windows Operating systems. and Microsoft supported Microsoft Office applications. Patches will include security updates, critical updates, definition updates, update roll ups, and service packs. This excludes Microsoft Windows Feature Releases
			Asset Monitoring	NinjaOne or Connectwise	Hardware and software inventories are maintained within the RMM systems. Asset reports are available. Additionally, warranty tracking and reporting for vendors such as Dell and HP can be provided.
			Warranty Status	NinjaOne or Connectwise	Warranty tracking and reporting for vendors such as Dell and HP can be provided when the RMM system is capable of doings so.
			Unlimited Help Desk		Helpdesk is available during normal business hours from 7am to 5pm, Monday through Friday, except during Holidays. Holidays are New Year's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, and Christmas Day. After-Hours Support is available on weekdays 5pm-7am, Holidays and Saturday and Sunday 24 hours a day. After-hours support is intended for critical systems outages. After-hours support has a one-hour call back response time and may incur additional charges as defined by the Order. Help Desk is available to provide phone and remotecontrol support on issues related to the operation and use of supported products.
		TIER 1 SERVER	RMM	NinjaOne or Connectwise	Remote Monitoring Management is used to manage the clients' IT systems, such as servers, desktops, laptops, and software, through locally installed agents.
			Patch management	NinjaOne or Connectwise	Provider will manage Microsoft patches for current Microsoft supported Windows Operating systems. and Microsoft supported Microsoft Office applications. Patches will include security updates, critical updates, definition updates, update roll ups, and service packs. This excludes Microsoft Windows Feature Releases
			Asset Monitoring	NinjaOne or Connectwise	Hardware and software inventories are maintained within the RMM systems. Asset reports are available. Additionally, warranty tracking and reporting for vendors such as Dell and HP can be provided.
			Warranty Status	NinjaOne or Connectwise	Warranty tracking and reporting for vendors such as Dell and HP can be provided when the RMM system is capable of doings so.
		TIER 2 SERVER	RMM	NinjaOne or Connectwise	Remote Monitoring Management is used to manage the clients' IT systems, such as servers, desktops, laptops, and software, through locally installed agents.
			Patch management	NinjaOne or Connectwise	Provider will manage Microsoft patches for current Microsoft supported Windows Operating systems. and Microsoft supported Microsoft Office applications. Patches will include security updates, critical updates, definition updates, update roll ups, and service packs. This excludes Microsoft Windows Feature Releases
			Asset Monitoring	NinjaOne or Connectwise	Hardware and software inventories are maintained within the RMM systems. Asset reports are available. Additionally, warranty tracking and reporting for vendors such as Dell and HP can be provided.
			Warranty Status	NinjaOne or Connectwise	Warranty tracking and reporting for vendors such as Dell and HP can be provided when the RMM system is capable of doings so.
			Unlimited Help Desk		Helpdesk is available during normal business hours from 7am to 5pm, Monday through Friday, except during Holidays. Holidays are New Year's Day, Memorial Day, Independence Day, Labor Day, Thanksgiving Day, and Christmas Day. After-Hours Support is available on weekdays 5pm-7am, Holidays and Saturday and Sunday 24 hours a day. After-hours support is intended for critical systems outages. After-hours support has a one-hour call back response time and may incur additional charges as defined by the Order. Help Desk is available to provide phone and remotecontrol support on issues related to the operation and use of supported products.
		Antivirus	Antivirus	SentinelOne or Webroot or Watchguard EDPR or Microsoft Defender for Business/Endpoints	Provider will provide and manage the Anti-Virus software to ensure virus software is installed and definitions are reasonably up to date. Customer recognizes that this service does not guarantee against infection
		Advanced Security for Endpoints	EDR	Watchguard EPDR or SentinelOne or BlackPoint Cyber or Microsft Defender for Busines/Endpoints	Provider will provide Endpoint Detection and Response (EDR), also referred to as endpoint detection and threat response, is an endpoint security solution that continuously monitors end-user devices to detect and respond to cyber threats like ransomware and malware
		Advanced Security for MS365	MDR	Sherweb or BlackPoint Cyber	Provider will provide Managed Detection and Response (MDR), a security solution to actively defends MS365 cloud workflows and provide contextual alerting for unauthorized logins by gathering contextual anaylysis about the unauthorized use of MS 365 logins
		Security Operations Center	SOC Services	Sentinel One or Connectwise or BlackPoint Cyber or Blumira or Sherweb	SOC services are included with SentinelOne EDR, BlackPoint Cyber MDR, Sherweb Advanced Security for MS365, Blumira SIEM or Connectwise SIEM
		Essentials Complete Email Security	Spam filtering	Barracuda Email Gateway Defense	Provider will manage the Essentials Complete Mail Security cloud based service. The Barracuda Email Security Gateway leverages Barracuda Central to identify email from known spammers and determine whether domains embedded in email lead to known spam or malware domains. Its industry-leading techniques protect against attempts to embed text inside images with the intent of hiding content from traditional spam filters.
			Email Archiving	Barracuda Email Archiving	Retain email communication. Capture an accurate and unmodified copy of each new message at the time it's sent or received and keep it for as long as needed. Reduce storage requirements. Cloud Archiving Service provides unlimited storage per user, reducing the need to store emails on your Exchange Server and in Office 365 mailboxes. Ensure compliance. Meet demanding compliance requirements and address e-discovery requests with tamper-proof archiving and granular retention policies.
			365 Mailbox, OneDrive, SharePoint backups	Barracuda Backup	Easy to use. Find and recover the exact data you want quickly and easily with a newly redesigned user interface that is accessible from anywhere with an internet connection. Flexible, comprehensive Office 365 support. Back up all your Teams, Exchange, SharePoint, and OneDrive data, and choose full or granular restore depending on your specific needs. Cloud native. Your Office 365 data is already in the cloud — saving secure, encrypted backups in the same network means better performance and instant scalability.
			email encryption	Barracuda Email Encryption	If you are sending a sensitive email, you can manually mark it for encryption. However, you can also create a policy to automatically encrypt emails based on their sender, content and other criteria. Encryption policies ensure that your organization complies with regulations designed to protect customer data, such as HIPAA.
		Impersonation Protection	Phishing protection	Barracuda Sentinel	Provider will manage the Barracuda service which can automatically detect and prevent spear-phishing attacks that evade traditional email security systems. Barracuda's AI engine learns each organization's unique communication patterns and leverages these patterns to identify anomalies and quarantine spear-phishing attacks in real time. Barracuda automatically quarantines business email compromise attacks by detecting anomalies in the email header, as well as the content of the email. The AI does not require any manual rules or user setup and can detect any type of BEC attack automatically from day one. Barracuda can detect any type of employee impersonation, including impersonation of executives, as well as mid- and low-level employees. It can detect spoofed emails, typo squatted domains, and impersonation emails sent from free or personal email clients. By discovering anomalous communication patterns within the body of the email, the link, or the email header, Barracuda can stop zero-day phishing attacks that evade other email security systems. It can detect any type of zero-day phishing attacks, including links leading to a fake sign-in page, as well as links to malicious websites. Barracuda has been trained to recognize and automatically quarantine phishing emails that impersonate web services, such as Microsoft Outlook, DocuSign, and Dropbox. The Barracuda AI can prevent web impersonations, even when they use deceptive characters or zero-day links. Barracuda automatically stops attacks that impersonate employees by spoofing their email address. The AI engine recognizes the anomalies in spoofing emails and quarantines them. Barracuda AI can automatically predict which employees are likely to be targeted by spear-phishing attacks, based on their role and their day-to-day access to sensitive information. Customers can report false positives and missed attacks to Barracuda, which are used to retrain the AI classifiers. This enables the AI to continuously improve its precision and adapt its detection capabilities. The raw data from the AI detections can be exported to a CSV file.
		Tenant Management	365 Tenant Management	Simeon Cloud	Provider will work with the customer to manage and deploy agreed upon configurations for O365, Intune, and Entra ID (formerly Azure AD). Establish and maintain baseline configurations. Document and track changes to configurations. Instantly compare an environment to best practices. Dashboards and emails flag drift. Tenant configurations backed-up daily. Deploy consistent security-focused configurations and enforce them.
		Remote Access Audit	Project to review who has Remote access via RDP and VPN capabilities	LionGard	Provider will perform a Project to review who has Remote access via RDP and VPN capabilities
		Privileged Account Audit	Project to review who has privileged accounts in O365, Active Directory, Local computers	LionGard	Provider will perform a Project to review who has privileged accounts in O365, Active Directory, Local computers

		User Account Management	Project to review password policy,admin groups, inactive accounts, inactive computers.	LionGard	Provider will perform a Project to review password policy,admin groups, inactive accounts, inactive computers.
		MFA for Privileged Accounts	MFA product	Cisco DUO or Watchguard AuthPoint	Provider will perform a Project to configure the service designed to ensure that only authorized personnel have access to your powerful privileged account passwords. You need to ensure that only the right people can utilize the powerful privileged account passwords that control access to your systems with sensitive data.
		MFA for Remote Access	MFA product	Cisco DUO or Watchguard AuthPoint	Provider will perform a Project to configure the service designed to protect remote access via Remote Desktop or VPN to corporate networks and business-critical systems.
		MFA for Office 365	Built into O365	Microsoft	Provider will perform a Project to configure the service designed to add an extra layer of security to your Microsoft 365 account sign-in. For example, you first enter your password and, when prompted, you also type a dynamically generated verification code provided by an authenticator app or sent to your phone.
		Microsoft Security PLUS	The Microsoft 365 Security PLUS Plan monitors over 50 different events within the 365 environments to protect from unauthorized access.	SaaS Alerts	Provider will perform a Project to configure the service which includes Independent third-party monitoring of Microsoft 365 Microsoft 365 activity report provided every month. Optimization and continuous monitoring of your Microsoft security score Access to 365 days of event data to help diagnose issues and conduct forensics(Microsoft only provides 30-90 days worth of event data in their own security plans.) Real-time monitoring and remediation of events as they occur Eliminate unnecessary guest user on a monthly basis
		Server Backup BDR	BDR Appliance sync'd offsite -servers only	Datto SIRIS	Provider will manage the service designed to backup and protect the customers data stored on an onpremises server. Security comes first with two-factor authentication and the immutable Datto Cloud to deliver the all-in-one solution for backup and recovery in a ransomware world.
		Server Backup files	File level backups sync'd offsite - servers only	Axcient	Provider will manage the service which is a Software-only data protection featuring local and cloud backup for physical and virtual environments.
		Backup workstations	File level backup of workstations	Carbonite or Microsoft OneDrive	Provider will perform a project to configure the backup of the customer's computer as long as it's connected to the internet. Depending on the customers needs, designated folders will be backed up or OneDrive can backup MyDocuments, My Desktop files, photos, videos, documents, & more.
		Backup Virtual	VM level backup of virtual machines sync'd to Azure blog storage	Veeam and Microsoft Azure	Provider will manage the Veeam Backup & Replication which is a comprehensive enterprise backup solution that protects all workloads, cloud, virtual & physical. Veeam backup jobs can use Azure blog storage as a backup repository which affectively places a copy of the backups into Microsoft Azure where they can be restored as an Azure server for DR purposes.
		Backup Cloud	Azure backup of Servers running in Azure	Microsoft Azure	Provider will manage the Azure Backup service which provides simple, secure, and cost-effective solutions to back up your data (virtual servers in Azure) and recover it from the Microsoft Azure cloud.
		SIEM	Security Incident and Event Monitoring	Blumira SIEM+ or Connectwise Perch	Provider will deploy 3rd party SIEM backed by a Security Operations Center (SOC).
		Firewall as a Service	Firewall hardware, Total Protection Suite licensing, hardware replacement, monitoring, support	Watchguard Firebox	Provider will deploy a firewall appliance that protects private networks from unauthorized users on the Internet. Traffic that enters or leaves the protected networks is examined by the firewall. The firewall denies network traffic that does not match the security criteria or policies. Firewall as a Service includes the appliance, all applicable licenses, and complete management of the firewall.
		Wireless as a Service	Wireless hardware, Hardware replacement, monitoring, support	Ubiquiti or Watchguard	Provider will deploy a Wireless as a Service that combines both infrastructure like access points as well as managed services including monitoring, configuration, hardware replacment, and support.
		Security Awareness Training	Implementation of Security Awareness Training	KnowBe4	AI-powered, new-school security awareness training and simulated phising that allows organizations to drive awareness and change user behavior. This enables you to build on stronger security culture by effectively managing the ongoing problem of social engineering.
		Monthly HelpDesk/Projects/Support Hours	Labor to provide HelpDesk or Onsite support as needed		Provider will install stated services per the Order which will be billed on an hour for hour basis and invoiced at the end of each month.
		Project work	Quoted or hourly project work		Provider will perform Project work as definded on the Order that will be estimated or quoted and invoiced when the project is completed
		Break Fix	Onsite or offsite hourly support		Provider will peform Break Fix support provided on an hourly basis and will be invoiced at the completion of the support incident.
		Email DNS Security	Project to configure SPF, DMARC, DKIM recores to further secure email		Provider will perform a Project to configure SPF, DMARC, DKIM DNS records to further secure email
		Service Installation			Provider will install the product specified on the Order and will bill based on the term of the order
		Vulnerability Scans	Scan network for know vulnerabilities	Nessus	Provider will peform a Project that includes peforming a scan using Nessus which is the de-facto industry standard vulnerability assessment solution for security practitioners. The latest intelligence, rapid updates, an easy-to-use interface.
		Password Manager	Password Manager	LastPass	Provider will provide the Service software which will Improve password hygiene and security, without compromising ease of use for employees or admins. With LastPass to manage your logins, it's easy to have a strong, unique password for every online account and improve your online security.
		Application and Hardware Lifecycle Management	5 year budget		Provider will request that you attend quarterly business reviews where we review a 5 year budget that we maintain for you
		Laptop Encryption	Service to encyrpt laptops	Microsoft Bitlocker	Provider will perform a project to assist the Customer with encrypting their laptops
		Mobile Device Management	MDM solution	Microsoft Intune (Device manger)	Provider will peform a project to implement Microsoft Intune which is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM). You control how your organization's devices are used, including mobile phones, tablets, and laptops. You can also configure specific policies to control applications. For example, you can prevent emails from being sent to people outside your organization. Intune also allows people in your organization to use their personal devices for school or work. On personal devices, Intune helps make sure your organization's data stays protected and can isolate organization data from personal data.
		Email External Source Notification	Project to configure MS365 to put notification at top of email	Microsoft 365	Provider will configure the Customer's 365 tenant to implement an Email External Source Notification
		Disaster Recovery Testing - minimal	File recovery		Provider will peform a Project to Restore some critical files to verify they can be restored
		Disaster Recovery Testing - FULL	Server(s) recovery		Provider will peform a Project to a Full recovery the servers in another environment or on other physical or virtual servers
		Website hosting	Hosting of customer's website	Microsoft Azure or Flywheel	Provider will manage the hosting environment of basic websites or WordPress websites.
		Server Hosting	Hosting of customer virtual server	Microsoft Azure	Provider will manage the hosting environment of Azure resources or Flywheel sites
		Privileged Account Manager	Manage user admin credentials	Cyberfox Autoelevate	Provider will manage the solution using a product, Cyberfox AutoElevate, which is a Privileged Access Management (PAM). Reduce local admin rights and secure clients with AutoElevate Privileged Access Solutions.

*** Third Party - Refer to:**

Schedule of Third-Party Services Attachment – notice of third-party services and waiver of claims.