



Effective May 29, 2024. These Service Descriptions supersede and replace all prior versions.

## Schedule of Services

### **MANAGED SERVICES**

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

**Desktop Monitoring and Management** – Provider will perform desktop monitoring and management including, alert monitoring & management of desktops, prioritization of alerts to identify high-priority incidents, remote remediation services as needed, quarterly configuration backups, quarterly firmware updates as required by manufacturer, and quarterly reporting and performance tuning. The Service Fee does not include hardware replacement or new hardware installations.

**Help Desk Services** – Provider will provide help desk support via client software, client portal, e-mail, and phone. Provider has the ability to remotely control desktops to support employees. Unless otherwise included in an order, all help desk services will include unlimited remote support as required.

**Core Security Services** – Provider will include in its services monthly Microsoft patch management, antivirus software and management, and remote software installations. Core Security Services also includes new / terminated employee setup and configuration.

**Problem Management Services** - Provider will undertake problem monitoring and management as soon as the Provider's monitoring staff becomes aware of an incident. All incidents, with status or resolution, will be documented by posting updates to the Problem (Incident) Ticket Tracking System assigned to Client ("Problem Tickets").

**Asset Management** – Provider will create a report of all monitored devices under management and make it available to client upon request and in a monthly report.

### **MANAGED SECURITY SERVICES**

Provider, through its Third-Party Service Providers will make its best effort to ensure the security of Client's information through third-party security software ("Security Software"). Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this Service is subject to the applicable Third-party Service Providers agreements regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client acknowledges that Third-Party Service Providers and their licensors own all intellectual property rights in and to the Security Software. Client will not engage in or authorize any activity that is inconsistent with such ownership. Client acknowledges and agrees to be bound by any applicable Third-Party Service Provider agreements regarding terms or use or end user licensing terms, and Client understands that

any applicable agreement regarding terms of use or end user licensing is subject to change without notice.

**Intelligent Antivirus** – leverages signature-less anti-malware solution that relies on artificial intelligence to automate malware discovery.

**Anti-virus** - Provider will provide and install anti-virus software of Provider's choosing for each Device covered by the Order. While Provider will make reasonable effort to ensure Client Devices and Client's network are safe from viruses, malware, bugs, hacking, phishing schemes or defective or malicious files, programs or links ("Harmful Content"), of any kind whether now known or hereinafter invented, Provider does not guarantee that Client computers or network cannot be infected by Harmful Content. Where this does happen, Provider will provide commercially reasonable Services to mitigate the Harmful Content. Additional Services will be available upon mutual agreement of the parties.

**Remote Access** - Provider will install remote access and remote monitoring and management software on Client's Devices possibly other equipment at Client's office. Client grants permission to Provider to install any remote access or remote monitoring and management software deemed necessary by Provider.

**APT Blocker** - detects and stops the most sophisticated attacks including ransomware, zero-day threats, and other advanced malware designed to evade traditional network security defenses.

## **CLOUD SERVICES**

**Public Cloud** - Provider will move all Client's data to a cloud computing platform, allow Client to have access to data via virtual desktop from Client's own devices or device provided by Provider, and manage the cloud environment for Client.

**Hybrid Cloud** - Provider will move some of Client's data to a cloud computing platform, and upon Client's request, place a server on premises at Client's location. Any Client data being moved shall be agreed to by the parties in writing prior to moving with specific instructions as to identify which data will be moved, managed or unmanaged by Provider. Any Client data being moved or managed shall be specifically identified as to the location of the data on a particular server. Any Client data not being moved, or that is not specifically identified by Client will be considered not managed. Provider shall not be responsible for the identification, classification, or location of the data. Client is solely responsible for its data up to the outermost point of Provider's firewall with the public internet (the "Demarcation Point"). Once data has been identified, classified, its final location determined, and moved past the Demarcation Point, Provider shall then become responsible for Client data. Provider will also manage the cloud environment for client and provide hardware that will be owned by Provider and will be licensed using an appropriate license agreement.

**Private Cloud or Software Subscriptions** - Provider will maintain all Client's data on premise at Client's location, manage the cloud environment and software subscriptions for Client, provide unmanaged cloud environment and software subscriptions for Client, and provide hardware that will be owned by Provider and will be licensed using an appropriate license agreement.

**Third-Party Cloud & SaaS Vendors** - Provider will provide, install, and support the Third-Party Cloud or software-as-a-service vendors listed on the Order, including but not limited to Microsoft or Google. Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this software is subject to the applicable third-party cloud or software-as-a-service vendor's agreement regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client agrees to be bound by any applicable third-party cloud or software-as-a-service vendor's agreements regarding terms or use or end user licensing, and Client understands that any applicable agreement regarding terms of user or end user licensing is subject to change by any Third-Party vendor or software-as-a-service provider without notice.

### **Optional Additional Services**

**Server Monitoring and Management** – Provider will perform server monitoring and management including, alert monitoring and management of servers, periodic reporting and performance tuning, and prioritization of alerts to identify high-priority incidents. Provider will also perform remote remediation services as needed, and backup software monitoring and management. The Service Fee does not include major hardware / software upgrades or replacements or new server installations.

**On-site Support** - Upon request and subject to the limitations identified in the Order, for Services that are within the scope of this Service Attachment, Provider will also deliver support Services on-site at your location during normal business hours. For on-site support that is not included in the Order, Client, Client will pay Provider's then-prevailing hourly rate.

**Mobile Device Management** – Provider will acquire and will assign licenses to and manage mobile devices using a Third-Party solution (such as but not limited to Phones and Tablets) by Provider on behalf of Client.

**Firewall, Anti-virus, and Intrusion Detection** – Provider can install and configure firewall traffic policies, apply updated firmware when applicable, and configure changes when needed. With respect to the firewall, Provider will include the following:

- Intrusion Prevention - provides real-time protection against network threats, including spyware, SQL injections, cross-site scripting, and buffer overflows.
- URL Filtering - blocks known malicious sites, and delivers granular content and URL filtering tools to block inappropriate content.
- Gateway Antivirus - continuously updated signatures, identify and block known spyware, viruses, trojans, worms, rogware and blended threats – including new variants of known viruses.

### **Security Risk Assessment**

**Malware and Vulnerability Review** – Using one or more tools to determine the existence of malware or vulnerabilities.

**Spam Prevention** - Real-time, continuous, and highly reliable protection from spam and phishing attempts.

**Email Encryption** – The ability for Client to send emails in an encrypted fashion through their designated email provider using a Third-Party provider.

**DNS Filtering** - detects and blocks malicious DNS requests, redirecting users to a safe page with information to reinforce security best practices.

**Client-Side DNS Filtering** - Provider will acquire and will assign an appropriate number of licenses to support the deployment of client-side DNS Filtering on all laptop systems. The DNS filtering is designed to detect and block malicious DNS requests, redirecting users to a safe page with information to reinforce security best practices and to protect laptops while away from the corporate network.

**Employee Activity Tracking** - Provider will acquire and will assign an appropriate number of licenses to assist in monitoring employee activity on their managed devices.

**SAAS Monitoring** – Provider will procure licenses from a Third-Party to monitor the activities of certain cloud Software as a Service solutions. Provider will take action on any alerts generated by this Third-Party Service.

**Dark Web Monitoring** – Provider will acquire through a Third-Party a monitoring service to monitor the Dark Web for credentials leaked in potential data breaches or compromises.

**Employee Password Portal** – Provider will acquire and will assign licenses to a password manager of the Provider's choosing to provide a central location for Client to store passwords and other information.

**Disk Encryption** – Provider will provide the management and monitoring of encryption of disks on Workstations using a Third-Party disk encryption platform.

### **CYBER TRAINING SERVICES**

Provider will implement and managed a managed cybersecurity awareness training platform ordered through a third party on Client's behalf. The program features:

- Enrolling all technology-facing workforce members in the program
- Access to a curriculum of industry-leading cybersecurity awareness education which can be customized to meet the unique needs and regulatory requirements of Client
- Management reporting and visibility into workforce participation and progress in the training
- Lowered risk to (Client) from cyberattacks which target unaware and untrained individuals

## **DATA BACKUP AND DISASTER RECOVERY SERVICE**

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a separate Order including those Services.

**Local Backups** - Using customer or provider provided hardware and software (backup software), backups will be performed on the basis specified in the Order. Client owns the hardware and software agents (backup software) used to perform the backups. If Client subscribes to periodic Server Maintenance, Provider will review the backups during Maintenance and notify Client of backup failures. Client will notify the Provider of any failures, and upon request, perform simple on-site tasks (e.g., powering down and rebooting hardware).

**Remote Backups** - Provider, through its First-Party or Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. Data files are backed up via a third-party client-side desktop/server software application (the "Application"), encrypted, and then sent to a storage server at third-party vendor's data center facility. There is no local copy of the backed-up data. Data files can be restored from the cloud but the server itself cannot be recovered or "booted" in the cloud. Therefore, this service is not considered a disaster recovery solution. All data is backed up via a third-party client-side desktop/server software application (the "Application"). Provider will monitor the backups daily, notify Client of any failures, and work with third-party to resolve backup failures.

**Cloud Backup** - Provider, through its First-Party or Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. Data is backed up via a third-party client-side desktop/server application, encrypted, stored locally on a Provider-owned storage device ("Provider Owned Storage"), and then sent to a third-party owned storage server at the Third-Party Services Provider's data center facility. Provider will monitor the status of all scheduled backup jobs, notify Client of Provider-owned storage failures and corrective actions. Provider will also provide remote administrative services of Data Backup Service as requested by Client. Offsite Backup copies will have one-year retention unless specified in Order. Upon termination of these Services, Provider will request return of the backup hardware and remove the Application from Client systems.

### **Disaster Recovery**

Provider will work with Client to develop a comprehensive disaster-recovery plan that incorporates the Services to be delivered under this Service Attachment.

If Client experiences an event precipitating a major, multi-user loss of data, Client may notify Provider that a data loss event has occurred.

## **FILE BACKUP AND RECOVERY**

Provider will create, monitor, and modify up to the number of file backup jobs listed in the Order. Provider will also notify Client by email of backup drive failures and corrective actions.

Upon request, Provider will remotely restore files, subject to the number of operations listed in the Order

**Fractional/Virtual Chief Information Officer (CIO)** - Provider will assign a technical team member to be available as a consultant to Client. The Fractional and or Virtual CIO will provide ongoing reporting and be available for ongoing meetings to discuss the overall technology

posture aligned to Client goals. The Fractional and or Virtual CIO will assist in managing Provider's team and documentation so that Provider may support Client to the best of their abilities.

**THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY  
TIME WITHOUT NOTICE.**