



Effective August 22, 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.

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.

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 portal, e-mail, and phone when Client creates a ticket by contacting Provider directly through the help desk via e-mail or 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.

Help Desk Incident Prioritization & Level Criteria

Help Desk incident prioritization is based upon the following:

- Urgency – an assessment of the speed with which the Incident requires resolution.
- Impact – reflects the likely effect the Incident will have on the business service.

Urgency levels will be determined by the Help Desk agent, and is defined as per the table below:

Priority	Definition
Level 1 (critical)	Has a significant adverse impact on the delivery of service to many sites. <ul style="list-style-type: none">• May cause significant financial loss and/or disruption.• May result in any material loss or corruption of client data.

Level 2 (critical)	Has a moderate adverse impact on the delivery of service to many sites. <ul style="list-style-type: none"> • May cause a financial loss and/or disruption to the Client that is more than trivial, but less severe than the significant adverse impact described in the definition of an Urgency Level 1 Incident.
Level 3	Has a moderate adverse impact upon the delivery of service to a small (i.e., 1 or more) or moderate number of sites.
Level 4	Has a minor adverse impact upon the delivery of service to a small number of sites.
Level 5	Has no impact upon the delivery of service

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.

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 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").

Cloud Protect Spam Filtering Ultimate Access

GB Tech will provide Ultimate Access email protection services to its clients. This hosted service is provided 24/7/365 and protects email accounts from viruses, spam, and email phishing/spear-phishing. This solution scans email, inbound and outbound, for malware, viruses or malicious links. All URLs are tested in a virtual sandbox before being allowed into the user's inbox. All attachments are scanned and checked before being allowed into user's inbox. This solution also blocks malicious email from being sent from your domain.

Phishing & Spear Phishing Protection

GB Tech's anti-phishing protection bundle collects email threat data and alerts from different sources, where incident analysis and triage can be performed automatically leveraging a combination of human and machine power to help define, prioritize and drive standardized incident response activities according to a standard workflow, making it quick and easy for security analysts to classify reported email incidents. Phishing threat intelligence delivers real-time, human verified, actionable phishing

campaign intelligence collaborated on by top security experts within the security community. This solution allows us to remove phishing emails from all users with one click in the central console.

Vendor Management

GB Tech aims to provide a turn-key solution for Client. Part of that turn-key solution requires IT Vendor Management. GB Tech's Vendor Management service provides Client one single point of contact for all IT related issues. GB Tech will manage the relationship and service issues for Client. Examples of the types of vendors we manage include, but are not limited to; internet service providers (ISPs), telephony system vendors, print service vendors, software vendors that require user connectivity, etc. By having this service available it allows Client to focus on running their business rather than chasing down vendors and wasting time sitting on hold to get a resolution.

Virtual Chief Information Officer (vCIO) Services

The mission of GB Tech's vCIO Service is to save your organization both time & money by using technology to achieve your business goals. Their sole responsibility is to make sure that your organization has what it needs currently, while working with your team to plan for the future. These services include but are not limited to:

- IT strategy & planning sessions
- Regularly scheduled meetings to ensure your organization is conforming to the strategic plan
- Layout a technology roadmap
- Plan and budget your technology needs for the next six – eighteen months out

Mobile Device Management

GB Tech will manage Client's MDM program and create policies around Bring Your Own Device (BYOD). BYOD is growing exponentially, and employers need a way to protect their data. In an MDM program, employees can receive a dedicated work device, such as laptops or smartphones, or have a personal device remotely enrolled. Personal devices receive role-based access to enterprise data and email, a secure VPN, password-protected applications, and other MDM software for optimal data security. MDM software can then monitor the behaviors and business-critical data on enrolled devices. And with more sophisticated MDM solutions, they can be analyzed by machine learning and AI. These tools ensure devices are kept safe from malware and other cyberthreats

MANAGED SECURITY SERVICES

Provider, through its Third-Party Services 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.

Firewall, Anti-malware, and Intrusion Detection – Subject to the services listed in the Order, Provider will 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 – Subject to the services listed in the Order, Provider will perform the following:

- Malware and Vulnerability Review – Using one or more tools to determine the existence of malware or vulnerabilities.
- Personally Identifiable Information (“PII”) – Review practices related to PII, including location, treatment, and risk mitigation.
- Report – Provider’s findings will be included in a Risk Assessment Report.

Network Discovery - generates a visual map of all nodes on your network, making it easy to see where you may be at risk.

Reputation-Based Threat Prevention - Cloud-based web reputation service that aggregates data from multiple feeds to provide real-time protection from malicious sites and botnets, while dramatically improving web processing overhead.

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

Application Control – Provides the ability to allow, block, or restrict access to applications based on a user’s department, job function, and time of day.

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.

Data Loss Prevention – works to enforce compliance by scanning text and files to detect sensitive information attempting to exit your network, whether it is transferred via email, web, or FTP.

Threat Detection & Response - Security data collected from the firewall is correlated by enterprise-grade threat intelligence to detect, prioritize and enable immediate action against malware attack.

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

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

Anti-malware - Provider will provide and install anti-malware 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.

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.

Security Awareness Training & Phishing Simulations - Provider will acquire and will assign an appropriate number of licenses to support the client environment. The Service will schedule phishing campaigns to send at random times during a specified period. The campaigns are trackable and fully customizable designed to keep track of every user's participation, making all cybersecurity education accountable and measurable.

Dark Web Monitoring - By utilizing our Dark Web Scanning tools, a combination of human and sophisticated Dark Web intelligence with search capabilities, we can identify, analyze and proactively monitor for your organization's compromised or stolen employee and client data. Our tool connects to multiple Dark Web services including Tor, I2P and Freenet, to search for compromised credentials, without requiring you to connect to these high-risk services directly. Provides intelligent awareness of compromised credentials before breaches occur.

Client Portal - The cloud portal allows for anyone in your organization to check the status of their tickets as well as indulge in training for Microsoft Office. For users recognized as Administrators is provides much, much more. Administrators will have access to see the status of all tickets in your environment, number of endpoints that we are managing, the age of the computers and servers we are managing, access to reports; including security, backup, and compliance reports, and access to invoices and quote sent to you by our team. It is truly a one-stop shop for full visibility into the environment.

Multi-Factor Authentication Services / Password Credential Management Services – Provider will configure two-factor authentication for compatible software applications, institute single sign-on services for compatible software applications and customized security policies and procedures. After performing a security assessment and assessing the state of Client's existing policies and procedures pertaining to network security (if any), Provider will work with Client to prepare a new or revised set of policies and procedures that incorporate best practices and that take advantage of the other Services delivered by Provider.

Security Operations Center – Subject to the services listed in the Order, the Services include:

- Advanced Malware Protection supported by Security Operations Center (SOC).
- Deployment of advanced malware protection applications to all Windows based devices on customer network.
- 24x7 SOC service analyzes quarantined applications and files, reducing false positives.
- Immediate risk identification – Provides rapid recognition of thousands of viruses and malware attack variants, including cryptomining attacks, as well as the root causes of these malicious behaviors, by quickly identifying and diagnosing corrupt source processes and system settings.
- Ransomware rollback - quickly rollback files to previous safe versions through tracking changes in your devices and restoring them to an acceptable risk state.

Security Log Management – With the purchase of the advanced security package, Provider will configure log sources to capture and retain information without creating excessive logging, limit user access to log files, avoid logging sensitive or protected information, secure the processes that generate logs, identify and resolve logging errors, and analyze log entries, prioritize entries, and respond to those requiring action. Standard packages do not include this service.

Security Incident Event Management (SIEM) Services supported by SOC – With the purchase of the advanced security package, Provider will deploy SIEM monitoring probes to monitor all critical network devices including; domain controller, firewalls, network switches and routers. When meeting compliance requirement deployment will include all Windows devices as well. Standard security packages do not include this service.

Incident Response - Provider will assist Client in the hours immediately following a data breach to identify the likely source of the breach and to begin formulating an appropriate response to the breach. However, any assistance with data breach-remediation efforts – including but not limited to breach-notification planning, initial and subsequent in-depth forensic examinations of the source of a breach, and significant, post-breach systems reconfiguration – are not within the scope of this Service Attachment. If Client requests Provider's assistance with such activities, Provider will prepare a separate Service Attachment for Project Services that will specify what the charges will be for such assistance.

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 – Client must use provider-supplied hardware and software to perform the backups.

Cloud Backup - Provider, through its Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. 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.

Software as a Service (SaaS) Backup – Provider will use third-party tools to backup certain Office 365 data.

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 must notify Provider that a data loss event has occurred.

If Client's insurance company approves, Provider may assist Client in the hours immediately following a multi-user loss of data to identify the likely source and to begin formulating an appropriate response. However, any assistance with disaster recovery past the first twenty-four (24) hours following the incident – including but not limited to notification planning, examinations of the source of the incident, and significant, systems reconfiguration – are not within the scope of this Service Attachment. If Client requests Provider's assistance with such activities, Provider will prepare a separate Service Attachment for Project Services that will specify what the charges will be for such assistance.

CLOUD AND HOSTING 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. 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.

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
- Regular campaigns to test each workforce member's ability to recognize and effectively respond to cyberattacks which typically target individuals
- Automated enrollment in remedial training for individual workforce members, when appropriate
- Management reporting and visibility into workforce performance on testing campaigns
- Management reporting and visibility into the improvement in workforce awareness and performance over time
- Lowered risk to (Client) from cyberattacks which target unaware and untrained individuals

**Provider does not provide internet connection. Client is responsible for providing internet connection to use the Service.

THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY TIME WITHOUT NOTICE.