



Effective May 26, 2025. 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.

SAAS BACKUP	Comprehensive backup solution for Microsoft 365 with unlimited data retention.
CLOUD CONTINUITY FOR PCS	Cloud-based backup and recovery service for individual computers.
CLOUD CONTINUITY FOR ENDPOINT - SERVER	Cloud-based backup and recovery service for server endpoints.
DRIVE ENCRYPTION	Encryption service for protecting data stored on hard drives on Windows machines.
DARK WEB MONITORING	Continuous monitoring of the dark web for compromised credentials.
END USER SECURITY TRAINING	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.
MANAGED ENDPOINT DETECTION AND RESPONSE WITH SOC SERVICES	Security for all endpoint devices, minimizing risks of malware, ransomware, and other cyber threats. Integrated Security Operations Center (SOC) support offers real-time monitoring and incident response, leveraging advanced threat intelligence and analytics to detect and mitigate security incidents.

MOBILE DEVICE MANAGEMENT	Provider will manage handheld mobile devices (primarily smartphones and media tablets). This may include PC cards, pagers, notebooks and other mobile devices.
2 FACTOR AUTHENTICATION	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 cutting edge best practices and that take advantage of the other Services delivered by Provider. We protect 365 as a standard - endpoints, VPN, and compatible applications are add-ons.
MANAGED SECURITY INFORMATION & EVENT MANAGEMENT WITH SOC SERVICES	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.
SIEM APPLIANCE MONTHLY MAINTENANCE	Monthly maintenance for SIEM physical security appliances
WK SECURE: ZERO TRUST ENDPOINT PROTECTION	Provides the ability to restrict applications except for those explicitly allowed to run in the environment.
EMAIL PROTECTION	Email security and spam prevention.
SAAS PROTECTION	Advanced monitoring and security for SaaS platforms.

ANTI VIRUS MANAGEMENT	Provides advanced, real-time protection against malware, ransomware, and other online threats – improving the security of your devices and data.
AZURE MANAGEMENT FEE	Monthly fee for managing cloud services.
EMAIL FILTERING MANAGEMENT	Provider will manage the client's email filtering platform, including the management of block lists and allow lists, and releasing messages from quarantine. Transformational changes or re-architecture of platform or policies may qualify as project work and additional fees.
MANAGED DEVICE (applies to additional devices on the Order)	Provider will provide help desk support via 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.
REMOTE MONITORING & MANAGEMENT	Provider will perform remote 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.
TECHNICAL USER ACCOUNT	Includes access to RMM, ticketing platform, and password management tool
TECHNICAL USER ACCOUNT LITE	Includes access to RMM, ticketing platform, and read-only access to password management tool
EMAIL SIGNATURE - MONTHLY SUBSCRIPTION	Subscription service for managing email signatures via cloud platform.
FEATURE-CONFBRIDGE	Multiple on-site, outside callers can simultaneously participate in password protected conference calls. Callers can be assigned talk-listen or listen only access.
UN128R_0.97	Administrative Surcharge
AUTOATTENDANT_4.1	Auto Attendant

CALLRECORD-DEVICE	Call Recording License for 1 Device User. Inbound, Outbound, and Dynamic
CALLRECORD-VPATH	Call Recording License for 1 Call Path. Inbound, Outbound, and Dynamic
CLOUDBXFAFAXLINE_7.79	Cloud PBX Fax Line
CONTACT-CNTR-AGENT	License for 1 Contact Center Agent
CONTACT-CNTR-SPRVSR	License for 1 Contact Center Supervisor with realtime monitor and reporting
GT300RC1	CYBERPOWER GT300RC1 - POWER STRIP - 1875 WATT
MH3021P	Dell Mobile Adapter Speakerphone 1/2 MH3021P
Desktop add on	Desktop Add On - Boomea
E911-ADDL	Enhanced 911 (E911) associates a phone number and physical address with the calling party's telephone extension
E911 Primary	Enhanced 911 (E911) associates a phone number and physical address with the calling party's telephone extension
EDGEVIEW-MANAGEMENT	EDGEVIEW MANAGEMENT (MONTHLY RECURRING)
FAX-ATA-HTTPS	Fax ATA over HTTPS, unlimited fax pages
FAX-EMAIL-IN	Fax to Email - Inbound Only (\$.05 per page)
FAX-EMAIL-IN-OUT	Fax to Email - Inbound and Outbound (\$.05 per page)
GRA-HT812	Supports 2 FXS ports for analog devices GRA-HT812
HPBXDEVICE-ADDL	Additional Device/Mobile App License. Add-on to Full User Seat only
JAB-6593-829-409	JABRA EVOLVE 65 UC MONO, HEADSET
MEETING-ENTERPRISE	MEETING ENTERPRISE -VIDEO & COLLAB/SCREEN SHARE
MEETING-LITE	MEETING LITE -VIDEO & COLLABORATION/SCREEN SHARE
MEETING-PROFESSIONAL	MEETING PROFESSIONAL-VIDEO & COLLAB/SCREEN SHARE
Mobilityaddon	Additional Mobile App License. Add-on to Full User Seat only
GS316EPP-100NAS	NETGEAR 16 PORT PoE+ GIGABIT ETHERNET PLUS SWITCH
GS105E-200NAS	NETGEAR 5 PORT PROSAFE PLUS SWITCH 5 x 10/100/1000Base-T No PoE+

Remote Call Forward	Remote Call Forward
SMSTEXT-MOBILE-APP	SMS TEXTING FROM MOBILE APP
TN-DOMESTIC-CID	Telephone Number and/or Direct Inward Dial (DID) with caller ID name
PPM-TFN -1500	Additional Domestic (US/Canada) usage billed at 2.5 cents per minute.
PPM-TFN -2500	Additional Domestic (US/Canada) usage billed at 2 cents per minute.
PPM-TFN -500	Additional Domestic (US/Canada) usage billed at 3 cents per minute.
TFN-CID	Toll Free telephone number with caller ID name. Inbound toll calls are billed at 5 cents per minute.
UV-ENTERPRISE-USER	Enterprise user license includes 2 device licenses, 1 mobile license, virtual trunk, domestic unlimited local and LD calling, domestic telephone number with CID, voicemail box, voicemail to email, find me follow me, personal conference bridge, fax to email (inbound only), UC desktop with chat / visual voicemail / call log / station presence.
UV-STANDARD-USER	Standard user license includes: device license, virtual trunk, domestic telephone number with CID, domestic unlimited local and LD calling, voicemail box, UC desktop with chat, visual voicemail, call log, station presence.
UV-PREM-MOBILE-USER	Premium/Mobility user license includes 1 device license, 1 mobile license, virtual trunk, domestic unlimited local and LD calling, domestic telephone number with CID, voicemail box, voicemail to email, find me follow me, UC desktop with chat, visual voicemail, call log, station presence.
UV-UTILITY-USER	Utility User Device License. Used for Page Adapters and Courtesy Phones and low speed/use modems.
UV-Limited Use Extension	Limited Use Extension license includes: device license, virtual trunk, domestic telephone number with CID, domestic unlimited local and LD calling, voicemail box, UC desktop with chat, visual voicemail, call log, station presence.
HPBXVIREXT	Virtual extension can be used for global speed dial and/or a quick way to route to: devices, groups, menus, timeframes, voicemails, etc.

VT-HST-UNLIMITED	Includes 1 concurrent PSTN call path and unlimited domestic minutes
VT-PBX-UNLIMITED	Includes 1 concurrent PSTN call path and unlimited domestic minutes
VT- Hosted Metered	Includes 1 concurrent PSTN call path and 50 domestic minutes with each Virtual Trunk. Minutes are billed at our current per minute rate.
FEATURE-VMBOX	Voicemail boxes for Device Users
VoIP LABOR	VoIP PROJECT LABOR

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 – During business hours, Provider will provide help desk support via 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.

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.

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").

Mobile Device Management – Provider manage handheld mobile devices (primarily smartphones and media tablets). This may include PC cards, pagers, notebooks and other mobile devices.

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 – Provider will install and configure of 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, rogueware 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.
- 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.

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 provider 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 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 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

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.

VOIP AND COLLABORATION SERVICES

Provider will deliver the Voice over Internet Protocol ("VoIP") and associated telephony and collaboration services specified and selected by you on the Order or Proposal. Additional Services may be added only by entering into a new Order including those Services.

The VoIP Services may be provided or delivered by Provider through the use of third-party vendors listed on the Order or Proposal. Use of the VoIP Services are subject to any applicable third-party vendor agreements. Client acknowledges and agrees to be bound by those third-party vendor agreements. Provider shall not be responsible for any third-party vendor service failures when accessing or using the Services. Client agrees to be bound by any applicable third-party vendor's agreements regarding terms and conditions or end user licensing, and Client understands that any applicable agreement regarding terms and conditions or end user licensing is subject to change by any third-party vendor without notice.

Network cabling, conduit, electrical, rack space, and any other required construction or trenching are additional charges are not included with the Service.

****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.**