



Effective December 13, 2024. These Service Descriptions supersede and replace all prior versions.

Schedule of Services

MANAGED SUPPORT LEVELS

Definition: Support can only be provided to things already in the environment (i.e., People, Computers, Devices, Software, Subscriptions, Accounts). Anything new must be implemented as a Project to be enabled into the environment.

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.

CORE SUPPORT (per Device Support)

Core Support is restricted to the named Devices identified for this program.

- To enable Core Support, a computer must be configured and installed with Provider software tools (On-Boarding).
- Core Support provides a set of automated services, updates, optimization, protection, and remote tools for support, and changes based on the discretion of the Provider.
 - Tools include Remote Management and Monitoring, Antivirus, AntiMalware, Web DNS filter, Security Operations Center (SOC)
- All support requiring a technician is billable at the contracted rate and thus requires authorization before any work is performed.
- Client shall have unlimited access to Provider technical Help Desk service during Provider Business Hours for the purpose of reporting System or Equipment failures, software issues or general how-to type questions and requesting services.
- Provider will provide help desk support via 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.
- Support calls for Core Support computers are treated with normal priority, with non-major malfunctions responded to within two (2) business days after notification, during Provider Business Hours.
- One (1) time per month, Provider performs scheduled automated software patches and updates for licensed software.
- 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.

BASIC SUPPORT (per Device Support)

Basic Support includes the features listed for Core Support, plus:

- Basic Support minimum requires a minimum of 10 named Devices.
- Includes a LIMITED hours of technician labor per month based on the number of devices.
- Support requiring a technician beyond the monthly limit is billable at the contracted rate.
- All support requests requires authorization before any work is performed.

STANDARD SUPPORT (per Device Support):

Standard Support includes the features listed for Basic Support, plus:

- Includes technician labor for included Devices on Standard Support.
- Support calls for Standard Support Devices are treated with high priority, with non-major malfunctions responded to within one (1) business day after notification, during Provider Business Hours.
- Provider shall respond to major system failure within one (1) hour after notification during Provider Business Hours. Major system failures are defined as any failure resulting in complete lack of access to the system by ALL personnel and resulting in a work stoppage.
- If in Provider's determination, an on-site maintenance visit is required, and if Client is in an approved distance from Provider's Office, Standard Support includes one visit per month at no additional charge.

PREMIUM SUPPORT (per Employee Support):

Premium Support includes the features of Core Support for up to 5 company-provided Devices that the EMPLOYEE uses, including Office Computers, Home Computers, Smart Phones, and Tablets.

Premium Support must include all Employees that use company-provided computers.

- Includes technician labor for named Employees on Premium Support.
- Support calls for Premium Support Employees are treated with highest priority, with non-major malfunctions responded to within half (½) business day after notification, during Provider Business Hours.
- Provider shall provide support services for Premium Support Employees on non-Microsoft Windows OS devices to the limit of connecting to company-provided devices and services. (e.g. phone to email, tablet to file sync, camera to laptop)
- If in Provider's determination, an on-site maintenance visit is required, and if Client is in an approved distance from Provider's Office, Premium Support includes one visit per month at no additional charge.

SITE SUPPORT (per Location):

Site Support provides services for Infrastructure Devices including routers, firewalls, switches, wireless access points, printers, and scanners.

- Secures network access for Network Appliances, Security Cameras, HVAC, and Phone Systems that are generally supported by an external system vendor. Active support contracts must be maintained for these systems.
- Device Updates are applied as required by the device manufacturer to maintain security.
- Internet based services require a 300mbps download and 20mbps upload or higher speeds for proper service functions of Internet based services including Cloud Backup & Storage, Cloud File Storage, Cloud Email, Cloud or Remote Applications.

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.

Intelligent Antivirus & Anti-malware - The provider will acquire and assign an appropriate number of licenses to support the client environment and install antivirus and 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.

WEB DNS Filtering - The provider will acquire and assign an appropriate number of licenses to support the client environment that blocks access to harmful or inappropriate websites at the Domain Name System (DNS) level. It works by using a list of known malicious or unwanted domains and preventing devices from accessing them. This helps protect networks from threats like malware, phishing attacks, and other malicious activities. It controls access to certain types of websites, such as social media or adult content, based on company policies.

Security Operations Center (SOC) The provider will acquire and assign an appropriate number of licenses to support the client environment that enables the 24x7 SOC service. The service analyzes quarantined applications and files, reducing false positives. It provides immediate risk identification by rapidly recognizing thousands of viruses and malware attack variants, including cryptomining attacks, and diagnosing the root causes of these malicious behaviors by identifying corrupt source processes and system settings. Additionally, the SOC offers ransomware rollback, which quickly restores files to previous safe versions by tracking changes in devices and returning them to an acceptable risk state.

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 past the first twenty-four (24) hours following a breach – including but not limited to breach-notification planning, 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.

OPTIONAL ADVANCED CYBER PROTECTIONS

IntelliShield: Intelligent Firewall Router Equipment and Cloud Service.

Provider will acquire the intelligent firewall device and the appropriate number of licenses to support the client environment. The service provides the configuration, periodic updates, and user requested penetrations to maximize the security for the client environment. The firewall service provides proactive defense by deep interrogation of data packets in and out-going from the client environment to alert and stop malicious virus, trojans and malware from entering or leaving the network.

Client is responsible for replacement costs for the loss of the device due to theft, fire, water, or misuse by Client or their employees. This includes equipment or software failure not caused by Provider. Additionally, the failure of the insurance company to honor a claim does not change the obligation of Client to compensate Provider for the full new replacement value of the equipment. The Client is also responsible for labor costs that are not related to the normal working of the system, such as the relocation of equipment, removing trash, and cleaning the equipment area. Furthermore, equipment failure resulting from site environments that do not meet manufacturer specifications, such as heat and moisture, is also the responsibility of Client. Upon termination of these Services, Client will allow removal from the client environment. Provider shall erase all Client related data from the devices within 30 days.

PhishGuard: Email Threat Intelligence - Using advanced AI technology to detect sophisticated email spoofing and phishing attacks. The provider will acquire and assign an appropriate number of licenses to support the client environment. The service blocks phishing emails by stopping harmful messages that pretend to be from trusted contacts and protects against ransomware and malware, preventing dangerous software from reaching employees. It also prevents Business Email Compromise (BEC) by stopping cybercriminals from taking over business email accounts and guards against Account Takeover (ATO) to protect accounts from unauthorized access. Additionally, the service prevents credential theft, keeping login details and sensitive information safe, enhances email security by adding extra protection to Google Workspace and Microsoft 365, and feeds into the Security Operations Center (SOC) to provide data for proactive monitoring and threat detection.

CloudGuard: Automated Email Defense - Automatic cloud email security threat detection and response. The provider will acquire and assign an appropriate number of licenses to support the client environment. The service exposes advanced threats by identifying sophisticated security threats in cloud environments and takes immediate action to swiftly neutralize detected threats while proactively addressing potential ones. It efficiently manages end-user behavior by monitoring and preventing risky activities. The service also offers a proactive threat response to

address potential threats before they escalate, reinforces user identity by strengthening identity verification processes, and protects business tools integrated with Microsoft 365. Additionally, it provides detailed reporting to prevent future incidents.

DarkCanary: Stealth Threat Defense - 24/7 Comprehensive credential monitoring on darkweb botnets, criminal chat rooms, blogs, websites, and black-market sites for stolen information. The provider will acquire and assign an appropriate number of licenses to support the client environment. The service provides immediate alerts to notify you of potential issues. It includes threat detection and mitigation, identifying and addressing cyber threats that use stolen credentials. Additionally, it offers credential change assistance to help update business credentials found on the dark web. The service also includes discussions on account and password health, reviewing and improving account security practices.

PhishPulse: Regular Email Security Drills - Periodic email phishing simulations and security awareness training. The provider will acquire and assign an appropriate number of licenses to support the client environment. The service will schedule email phishing simulations to be sent at random times during a specified period. These campaigns are trackable and fully customizable, designed to monitor every user's participation, making all cybersecurity education accountable and measurable. The service includes security awareness training to educate employees on identifying and stopping phishing threats, and integrated solutions that work with the Security and Operations Center for comprehensive protection.

NetBreach: Proactive Security Testing - Comprehensive Network Penetration testing of Internal and External tests based on the order. The provider will acquire and assign an appropriate number of licenses to support the client environment. The service detects vulnerabilities by identifying weaknesses that can be exploited both externally and internally. It provides a comprehensive assessment by evaluating software, hardware, configurations, applications, and any device with an IP address. The service also includes identifying problems that attackers could use to infiltrate or damage your system. Additionally, it supports continuous improvement by tracking progress over time, using historical scans identify corrected deficiencies and new threats.

NetSecure: Multi-Factor Shield - Enhanced Multifactor Authentication beyond the free authenticator apps. The provider will acquire and assign an appropriate number of licenses to support the client environment and configure multi-factor authentication for compatible software applications, supported devices, and customized security policies and procedures. After performing a security assessment and evaluating the state of the client's existing policies and procedures related to network security, the provider will work with the client to prepare a new or revised set of policies and procedures that incorporate cutting-edge best practices and leverage the other services delivered by the provider. This setup prevents unauthorized access by adding an extra layer of security to online accounts, even if passwords are compromised. It establishes trust for devices accessing the network and offers versatile configuration options to protect VPN logins, computer access, email, and most third-party applications. Additionally, it provides secure connections to company networks and applications.

ReStartDR - 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.

The provider will acquire licenses, software application and equipment to provide ReStartDR Data Backup to enable daily backup monitoring, periodic backup testing, and provide data restoration upon request. Provider, through its Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. All target backup storage will utilize the third-party cloud storage unless Internet connection speed is insufficient for Cloud Backup or is mandated by law compliance.

Off-site Backup copies will have one-year retention unless specified in Order. Upon termination of these Services, Client will return backup equipment, allow removal of backup software applications Client systems. Provider shall erase all Client backup data from all storage locations (i.e. ReStartDR equipment, off-site storage) within 30 days.

Local Equipment - The Provider will determine if local backup equipment is required. Client will notify the Provider of any failures, and upon request, perform simple on-site tasks (e.g., powering down and rebooting hardware).

The Client is responsible for replacement costs for the loss of the device due to theft, fire, water, or misuse by Client or their employees. This includes equipment or software failure not caused by Provider. Additionally, the failure of the insurance company to honor a claim does not change the obligation of Client to compensate Provider for the full new replacement value of the equipment. The Client is also responsible for labor costs that are not related to the normal working of the system, such as the relocation of equipment, removing trash, and cleaning the equipment area. Furthermore, equipment failure resulting from site environments that do not meet manufacturer specifications, such as heat and moisture, is also the responsibility of Client.

Data Backup – This backup provides an off-computer (i.e., cloud or removable storage) copy of the data over a period of time. It is a fail-safe to restore data when the original data is lost (i.e. deleted, ransomware encrypted, corrupted).

Image Backup – This backup provides an off- computer (i.e., cloud or removable storage) copy of the entire system (i.e., Operating System and all data on hard drive). The backup can restore data and restore to another computer, when the computer hardware has failed.

Hot Backup – This backup provides an off- computer (i.e., cloud or a separate computer) copy of the entire system (i.e., Operating System and all data on hard drive) to a backup environment that allows for running of the backup when the original system is not available (e.g., physical failure, cybersecurity breach). The backup can restore data and restore to another computer.

DISASTER RECOVERY FOR RESTARTDR

Disaster Recovery has 2 phases.

REMEDIATION is the process of recovering the operability of the systems to a temporary system - Provider shall provide service that includes backup software, hardware, daily backup monitoring and the use of a loaner server for 5 business days to recover data files to temporarily resume business operation. After the time period, the client is charged a weekly rental fee.

RESTORATION is the process of installing the production systems and recovering all working functions for business operations. - If new equipment or software is required to recover the system, the project is billable at the contracted hourly rate.

Based on the Provider determination, an on-site equipment maybe required and is provided. Labor charges for disaster recovery (i.e., remediation and restoration) is based on the support level of the device being backed up.

EXCLUSIONS for Disaster Recovery

Service does not include replacement for any client equipment that is part of a disaster.

Recovery labor from cyber breaches caused by users not following recommended security protocols is billable at the contracted hourly rate.

CYBER TRAINING SERVICES

Provider will provide live (i.e., on-site or video conference) cybersecurity employee awareness training with up-to-date information on cyber threats and best practice tips for personal protection behavior. The cybersecurity training is designed to meet most cyber insurance requirements for annual employee training.

FLOWFILE Document Management

The TechBldrs Flowfile document management system is provided as a limited “Right to Use” application. Flowfile is installed on a named computer and is licensed for a setup fee. Licenses are not transferable. The client is responsible for the storage, backup, and recovery of all data. Upon termination, the client must return the Flowfile license to end the monthly fee.

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.**