



Effective September 3, 2026. 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.

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.

Server/Networking Monitoring and Management – Provider will perform server and networking 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, configuration backups, firmware updates as required by manufacturer, and 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. 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 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").

WORKSTATION DEPLOYMENT SCHEDULE

For new or reimaged workstation deployments, the work is considered a project. Provider will prepare, configure, deploy and train based on the instructions, guidelines and standards provided by Client at the applicable hourly rate. Onsite deployment is available, travel time may be chargeable.

BACKUP & DISASTER RECOVERY SERVICES

Data Backup Only

Included in this monthly fee:

- Constant monitoring of all servers and covered systems via backup monitoring software
- Error and syncing repairs
- Configuration changes & updates
- Unlimited file-level data recovery

Not included in this fee:

- Disaster recovery- any server-level recovery efforts will be billed at Time & Material ratesⁱ
- Ransomware scanning & preventionⁱⁱ
- Disaster and recovery testing and simulationⁱⁱⁱ

Data Backups and Azure Site Recovery Management

All services identified in the Data Backup Only, plus:

- Management of Azure site recovery resources
- Maintenance of near-line Azure recovery points

Monthly Backup fee does not include the initial setup and configuration of backup services.

i: Emergency Rates may apply

ii: Additional products are available for scanning data in transit as it is backed up

iii: Disaster recovery testing is recommended as a once-a-year project for all clients

CLOUD AND HOSTING SERVICES

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.

WORKSTATION DEPLOYMENT SCHEDULE

Provider offers different types of workstation deployment plans, designed to accommodate the budget and operational standards of any client.

Light & Spare (laptops only)	Standard & Rush	Autopilot**
Included:	Included:	Included:
Order & Prepare device	Order & Prepare device	Customized for each environment
Image & Configure	Image & Configure	Automated deployment
Load General Apps	Load General Apps	Expedited/automated disaster recovery
Load Custom Apps	Load Custom Apps	Central administration
Join to Domain	Join to Domain	Enterprise-grade management
Test configuration	Test configuration	Deployments in as little as 15 minutes
Ship device to user*	Onsite deployment	
Asynchronous User training	Asynchronous User training	
Up to 60 minutes deployment support	Unlimited user training and deployment support	

Bulk purchasing discounts always apply.

*Shipping charges apply

**Autopilot maintenance agreement may apply.

MICROSOFT TEAMS VOICE SUPPORT ADDENDUM

Unless otherwise agreed upon, Provider provides best effort support on phone systems. Clients without a maintenance agreement for their Provider installed phone system will be subject to Time & Materials charges at Providers sole discretion.

Scope of support

Maintenance includes initial system configuration as defined in the implementation scope, end user support and troubleshooting:

- User termination: voicemail archival, migrating lines between users
- User transfers: voicemail migrations, desk migrations (remote)
- Audio Conferencing support
- User support and troubleshooting (ticket support)
- User migration, voicemail archival
- Manufacturer patching and updates

What is not included:

- Addition of hardware (handsets, headsets, etc)
- Reconfiguration of departmental or companywide phone tree or workflows
- Integration of additional or 3rd party software applications

Microsoft Teams is a system designed for end-user self service. Provider typically trains a power user for each client who is responsible for helping with general training and guidance for users. Additionally, there are excellent knowledgebase articles and videos available from Microsoft. Client acknowledges that system performance relies on Microsoft and Internet Service Provider, Provider cannot warranty the uptime of the system. Client acknowledges that Provider relies on Microsoft to provide support for many troubleshooting situations, and our Service Level Agreement for Teams Voice issues is Best Effort.

Phone Hardware

Provider does not provide any warranties for phone equipment (handsets). Our general recommendation will be to replace faulty units.

FIREWALL AS A SERVICE RENTAL AGREEMENT

Rather than making a capital outlay for hardware that may become obsolete if you change your internet bandwidth or the threat landscape changes, most companies now opt to rent firewalls (Firewall as a Service -FWaaS). This arrangement provides a convenient and flexible solution for you to adapt your security without the risk of owning obsolete hardware.

If included on the Order, The cost of the FWaaS will appear on Client's monthly invoice (typically billed on the 5th of each month) and will be due within the terms of the invoice. Minimum term is 18 months from date of install and Client is liable for entire 18-month term. The first month may be prorated depending on install date. Cancellation terms are 60-day notice after initial non-refundable 18-month term. At the end of the initial term, Provider may change the monthly fee to the client to reflect changes in the cost or bundle of the annual security software package running on the device. Provider will provide advance notice of any recommended changes.

Non-Refundable. Subscription plans for customer purchases of software and hardware are non-refundable. Paying all sums due, directly or by reimbursement to Provider Technology, under any subscription is the customer's responsibility, as these are prepaid for the most part by Provider Technology.

Transferability Administration Client's Responsibility. Device can be returned to Provider or exchanged for a different model after initial term. Client is responsible for paying the difference between the amounts, and for the shipping costs associated with the exchange. Provider will continue invoicing for the device until the purchase is approved. If the device or licensing is transferrable, it is Client's sole obligation to cover all administration, costs, fees, penalties and expenses.

Equipment Moves, Early Terminations, Upgrades, Lost assets or Cancellations

If Client elects to make any changes to the agreement prior to 18-months, including equipment moves, Provider will make reasonable efforts to accommodate, but re-installation, administrative, shipping, re-stocking fees may apply at our sole-discretion. Provider will continue invoicing for the device until it is returned in working condition to Provider. For unreturned or damaged hardware, Provider will provide client with a depreciated purchase quote. It is the responsibility of the Client to carry appropriate insurance to protect themselves against undue losses.

i Emergency Rates may apply

ii Additional products are available for scanning data in transit as it is backed up

iii Disaster recovery testing is recommended as a once-a-year project for all clients

ROCKET CYBER SERVICES

Rocket Cyber is an enterprise-grade Security Information and Event Management (SIEM) and Security Operations Center (SOC) solution designed to provide comprehensive threat detection and response capabilities. The platform continuously ingests and analyzes logs and heuristic data from multiple security sources, including:

- Antivirus and Endpoint Detection and Response (EDR) software
- Remote Management and Monitoring (RMM) tools
- Microsoft Office 365 environments
- Network firewalls
- DNS filtering solutions

Through 24/7/365 monitoring of integrated data sources, Rocket Cyber delivers enhanced cybersecurity detection and incident response capabilities for our clients.

Standard Integration Scope

As part of the initial deployment, Rocket Cyber will be configured to ingest and monitor logs from the following sources:

- Antivirus/EDR Platform – Primary endpoint protection solution
- Microsoft Office 365 – Email, collaboration, and productivity suite
- DNS Filtering Tools – ThreatSTOP or equivalent DNS security solutions
- Network Firewall(s) – Perimeter and internal network security devices
- Additional Systems – Integration of other security tools may be available upon request and may incur additional fees

Automated Threat Response

In the event of confirmed malicious activity, Rocket Cyber may automatically disable services or restrict access to contain threats. This automated response helps minimize the potential impact of security incidents.

After-Hours Incident Response

Security incidents requiring immediate attention outside of standard business hours will be addressed according to your selected response protocol (see After-Hours Response Options below).

Security Reporting

Rocket Cyber provides comprehensive security analytics and reporting capabilities, including:

- Enhanced security metrics for quarterly business reviews
- Automated security reports delivered on a scheduled basis
- Detailed threat intelligence and incident summaries
- Compliance and risk assessment reporting

After-Hours Response Options

Cyber threats operate continuously and may be detected outside of normal business hours. When the Rocket Cyber SOC identifies critical threats after hours, the following response protocols are available:

Option 1: Immediate Response (Standard)

The SOC will respond immediately to contain and isolate threats. For elevated-risk incidents requiring engineering intervention, our after-hours support team will be engaged to remediate the issue. After-hours support rates will apply to remediation activities.

Option 2: Delayed Response

If you prefer to avoid after-hours charges and accept the risk of delayed mitigation, we can configure your environment to queue non-critical incidents for response during the next business day. This option may increase exposure to active threats.

Your Account Manager can assist in selecting the appropriate response protocol for your organization's risk tolerance and operational requirements.

****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.**