



Effective October 9, 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.

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.

Backup and File Recovery

Implementation and facilitation of a backup and file recovery solution from our designated Third Party Provider.

- 24/7 monitoring of backup system, including offsite backup, offsite replication, and an onsite backup appliance ("Backup Appliance").
- Troubleshooting and remediation of failed backup disks.
- Preventive maintenance and management of imaging software.
- Firmware and software updates of backup appliance.
- Problem analysis by the network operations team.
- Monitoring of backup successes and failures.
- Daily recovery verification.

Backup Data Security: All backed up data is encrypted in transit. All facilities housing backed up data implement physical security controls and logs, including security cameras, and have multiple internet connections with failover capabilities.

Backup Retention: Backed up data will be retained for the periods indicated below, unless a different time period is expressly stated in the Order. This includes both on-premise and cloud backups.

•*On-Premise Backups*

All on-premise backups will be stored on a Network Attached Storage (NAS) device, which will be kept in a secure location with restricted access. On-premise backups will be performed daily and retained on a rolling thirty (30) day basis.

•*Cloud Backups*

All cloud backups will be stored in a secure, off-site location that meets the organization's security standards. Cloud backups will be performed daily and retained on a rolling thirty (30) day basis.

Backup Alerts: Managed servers will be configured to inform of any backup failures.

Recovery of Data: If you need to recover any of your backed up data, then the following procedures will apply:

•Service Hours: Backed up data can be requested during our normal business hours, which are currently Monday-Friday 8:00 a.m. to 5:00 p.m. PST.

•Request Method. Requests to restore backed up data should be made through one of the following methods:

o Email: ticket@firefly.ms

o Telephone: 509-663-8324

•Restoration Time: We will endeavor to restore backed up data as quickly as possible following our receipt of a request to do so; however, in all cases, data restoration services are subject to (i) technician availability and (ii) confirmation that the restoration point(s) is/are available to receive the backed up data. (iii) Size of data to be restored (iiii) internet speed.

Backup Monitoring

Implementation and facilitation of a backup monitoring solution from our designated Third Party Provider.

Features include:

·Monitoring backup status for certain backup applications then-installed in the managed environment, such as successful completion of backup, failure errors, and destination free space restrictions/limitations.

·Helping ensure adequate access to Client's data in the event of loss of data or disruption of certain existing backup applications.

Note: Backup monitoring is limited to monitoring activities only and is not a backup and file recovery solution. Backup monitoring is limited to our business hours Monday-Friday 8:00 a.m.-5:00 p.m. PST.

Email Threat Protection

Implementation and facilitation of a trusted email threat protection solution from our designated Third Party Provider.

- Managed email protection from phishing, business email compromise (BEC), SPAM, and email-based malware.
- Friendly Name filters to protect against social engineering impersonation attacks on managed devices.
- Protection against social engineering attacks like whaling, CEO fraud, business email compromise or W-2 fraud.
- Protects against newly registered and newly observed domains to catch the first email from a newly registered domain.
- Protects against display name spoofing.
- Protects against “looks like” and “sounds like” versions of domain names.

Endpoint Antivirus & Malware Protection

Implementation and facilitation of an endpoint malware protection solution from our designated Third Party Provider.

- Artificial intelligence and machine learning to provide a comprehensive and adaptive protection paradigm to managed endpoints.
- Detection of unauthorized behaviors of users, applications, or network servers.
- Blocking of suspicious actions before execution.
- Analyzing suspicious app activity in isolated sandboxes.
- Antivirus and malware protection for managed devices such as laptops, desktops, and servers.
- Protection against file-based and fileless scripts, as well as malicious JavaScript, VBScript, PowerShell, macros and more.
- Whitelisting for legitimate scripts.
- Blocking of unwanted web content.
- Detection of advanced phishing attacks.
- Detection / prevention of content from IP addresses with low reputation.

Extended Detection & Response (XDR)

Implementation and facilitation of an endpoint malware protection solution with extended functionalities from our designated Third Party Provider.

- Automated correlation of data across multiple security layers*—email, endpoint, server, cloud workload, and the managed network, enabling faster threat detection.
- Provides extended malware sweeping, hunting, and investigation.
- Allows whitelisting for legitimate scripts.

- Next-generation deep learning malware detection, file scanning, and live protection for workstation operating system.
- Web access security and control, application security and control, intrusion prevention system.
- Data loss prevention, exploit prevention, malicious traffic detection, disk and boot record protection.
- Managed detection, root cause analysis, deep learning malware analysis, and live response.
- On-demand endpoint isolation, advanced threat intelligence, and forensic data export.

* Requires at least two layers (e.g., endpoint, email, network, servers, and/or cloud workload.)

End User Security Awareness Training

Implementation and facilitation of a security awareness training solution from an industry-leading third party solution provider.

- Online, on-demand training videos (multi-lingual).
- Online, on-demand quizzes to verify employee retention of training content.
- Baseline testing to assess the phish-prone percentage of users; simulated phishing email campaigns designed to educate employees about security threats.

Firewall Solution

(firewall appliance provided / purchased by Client)

- Monitors, updates (software/firmware), and supports Client-supplied firewall appliance.
- Helps to prevent hackers from accessing internal network(s) from outside the network(s), while providing secure and encrypted remote network access; provides antivirus scanning for all traffic entering and leaving the managed network; provides website content filtering functionality.

Labor for New / Replacement Workstations

Includes all labor charges for setup of new workstations, or replacement of existing workstations.

Labor covers:

- New computers / additional computers added during the term of the Order;
- Replacement of existing computers that are four (4) or more years old (as determined by the manufacturer's serial number records);
- Replacement of existing computers that lost/stolen or irreparably damaged and/or out of warranty but not yet four years old;
- Operating systems upgrades – subject to hardware compatibility.

The following restrictions apply:

- Upgrades or installs of new or replacement computers are limited to four (4) devices per month unless otherwise approved in advance by Firefly;
- This service is not available for used or remanufactured computers; and,
- New/replacement computers must be business-grade machines (not home) from a major manufacturer like Dell, HPE, or Lenovo.

Managed Detection & Response (MDR)

Implementation and facilitation of a top-tier MDR solution from our designated Third Party Provider.

- 24x7 Managed network detection and response.
- Real time and continuous (24x7) monitoring and threat hunting.
- Real time threat response.
- Alerts handled in accordance with our Service response times, below.
- Security reports, such as privileged activities, security events, and network reports, are available upon request.
- 24x7x365 access to a security team for incident response*

* Remediation services provided on a time and materials basis.

Remote Helpdesk

Remote support provided during normal business hours for managed devices and covered software

Remote Infrastructure Maintenance & Support

- Configuration, monitoring, and preventative maintenance services provided for the managed IT infrastructure
- If remote efforts are unsuccessful, then Firefly will dispatch a technician to the Client's premises to resolve covered incidents (timing of onsite support is subject to technician availability and scheduling).

Onsite Support

- Onsite support provided during normal business hours for managed devices and covered software within 60 miles of the Wenatchee location.

Remote Monitoring and Management

Software agents installed in Covered Equipment (defined below) report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below.

- Review and installation of updates and patches for supported software.
- Server Monitoring & Maintenance

- As part of our RMM service, we will monitor and maintain managed servers as follows:
- Software agents installed in covered servers report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below.
- Online status monitoring, alerting us to potential failures or outages
- Capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD and SSD partitions, not external devices such as USB or mapped network drives)
- Server essential service monitoring, alerting us to server role-based service failures
- Endpoint protection agent monitoring, alerting us to potential security vulnerabilities
- Secure remote connectivity to the server and collaborative screen sharing
- Review and installation of updates and patches for Windows and supported software
- Asset inventory and server information collection

Two Factor Authentication

Implementation and facilitation of a two factor authentication solution from our designated Third Party Provider.

- Advanced two factor authentication with advanced admin features.
- Secures on-premises and cloud-based applications.
- Permits custom access policies based on role, device, location.
- Identifies and verifies device health to detect “risky” devices

Updates & Patching

- Remotely deploy updates (e.g., x.1 to x.2), as well as bug fixes, minor enhancements, and security updates as deemed necessary on all managed hardware.
- Perform minor software installations.
- Perform minor installations (i.e., tasks that can be performed remotely and typically take less than thirty (30) minutes to complete).
- Deploy, manage, and monitor the installation of approved service packs, security updates and firmware updates as deemed necessary on all applicable managed hardware.

Dedicated Account Manager

Act as the main point of contact for certain business-related IT issues and concerns.

- Assist in the creation of information/data-related plans and budgets.
- Provide strategic guidance and consultation across different technologies.
- Provide education and recommendations for business technologies.
- Participate in scheduled meetings to maintain goals.
- Maintain technology documentation.
- Assess and make recommendations for improving technology usage and services.

Website Hosting

Our designated Third Party Provider will provide sufficient space and bandwidth to host your designated website ("Website") which, except for scheduled downtime or force majeure events, will be available on a 24x7 basis. The Website will be hosted on a server that may be shared between many customers; however, the Website will be given a unique address.

- **Migration of Servers.** As a normal course of business, we or our Third Party Provider, as applicable, may migrate the servers on which the Website is hosted. This process will not interfere with the Hosting Services, however, due to the potential for migration, you are not guaranteed a permanent or dedicated IP address.
- **Administration.** You will be provided with access to a dashboard through which you may make configuration adjustments to the hosted environment; however, we strongly advise you to refrain from making changes to the hosted environment without our guidance or direction. We will not be responsible for remediating issues caused by your adjustments to the hosted environment unless those adjustments were made pursuant to our written directions or under our supervision.
- **Resource/Load Balancing.** The bandwidth made available to your website is shared and allocated among all of our customers. You must comply with all bandwidth and Firefly-imposed limitations on the hosting services as established by Firefly from time to time. We reserve the right to load-balance applicable bandwidth to ensure that your activity will not restrict, inhibit, or diminish any other user's use of the bandwidth or create an unusually large burden on the bandwidth. We reserve the right to restrict your access to your hosted website in the event that your activities create a disproportionate burden on our network or our third party providers' networks (if applicable), or any other crucial resources reasonably needed to ensure the functionality, integrity, and/or security of the hosting services.
- **Storage and Security.** We and/or our third party providers will take reasonable steps to prevent unauthorized access to the Website and the hosted environment; however, you understand and agree that no security solution is 100% effective, and we do not warrant or guarantee that the hosted environment will be free from unauthorized access or malware at all times.

Wi-Fi Services

Firefly will install at the Client's premises Wireless Access Points to provide bandwidth in all areas requiring wireless network coverage, as agreed upon by Firefly and Client.

- Firefly will maintain, supervise, and manage the wireless system.
- Installed equipment, if provided by Firefly, will be compatible with the then-current industry standards.
- Firefly will provide remote support services during normal business hours to assist with device connectivity issues if the client's service plan permits. (Support services will be provided on a "best efforts" basis only, and Client understands that some end-user devices may not connect to the wireless network, or they may connect but not perform well).

Please note: Any Wi-Fi devices, such as access points or routers, that are supplied by Client cannot be older than five (5) years from the applicable device's original date of manufacture, and in all cases must be supported by the manufacturer of the device(s).

Workstation Monitoring & Maintenance

Software agents installed on covered workstations report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below.

- Online status monitoring, alerting us to potential failures or outages.
- Capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD and SSD partitions, not external devices such as USB or mapped network drives).
- Performance monitoring, alerting us to unusual processor or memory usage.
- Routine operating system inspection and cleansing.
- Secure remote connectivity to the workstation and collaborative screen sharing.
- Review and installation of updates and patches for Windows and supported software.
- Asset inventory and workstation information collection.

ZTNA (Zero Trust Network Access)

Ensures that users are granted access only to the specific applications or services they need based on their identity, device, and context. This minimizes the attack surface and reduces the risk of lateral movement within the network if a user's credentials are compromised.

PLAN COVERAGES

	Security Core	Essentials	Remote	Complete
CyberSecurity Solution	Covered	Covered	Covered	Covered
Patches & Updates	Covered	Covered	Covered	Covered
Scheduled Restarts	X	Covered	Covered	Covered
Dedicated Account Team	X	Covered	Covered	Covered
Asset Inventory w/ Rotation	X	Covered	Covered	Covered
Priority Queue/SLA	X	Covered	Covered	Covered
Mapping & Documentation	X	Covered	Covered	Covered
Backup Management*	\$250/hr	Covered	Covered	Covered
Email License Management*	\$250/hr	Covered	Covered	Covered
Email Inbox/User Support*	\$250/hr	\$135/hr	Covered	Covered
Strategic Budget Recommendations	\$250/hr	\$135/hr	Covered	Covered
Remote Support	\$250/hr	\$135/hr	Covered	Covered
Onsite Support	\$250/hr	\$135/hr	\$135/hr	Covered
Inshop Support	\$250/hr	\$135/hr	\$135/hr	Covered
Travel Fees	\$250/hr	\$135/hr	\$135/hr	Covered
New Hardware/Software Configuration	\$250/hr	\$135/hr	\$135/hr	\$135/hr
Software Migration	\$250/hr	\$135/hr	\$135/hr	\$135/hr
Afterhours Support	\$500/hr	\$250/hr	\$250/hr	\$250/hr

Monthly Price Per Device: **\$30** **\$50** **\$75** **\$100**

* Email and Backup Services Require add-on licenses managed through Firefly

Advanced Cybersecurity

Security Core
Cybersecurity Essentials

- Security Awareness Training
- Phishing Testing
- 24/7/365 Threat Monitoring
- Heuristic EDR + MDR
- Automated Patches & Updates
- Remote Access & Controls
- DNS Filtering
- Security Stack Maintenance

\$30 Per Device
\$250 hr. For All IT Services

Please Note: Security Core Does not come with any IT Helpdesk or Project services



thinkfirefly.com
CYBERSECURITY • NETWORK IT • COMPUTER SALES

Charlie@Firefly.ms
(509) 663 8324

Managed IT & Cybersecurity

Month to Month & Contractual Options Available

Essentials
Proactive IT & Cybersecurity

- Full Cybersecurity Solution
- Proactive IT Management
- Patches & Updates
- Scheduled Device Restarts
- Priority Support Queue & SLA
- Personal Account Team
- Network Planning & Review
- Inventory & Budgeting
- Self-Service Password Resets
- Mapping & Documentation

\$50 Per Device
\$135 Hr. for all Projects/Helpdesk

Remote
Remote Full-Service IT/Security

- All Previous Tier Benefits
- Remote Support Included
- Phone Support Included

Most Popular

\$75 Per Device
Unlimited Remote & Phone Support

Complete
Full-Service IT/Security

- All Previous Tier Benefits
- Onsite Support Included
- In Shop Support Included
- Travel Time Included

\$100 Per Device
Unlimited Onsite, In-shop, & Travel

Monthly Add On Services:
Firefly Secure Email: \$42.50 per inbox
Workstation Backup: \$15 | Server Backup: \$135

Advanced Onboarding:
Tool Configuration, Network Mapping, Documentation, & Environment Recommendations

\$500 - \$7,500 Based Upon Device Count
25% Off for Each Year Committed | FREE with 5-Year Commitment

*Device = Laptops, Desktops, Servers, and Virtual Machines
**New Hardware Configuration and Software Migrations are Always a Billable Project.

**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.