Service Statement

This Service Statement contains provisions that define, clarify, and govern the services described in the quote provided to you (the "Quote"). If you do not agree with the terms of this Service Statement, you should not sign the Quote and you must contact us for more information.

This Service Statement is our "owner's manual" that generally describes all managed services provided or facilitated by Layer 9, Inc. ("Layer 9"); however, only those services specifically described in the Quote will be facilitated and/or provided to you (collectively, the "Services"). Activities or items that are not specifically described in the Quote will be out of scope and will not be included unless otherwise agreed to by us in writing.

This Service Statement contains important provisions pertaining to the auto-renewal of the Services your Quote, as well as fee increases that may occur from time-to-time. Please read this Service Statement carefully and keep a copy for your records.

Onboarding Services

If onboarding services are provided under the Quote, then the following services will be provided to you.

Inventory Management:

- Uninstall any monitoring tools or other software installed by previous IT consultants.
- Uninstall any previous endpoint and or virus protection.
- Uninstall unsafe applications or applications that are no longer necessary. List of "unsafe applications" will be reviewed with Client before removed.
- Install remote support access application on each managed device to enable remote support.
- Install Layer 9 Managed Antivirus Application. (Generation of Antivirus is based on Security Package selected on Quote)
- Configure patch management application and check for missing security updates. (See patch management section for specific information on patch management.)
- Compile a full inventory of all protected servers, workstations, and laptops.

Network Status /Infrastructure Review:

- Review firewall configuration and other network infrastructure devices.
- Perform baseline internal and external vulnerability scans.
- Review existing backup strategy and status.

- Review current password policies and update user and device passwords that include any administrative passwords used by the previous IT provider.
- Perform initial workflow analysis to determine day to day operations and programs that are most utilized

Documentation:

- Review and document current server configuration.
- Review and document current workstation configuration.
- Document network devices such as; printers, scanners, phone systems, credit card devices, mobile devices
- Document current email configuration

Onboarding Kick Off

Onboarding kick off meetings are performed on onboarding day with our Customer Success Team. At the onboarding kick off meeting, the client should make their entire team available for a quick presentation on how onboarding will be performed, what they can expect, and how to get in touch with support if necessary. At that same time, Layer 9 Technical Alignment Manager (TAM) will be onsite to begin the onboarding tasks. We ask that the client make at least one employee available to the TAM to answer any questions, talk through workflows and provide access to any systems as necessary.

Onboarding Wrap Up

Onboarding can take anywhere between 30-60 days to complete, depending on the complexity of the network or service packages. The end of onboarding will be marked by a wrap up meeting with our Customer Success team. At this meeting, a status of the network will be presented along with any priority items that will need to be knocked out within the first 90 days of the agreement.

The foregoing list is subject to change if we determine, in our discretion, that different or additional onboarding activities are required.

If deficiencies are discovered during the onboarding process, we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of our monthly managed services. Please note, unless otherwise expressly stated in the Quote, onboarding-related services do not include the remediation of any issues, errors, or deficiencies ("Issues"), and we cannot guarantee that all Issues will be detected during the onboarding process.

Ongoing / Recurring Services

Ongoing/recurring services are services that are provided to you on an ongoing basis and, unless otherwise indicated in a Quote, are billed to you monthly. Ongoing services generally begin upon the commencement of onboarding services.

Managed Services

The following Services, if listed in the Quote, will be provided to you.

Managed Service Package: Advance

SERVICES	DESCRIPTION
Remote	*See Service Levels for Description of Support*
Onsite Support	Onsite support is available during Layer 9 business hours. All support requests are attempted to be resolved remotely; Onsite support is escalated if issue cannot be resolved remotely. Service Coordinator will work with client to schedule a next available tech. Same day onsite service cannot be guaranteed.
After Hours Support	After Hours is considered anytime outside of Layer 9 standard business hours and/or holidays. After Hours support is reserved for Emergencies only. Emergencies are considered, network down or critical function down. To receive After Hours support, a ticket has to be submitted through the Layer 9 portal at www.layer9it.com/support, using the After Hours ticket type, or by emailing afterhours@layer9it.com . Any ticket submitted to the regular ticket board will not be worked during After Hours. After Hours fees are charged in increments of 15 minutes. If technician needs to come onsite to client location during After Hours, there is a minimum of 1 hour billed.
Self Service Portal	Layer 9 utilizes a customer portal which can be found at www.layer9it.com/support . From this portal the client can: • Submit Support Tickets • Submit Quote Requests • Submit New User Request • Review Ticket Status • View / Pay Invoices • Review Layer 9 documentation All support requests should be generated through the customer portal to ensure accurate troubleshooting.
Darkweb Monitoring	*See Additional Terms for detailed information on Darkweb Monitoring*
Cyber Awareness Training	*See Additional Terms for detailed information on Cyber Awareness Training*
Technology Business Review	A technology business review is a meeting between the client decision makers and our customer success team. During this meeting the client will be presented with a current status of the network report as well as a road map for any items that need to be addressed or purchased over the next quarter. On an annual basis, we provide a 12 month proposed budget that includes devices that need to be replaced as well as any other initiatives that need to be tackled.
Quarterly Security Assessments	Review of current security status based on security package. *See "Security Packages" below for information on the package you are subscribed to" .*

Client Success Manager	Your Client Success Manager (CSM) will be your go-to for all Layer 9 items. The CSM works as the intermediary between the client and Layer 9's (5) Service Delivery Teams. The CSM will keep careful watch over the health of your account and will be proactively reaching out with updates on service, projects, and security. The CSM is not a technical resource and therefore will not be able to resolve technical issues. The CSM will work with you, however, to direct your technical requests to the correct service delivery team.
IT Budget Planning	Layer 9 will provide automated Lifecycle reports in Q4 of the calendar year that can be used for budgeting for the next fiscal year.
Patch Management – Microsoft	Through our remote monitoring and management tool, we push out all Microsoft security patching on a weekly basis. Patch windows are Tuesday's – Thursday's. Users will receive a pop-up on their machine letting them know that Patching has completed and is requiring a reboot. Users can post-pone the reboot until all work has been saved, but all machines need to be rebooted at least once weekly to prevent any security vulnerabilities. *See Additional Terms for further details.*
Auto Escalation and Resolution Alerts	During each stage of the ticket life cycle, when a status changes, the end user will be notified. When the issue is resolved, the end user is notified, and a survey will be sent in the closure message to rate our service during this single instance
Network Alignment	Network Alignments review the status of the network against Manufacturer and Industry Best Practices. Any items found to be out of alignment could result in a fixed fee project.
Secure Remote Connectivity	Remote sessions are sheltered by a proprietary communication protocol with guaranteed global security by AES using a 256-bit cipher when establishing, or for the duration, of the session. The key exchange is protected by an SSL based in AES-CBC with TLS 1.2. All commands, including keyboard and mouse strokes, file transfers and clipboard information are digitally signed. The Remote-Control application does not have access to session content. All encryption is based on an end-to-end negotiation that does not intercept transferred information or decode the information in the gateway. Encryption keys are randomly generated for each session.
Firmware Updates	Firmware updates on Layer 9 supported hardware, is installed within 60 days of release. Firmware, unless to patch a critical vulnerability is not pushed immediately to allow for known issues and bug checks to be completed. Layer 9 supported hardware includes Layer 9 supported vendors. *Supported hardware is detailed in additional description of services below for further detail.*
Add/Move/Change Users	Layer 9's "MAC" team handles all Moves, Adds, and Changes. This includes onboarding and offboarding of users as well as any changes to permissions or group management. For a new user setup "onboarding", our team requires at least 5-business days' notice before the users start date. All requests for new user onboarding should come directly from the Layer 9 support portal found at www.layer9it.com/support , using the "New User Setup Request Form". Failure

	to follow this process could result in a delay of user setup. If your new user requires hardware, we need at least 14-business days' notices to get appropriate hardware in stock. During our new user onboarding, Layer 9 will configure all necessary accounts, access, and programs the new employee will need. Layer 9 will work with that user's manager to test access before the employee start date. Layer 9 is not responsible for configuring user permissions within 3rd party applications. The customer will need to configure these accounts.
O365 Management and Support	Layer 9 will manage the Office365 tenant. Layer 9 will need to be the "Partner of Record" on the email tenant for proper management. This will move your licensing purchases to your Monthly Layer 9 Agreement. Implementation of specific O365 Apps and Services may require a fixed fee project. *See the Fee section for Microsoft Licensing below for further details.*
Mobile Phone Support	If customer provides company cell phones, Layer 9 will assist with troubleshooting access to company provided apps and services only.

Managed Service Package: ProCare

ProCare Managed Services includes all the features of the Advanced Manage Services packages as well as those services listed below.

SERVICES	DESCRIPTION
Custom Employee Onboarding and Offboarding	Our customer success team will work with the client to create custom forms in the portal if necessary for new user onboarding and employee offboarding. These forms are necessary for businesses that have several departments with specific access and permissions based on role or department. Therefore, when the client submits a new user request from the Layer 9 support portal, all relevant details will be available for a quick setup. This is the same for employee offboarding.
Proactive On-Site Visits / Workflow Review	Part of your strategic team is a Technical Alignment Manager (TAM) will be assigned to your account. The TAM will work to understand and document all systems and software and will be able to dive into root cause issues as well as offer strategic solutions to better workflow and security.
Automatic Software Deployment	Layer 9 strives to automate what can be automated. The majority of Layer 9 security services are deployed through automation. We are able to also automate some line-of-business applications if a large software deployment or upgrade needs to be completed, but this is depended on vendor/manufacturer limitations.
Vulnerability Scanning	Vulnerability scanning points out holes in the network that could be exploited. Layer 9 runs external vulnerability scans monthly and internal vulnerability scans annually. External scans pertain to the IP address assigned to each customer location through the customers ISP. Internal scans look at all systems inside the network. Vulnerability results will be discussed during the technical business

	review. Vulnerability reports will be available on request. *See additional terms "Vulnerability Scanning" for more information.*
Vulnerability Remediation	Items found from the vulnerability report will be prioritized based on risk to the client's network. Vulnerabilities the require simple firmware upgrades will be covered. But if equipment must be changed out or reconfigured, a project may have to be scoped.
Custom Alerts	By default Layer 9 monitoring systems are monitoring for machines offline or outsize of best practice guidelines. If the client would like for us to monitor for non standard items, such as but not limited to: SQL services, Application dependent services, printer offline, etc., a custom alert can be configured.
Business Continuity Planning	In addition to backup systems, a client also benefits having a Business Continuity Plan (BCP) on hand, so it is understood what systems are to be prioritized to be brought back online and what critical functions need to be available. Knowing these items below can help build out a more robust Disaster Recovery Solution. BCP Includes: • Risks and potential business impact. • Planning an effective response. • Roles and responsibilities. • Communication. • Testing and training. *See Backup and Disaster Recovery under Additional Items for further details*
Whitelist and Blacklist Spam Email	Our advance spam filter can create custom allow and deny list(s). This configuration can be completed on the user or company level. If customer does not have a Procare package, they can still manage and maintain their own whitelist and blacklist. Advance spam filter licensing is only available in the Active and Complete security packages.

Managed Cybersecurity Services

The following Services, if listed in the Quote, will be provided to you.

SERVICES	PACKAGE	DESCRIPTION
Two-Factor/ Multi-Factor Authentication	Basic Active Complete	Two Factor setup and configuration is included for O365. Layer 9 is not responsible for or will troubleshoot personal own devices. (Devices not owned by the client). If any other system is requested to have two factor, there may be a project that needs to be scoped. Layer 9 requires that all remote applications have two-factor enabled. • 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
EDR (Endpoint Detection and Response)	Basic Active Complete	Layer 9 Managed EDR is deployed to all machines. EDR is a next-gen antivirus solution that uses behavioral heuristics to evaluate and respond to threats. If a threat is found, the EDR system will isolate the device so that it cannot infect additional machines on the network. Some legitimate applications are quarantined by the EDR system. Layer 9 will work with the client to create a whitelist of systems and processes. **Note that EDR licensing is billed per device. Each security package user includes (1) license, all additional licenses will be billed as a separate line item on the monthly agreement.*
User Training	Basic Active Complete	User training is one of the biggest ways to prevent a breach. Training user on how to identify and avoid costly mistakes is your last line of defense. Layer 9 User training requires that each employee complete a quarterly security training. All training is offered online and is self-paced ranging between 5-15 minutes. • Award-winning, on-demand, engaging, interactive browser-based training • Hints & Tips Security Awareness emails for compliance if necessary • Point-of-failure training auto-enrollment options • Phish-Prone Reporting and Participation Reporting All reporting will be provided by the Customer Success Manager.
Phishing Simulation	Basic Active Complete	Phishing Simulation puts User Training to the test. Automatic Phishing campaigns are sent out monthly. • The AI-Driven Phishing feature helps you deliver a personalized simulated phishing experience to every single user. The KnowBe4 phishing platform leverages machine learning to automatically choose the best phishing security test template for each user based on their individual phishing and training performance metrics. • Industry Benchmarking feature lets you compare your organization's Phish-prone percentage™ with other same-size organizations in your space • Ability to create anti-fraud templates that emulate spoofed CEO Fraud attacks • Automatic "Scam of The Week" Campaign - sent to all employees

		All reporting will be provided by the Customer Success Manager.
Advance Spam Filtering	Basic Active Complete	Advance SPAM filter prevents malicious items from getting into the users inbox. No solution can be 100% and some items may slip through. If a suspicious item is delivered, the user should submit a ticket to the Layer 9 Support Portal found at www.layer9it.com/support. During setup and configuration of the Advance Spam Filter, Layer 9 will need to make changes to the client's domain MX records. These are public facing records that point the client's email where it should be delivered. If Layer 9 does not have management of the client's public domain, the client must provide access to their management portal to Layer 9. Changes to the MX records can pause delivery of email temporarily. Layer 9 will attempt to work around business hours as much as possible to minimize production downtime. Once Spam Filter is in place, Layer 9 will provide user training of the system which includes how to mark suspicious email as SPAM or block unwanted emails. Users will receive a digest email a few times throughout the day, the purpose of the digest emails is to alert the user of emails that have been blocked. For security purposes, Layer 9 does not allow the end-user to unblock quarantine email on the own. User will need to open a ticket in the Layer 9 support portal for quarantine emails to be released. *See service levels for response time on non-critical emails.* **Note: Advance Spam Filtering is licensed per active email account. Each security package user includes (1) license, all additional licenses will be billed as a separate line item on the monthly agreement.*
Email Encryption	Active Complete	Layer 9 email encryption provides a secure way to communicate with clients, patients, or vendors. • Help manage compliance through strong integration with data-loss prevention capabilities. • Deliver encrypted email directly to recipients' inboxes and not to a Web service. • Decrypt and read encrypted email with confidence, without installing client software. Encrypted email is setup based on client and user need. Encrypted email should be configured for users who send out sensitive or protected information. Encrypted email

		setup is included and does not require downtime. Layer 9 will complete user training once the system has been implemented.
Security Operations Center	Active Complete	Layer 9's Managed Detection and Response is monitored by a third-party security operations center (SOC) 24/7. The SOC actively watches all network actively to quickly detect, remediate, and notify Layer 9 Incident Response team to any suspicious activity. Remediation is based on threat level and confidence. If a valid threat is detected the SOC team will do everything it can to stop its spread through the network. These actions include but are not limited to kill malicious processes and disconnecting the machine from the network through a managed agent. If a machine is found to be offline and inaccessible, please contact Layer 9 immediately. ****Note: SOC is licensed per computer/server device. Each security package user includes (1) license, all additional licenses will be billed as a separate line item on the monthly agreement.*
Computer Encryption	Complete	*Desktop Encryption is built into Windows systems and encrypts hard drives using AES-256 Layer 9 recommends encrypting of all drives, especially drives in mobile devices. Computer must meet minimum requirements for encryption to be applicable.* Layer 9 will utilize encryption software, included with your Office 365 E3 Subscription, to encrypt the hard drive of the user's workstation. ***Note: Computer encryption requires at least Office 365 E3 licensing, fees may be applicable for implementation of encryption*
Office 365 Defense	Complete	Cloud defense is the application of the Security Operations Center to the Microsoft Tenant. The SOC is watching all activity in the Microsoft tenant for malicious behavior and will take action to block such behaviors. *** Note: Cloud Defense license is licensed per email account. Each security package user includes (1) license, all additional licenses will be billed as a separate line item on the monthly agreement*
Security Information and Event Monitoring	Complete	Security Information and event monitoring (SIEM) captures all activity on the network from user logins, log offs, file modifications and deletions, etc. In the event of an incident, the SIEM is used to identify the source of the incident. Many regulated compliances require an auditing system. ***Note: SIEM licensing is based on log ingestion and retention of network devices. This licensing is not included in the monthly agreement and will be billed as an additional line item.*

Governance, Risk and Compliance	Complete	Layer 9 follows CIS framework as a standard in cyber security. On top of this framework, Layer 9 will assist with any industry compliance that the client falls under. This includes assessing against such controls, budgeting to meet controls and auditing that the network remains within such controls. *Note: Some industry compliance will require a management system to track progress on controls. If such system is necessary, it will be billed directly to the customer.*
Application Whitelisting	Complete	Allow listing has long been considered the gold standard in protecting businesses from known and unknown executables. Unlike antivirus, Allow listing puts you in control over what software, scripts, executables, and libraries can run on your endpoints and servers. This approach not only stops malicious software, but it also stops other unpermitted applications from running Layer 9 will work with your team to create the allow list for each job function. *** *Note: Application Whitelisting license is licensed per user account. Each security package user includes (1) license, all additional licenses will be billed as a separate line item on the monthly agreement*

ADDITIONAL SERVICES

SERVICES	GENERAL DESCRIPTION
Backup and Disaster Recovery	• 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 and at rest in 256-bit AES encryption. 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 by default for 12 months, client can subscribe to Infinite Retention if requested or required. 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 7AM – 6PM Monday - Friday. • Request Method. Requests to restore backed up data should be made through one of the following methods: ○ Email: support@layer9it.com ○ Web portal: support.layer9it.com ○ Telephone: 757-644-3291 • 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 technician availability. Generally, we can restore between 0 and 100MB of data within 8 business hours of your request, and 100 MB to 500 MB within 16 business hours hours of your request. Data restoration exceeding 500 MB will be handled in accordance with technician availability.
Updates & Patching	• 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 hardware and software installations and upgrades of managed hardware. • 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.
Firewall Solution	• Provide a FIPS 140-2 compliant firewall configured for your organization's specific bandwidth, remote access, and user needs. • 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 Quote;
	  ○ 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 Layer 9;
	• This service is not available for used or remanufactured computers;
	• New/replacement computers must be business-grade machines (not home) from a major manufacturer like Dell or HP

Covered Equipment / Hardware / Software

The Services will apply to the software listed in the Quote ("Supported Software") provided, however, that all Supported Software must, at all times, be properly licensed, and under a maintenance and support agreement from the Supported Software's manufacturer. In this Service Statement, Covered Hardware and Supported Software will be referred to as the "Environment" or "Covered Equipment."

We will provide support for any software applications that are licensed through us (see "Recurring Services" above). Such software ("Supported Software") will be supported on a "best efforts" only, and any support required beyond Level 2-type support will be facilitated with the applicable software vendor/producer. Coverage for non-Supported Software is outside of the scope of this SOW, and will be provided to you on a time and materials basis. Should our technicians provide you with advice concerning non-Supported Software, the provision of that advice should be viewed as an accommodation, not an obligation, to you.

The Services will be applied to the equipment, hardware and software listed in the "Managed Environment" schedule (collectively, the "Environment"), a copy of which will be provided upon completion of onboarding. Your strategic team will present the acquired inventory for approval before

they are entered into the agreement. Items that are not included in the Environment will not receive or benefit from the Services.

Physical Locations Covered by Services

Services will be provided remotely unless, in our discretion, we determine that an onsite visit is required. Onsite visits will be scheduled in accordance with the priority assigned to the issue (below) and are subject to technician availability. Unless we agree otherwise, all onsite Services will be provided at Client's primary office location listed in the Quote. Additional fees may apply for onsite visits or for offices outside of our service location: Please review the Service Level section below for more details.

Term; Termination

The Services will commence, and billing will begin, on the date indicated in the Quote ("Commencement Date") and will continue through the initial term listed in the Quote ("Initial Term"). We reserve the right to delay the Commencement Date until all onboarding/transition services (if any) are completed, and all deficiencies / revisions identified in the onboarding process (if any) are addressed or remediated to Layer 9's satisfaction.

The Services will continue through the Initial Term until terminated as provided in the Agreement, the Quote, or as indicated in this section (the "Service Term").

Auto-Renewal. After the expiration of the initial Service Term, the Service Term will automatically renew for contiguous terms equal to the initial Service Term unless either party notifies the other of its intention to not renew the Services no less than sixty (60) days before the end of the then-current Service Term.

Microsoft NCE Licensing: **Regardless of the reason for the termination of the Services, you will be required to pay for all NCE Licenses that we acquire on your behalf. Please see "Microsoft Licensing Fees" in the Fees section below for more details.**

Assumptions / Minimum Requirements / Exclusions

The scheduling, fees and provision of the Services are based upon the following assumptions and minimum requirements:

- Server hardware must be under current warranty coverage.
- All equipment with Microsoft Windows® operating systems must be running then-currently supported versions of such software and have all of the latest Microsoft service packs and critical updates installed.
- All software must be genuine, licensed and vendor-supported.
- The Environment must have a currently licensed, vendor-supported server-based backup solution that can be monitored.
- All wireless data traffic in the environment must be securely encrypted.
- All servers must be connected to working UPS devices.
- Client must provide all software installation media and key codes in the event of a failure.

- Any costs required to bring the Environment up to these minimum standards are not included in this Service Statement.
- Client must provide us with exclusive administrative privileges to the Environment.
- Client must not affix or install any accessory, addition, upgrade, equipment, or device on to the firewall, server, or NAS appliances (other than electronic data) unless expressly approved in writing by us.

Exclusions. Services that are not expressly described in the Quote will be out of scope and will not be provided to Client unless otherwise agreed, in writing, by Layer 9. Without limiting the foregoing, the following services are expressly excluded, and if required to be performed, must be agreed upon by Layer 9 in writing:

- Customization of third-party applications, or programming of any kind.
- Support for operating systems, applications, or hardware no longer supported by the manufacturer.
- Data/voice wiring or cabling services of any kind.
- Server or Network Battery backup replacement.
- Equipment relocation.
- The cost to bring the Environment up to the Minimum Requirements (unless otherwise noted in "Scope of Services" above).
- The cost of repairs to hardware or any supported equipment or software, or the costs to acquire parts or equipment, or shipping charges of any kind.

Service Levels

Automated monitoring is provided on an ongoing (*i.e.*, 24x7x365) basis; response, repair, and/or remediation services (as applicable) will be provided only during business hours unless otherwise specifically stated in the Quote. We will respond to problems, errors, or interruptions in the provision of the Services in the timeframe(s) described below. Severity levels will be determined by Layer 9 in our discretion after consulting with the Client. All remediation services will initially be attempted remotely; Layer 9 will provide onsite service only if remote remediation is ineffective and, under all circumstances, only if covered under the Service plan selected by Client.

	Response Time[1]	Normal Business Hours Monday – Thursday, 7am to 6pm Friday, 7am to 5pm	Emergency After Hours[2] Holidays, Non-Normal Business Hours
Portal	60 Min. Avg.	An engineer will respond, on average, in less than 60 minutes of opening a support ticket via portal, email, or phone call during Layer 9's normal business hours. • For contact initiated during our normal business hours, an engineer will begin working on the issue in the order in which it was received, subject to engineer availability. • Phone calls to support are treated as a portal request. A ticket will be entered and triaged appropriately. • If an issue is not resolved during normal business hours, it will be logged and continued the following day. • For contact initiated outside of normal business hours, a ticket will be logged, and work will begin on the next business day. • For issues where an engineer is required onsite, we will schedule an engineer for an onsite visit in accordance with the severity of the problem and always subject to engineer availability.	An engineer will respond, on average, in less than 60 minutes of opening a support ticket via portal, email, or phone call any time, or day of week. • An engineer will begin working on the issue immediately subject to engineer availability. • For critical issues where an engineer is required onsite, we will schedule an engineer for an onsite visit in accordance with the severity of the problem and always subject to engineer availability.[4]
Phone	Emergency User or Site Down		
Email	60 Min. Avg.	Email support is preferred for non-critical requests. • Response time can vary from 4 hours to 48 hours depending on engineer availability and request severity. Examples of non-critical requests are: • Software installation (which may be quoted as a project) • Issues for which a workaround has been implemented • Frequently asked questions (FAQ)-type requests • General consulting questions	

[1] **Response time is calculated from the time that the request for help is received by us though our designated support channels and the ticket is put in a status of In Progress. Requests received in any other manner may result in delays or non-responses.**

[2] **Emergency after hours are not included. If Emergency after hours support is provided, Client will be billed for such support ticket at a rate of $275 per hour, with a minimum of one (1) hour. All partial hours after the first hour are billed in fifteen (15) minute increments, with partial increments billed to the next higher increment. If applicable travel time will be billed from the engineer's location to client site, and back to the engineer's location.**

Trouble / Severity	Response Time
Critical: Service not available (*e.g.*, all users and functions unavailable)	Response within two (2) business hours after notification.
Significant Degradation (*e.g.*, large number of users or business critical functions affected)	Response within four (4) business hours after notification.
Limited Degradation (*e.g.*, limited number of users or functions affected, business process can continue).	Response within eight (8) business hours after notification.

Small Service Degradation (e.g., business process can continue, one user affected).	Response within two (2) business days after notification.

Fees

The fees for the Services will be as indicated in the Quote.

Changes to Environment. Initially, you will be charged the monthly fees indicated in the Quote. Thereafter, if the managed environment changes, or if the number of authorized users accessing the managed environment changes, then you agree that the fees will be automatically and immediately modified to accommodate those changes. Changes to the agreement are contingent upon Layer 9 receiving a new user or termination request through the Layer 9 portal. Changes to user count will not be made if there is not a corresponding termination request. Layer 9 will proactively perform an audit on a quarterly basis. Any discrepancies in user counts will credit or charged for if Layer 9 was not properly notified.

Minimum Monthly Fees. The initial Fees indicated in Quote are the minimum monthly fees ("MMF") that will be charged to you during the term. You agree that the amounts paid by you under the Quote will not drop below the MMF regardless of the number of users or devices to which the Services are directed or applied, unless we agree to the reduction. All modifications to the amount of hardware, devices, or authorized users under the Quote (as applicable) must be in writing and accepted by both parties.

Increases. In addition, we reserve the right to increase our monthly recurring and data recovery fees; provided, however, if an increase is more than five percent (5%) of the fees charged for the Services in the prior calendar year, then you will be provided with a sixty (60) day opportunity to terminate the Services by providing us with written notice of termination. You will be responsible for the payment of all fees that accrue up to the termination date and all pre-approved, non-mitigatable expenses that we incurred in our provision of the Services through the date of termination. Your continued acceptance or use of the Services after this sixty (60) day period will indicate your acceptance of the increased fees.

Travel Time. If onsite services are provided, we will travel up to 45 minutes from our office to your location at no charge. Time spent traveling beyond 45 minutes (*e.g.,* locations that are beyond 45 minutes from our office, occasions on which traffic conditions extend our drive time beyond 45 minutes one-way, etc.) will be billed to you at our then current hourly rates. In addition, we reserve the right to bill for all tolls, parking fees, and related expenses that we incur if we provide onsite services to you.

Appointment Cancellations. You may cancel or reschedule any appointment with us at no charge by providing us with notice of cancellation at least one business day in advance. If we do not receive timely a notice of cancellation/re-scheduling, or if you are not present at the scheduled time or if we are otherwise denied access to your premises at a pre-scheduled appointment time, then you agree to pay us a cancellation fee equal to two (2) hours of our normal consulting time (or non-business hours consulting time, whichever is appropriate), calculated at our then-current hourly rates.

Automated Payment. You may pay your invoices by credit card and/or by ACH, as described below. If you authorize payment by credit card and ACH, then the ACH payment method will be attempted first. If that attempt fails for any reason, then we will process payment using your designated credit card.

- **ACH**. When enrolled in an ACH payment processing method, you authorize us to electronically debit your designated checking or savings account, as defined and configured by you in our payment portal, for any payments due under the Quote. This authorization will continue until otherwise terminated in writing by you. We will apply a $35.00 service charge to your account for any electronic debit that is returned unpaid due to insufficient funds or due to your bank's electronic draft restrictions.
- **Credit Card**. When enrolled in a credit card payment processing method, you authorize us to charge your credit card, as designated by you in our payment portal, for any payments due under the Quote. We reserve the right to pass on credit card processing fees based on transaction total.
- **Check.** You may pay by check provided that your check is delivered to us prior to the commencement of Services. Checks that are returned to us as incorrect, incomplete, or "not sufficient funds" will be subject to a $50 administration fee and any applicable fees charged to us by your bank or financial institution.

Microsoft Licensing Fees. The Services require that we purchase certain "per seat" licenses from Microsoft (which Microsoft refers to as New Commerce Experience or "NCE Licenses") in order to provide you with one or more of the following applications: Microsoft 365, Dynamics 365, Windows 365, and Microsoft Power Platform (each, an "NCE Application"). To leverage the discounts offered by Microsoft for these applications and to pass those discounts through to you, we will purchase NCE Licenses for one (1) year terms for the NCE Applications required under the Quote. **As per Microsoft's requirements, NCE Licenses cannot be canceled once they are purchased and cannot be transferred to any other customer. Each NCE License that we purchase may require a one (1) or three (3) year term. For that reason, you understand and agree that regardless of the reason for termination of the Services, you are required to pay for all applicable NCE Licenses in full for the entire term of those licenses.** Provided that you have paid for the NCE Licenses in full, you will be permitted to use those licenses until they expire, even if you move to a different managed service provider.

Additional Terms

Authenticity

Everything in the managed environment must be genuine and licensed—including all hardware, software, etc. If we ask for proof of authenticity and/or licensing, you must provide us with such proof. All minimum hardware or software requirements as indicated in a Quote or this Services Statement ("Minimum Requirements") must be implemented and maintained as an ongoing requirement of us providing the Services to you.

Monitoring Services; Alert Services

Unless otherwise indicated in the Quote, all monitoring and alert-type services are limited to detection and notification functionalities only. Monitoring levels will be set by Layer 9, and Client shall not modify these levels without our prior written consent.

Remediation

Unless otherwise provided in the Quote, remediation services will be provided in accordance with the recommended practices of the managed services industry. Client understands and agrees that remediation services are not intended to be, and will not be, a warranty or guarantee of the functionality of the Environment, or a service plan for the repair of any particular piece of managed hardware or software. Some remediation fees may incur fees, in which case a new Quote will be created.

Configuration of Third Party Services

Certain third party services provided to you under this Service Statement may provide you with administrative access through which you could modify the configurations, features, and/or functions ("Configurations") of those services. However, any modifications of Configurations made by you without our knowledge or authorization could disrupt the Services and/or or cause a significant increase in the fees charged for those third party services. For that reason, we strongly advise you to refrain from changing the Configurations unless we authorize those changes. You will be responsible for paying any increased fees or costs arising from or related to changes to the Configurations.

Dark Web Monitoring

Our dark web monitoring services utilize the resources of third party solution providers. Dark web monitoring can be a highly effective tool to reduce the risk of certain types of cybercrime; however, we do not guarantee that the dark web monitoring service will detect all actual or potential uses of your designated credentials or information.

Modification of Environment

Changes made to the Environment without our prior authorization or knowledge may have a substantial, negative impact on the provision and effectiveness of the Services and may impact the fees charged under the Quote. You agree to refrain from moving, modifying, or otherwise altering any portion of the Environment without our prior knowledge or consent. For example, you agree to refrain from adding or removing hardware from the Environment, installing applications on the Environment, or modifying the configuration or log files of the Environment without our prior knowledge or consent.

Co-Managed Environment

In co-managed situations (e.g., where you have designated other vendors or personnel, or "Co-managed Providers," to provide you with services that overlap or conflict with the Services provided by us), we will endeavor to implement the Services an efficient and effective manner; however, (a) we will not be responsible for the acts or omissions of Co-Managed Providers, or the remediation of any problems, errors, or downtime associated with those acts or omissions, and (b) in the event that a Co-managed Provider's determination on an issue differs from our position on a Service-related matter, we will yield to the Co-Managed Provider's determination and bring that situation to your attention

Anti-Virus; Anti-Malware

Our anti-virus / anti-malware solution will generally protect the Environment from becoming infected with new viruses and malware ("Viruses"); however, Viruses that exist in the Environment at the time that the security solution is implemented may not be capable of being removed without additional services, for which a charge may be incurred. We do not warrant or guarantee that all Viruses and malware will be capable of being detected, avoided, or removed, or that any data erased, corrupted, or encrypted by malware will be recoverable. In order to improve security awareness, you agree that Layer 9 or its designated third party affiliate may transfer information about the results of processed files, information used for URL reputation determination, security risk tracking, and statistics for protection against spam and malware. Any information obtained in this manner does not and will not contain any personal or confidential information.

Breach/Cyber Security Incident Recovery

Unless otherwise expressly stated in the Quote, the scope of the Services does not include the remediation and/or recovery from a Security Incident (defined below). Such services, if requested by you, will be provided on a time and materials basis under our then-current hourly labor rates. Given the varied number of possible Security Incidents, we cannot and do not warrant or guarantee (i) the amount of time required to remediate the effects of a Security Incident (or that recovery will be possible under all circumstances), or (ii) that all data impacted by the incident will be recoverable. For the purposes of this paragraph, a Security Incident means any unauthorized or impermissible access to or use of the Environment, or any unauthorized or impermissible disclosure of Client's confidential information (such as user names, passwords, etc.), that (i) compromises the security or privacy of the information or applications in, or the structure or integrity of, the Environment, or (ii) prevents normal access to the Environment, or impedes or disrupts the normal functions of the Environment.

Environmental Factors

Exposure to environmental factors, such as water, heat, cold, or varying lighting conditions, may cause installed equipment to malfunction. Unless expressly stated in the Quote, we do not warrant or guarantee that installed equipment will operate error-free or in an uninterrupted manner, or that any video or audio equipment will clearly capture and/or record the details of events occurring at or near such equipment under all circumstances.

Fair Usage Policy

Our Fair Usage Policy ("FUP") applies to all Services that are described or designated as "unlimited." An "unlimited" service designation means that, subject to the terms of this FUP, you may use the service as reasonably necessary for you to enjoy the use and benefit of the service without incurring additional time-based or usage-based costs. However, unless expressly stated otherwise in the Quote, all unlimited services are provided during our normal business hours only and are subject to our technicians' availabilities, which cannot always be guaranteed. In addition, we reserve the right to assign our technicians as we deem necessary to handle issues that are more urgent, critical, or pressing than the request(s) or issue(s) reported by you. Consistent with this FUP, you agree to refrain from (i) creating

urgent support tickets for non-urgent or non-critical issues, (ii) requesting excessive support services that are inconsistent with normal usage patterns in the industry (*e.g.*, requesting support in lieu of training), (iii) requesting support or services that are intended to interfere, or may likely interfere, with our ability to provide our services to our other customers.

Hosted Email

You are solely responsible for the proper use of any hosted email service provided to you ("Hosted Email"). Hosted Email solutions are subject to acceptable use policies ("AUPs"), and your use of Hosted Email must comply with those AUPs. In all cases, you agree to refrain from uploading, posting, transmitting or distributing (or permitting any of your authorized users of the Hosted Email to upload, post, transmit or distribute) any prohibited content, which is generally content that (i) is obscene, illegal, or intended to advocate or induce the violation of any law, rule or regulation, or (ii) violates the intellectual property rights or privacy rights of any third party, or (iii) mischaracterizes you, and/or is intended to create a false identity or to otherwise attempt to mislead any person as to the identity or origin of any communication, or (iv) interferes or disrupts the services provided by Layer 9 or the services of any third party, or (v) contains Viruses, trojan horses or any other malicious code or programs. In addition, you must not use the Hosted Email for the purpose of sending unsolicited commercial electronic messages ("SPAM") in violation of any federal or state law. Layer 9 reserves the right, but not the obligation, to suspend Client's access to the Hosted Email and/or all transactions occurring under Client's Hosted Email account(s) if Layer 9 believes, in its discretion, that Client's email account(s) is/are being used in an improper or illegal manner.

Patch Management

We will keep all managed hardware and managed software current with critical patches and updates ("Patches") as those Patches are released generally by the applicable manufacturers. Patches are developed by third party vendors and, on rare occasions, may make the Environment, or portions of the Environment, unstable or cause the managed equipment or software to fail to function properly even when the Patches are installed correctly. We will not be responsible for any downtime or losses arising from or related to the installation or use of any Patch. We reserve the right, but not the obligation, to refrain from installing a Patch if we are aware of technical problems caused by a Patch, or we believe that a Patch may render the Environment, or any portion of the Environment, unstable.

Backup (BDR) Services

All data transmitted over the Internet may be subject to malware and computer contaminants such as viruses, worms and trojan horses, as well as attempts by unauthorized users, such as hackers, to access or damage Client's data. Neither Layer 9 nor its designated affiliates will be responsible for the outcome or results of such activities.

BDR services require a reliable, always-connected internet solution. Data backup and recovery time will depend on the speed and reliability of your internet connection. Internet and telecommunications outages will prevent the BDR services from operating correctly. In addition, all computer hardware is prone to failure due to equipment malfunction, telecommunication-related issues, etc., for which we will

be held harmless. Due to technology limitations, all computer hardware, including communications equipment, network servers and related equipment, has an error transaction rate that can be minimized, but not eliminated. Layer 9 cannot and does not warrant that data corruption or loss will be avoided, and Client agrees that Layer 9 shall be held harmless if such data corruption or loss occurs. **Client is strongly advised to keep a local backup of all of stored data to mitigate against the unintentional loss of data.**

Procurement

Equipment and software procured by Layer 9 on Client's behalf ("Procured Equipment") may be covered by one or more manufacturer warranties, which will be passed through to Client to the greatest extent possible. By procuring equipment or software for Client, Layer 9 does not make any warranties or representations regarding the quality, integrity, or usefulness of the Procured Equipment. Certain equipment or software, once purchased, may not be returnable or, in certain cases, may be subject to third party return policies and/or re-stocking fees, all of which shall be Client's responsibility in the event that a return of the Procured Equipment is requested. Layer 9 is not a warranty service or repair center. Layer 9 will facilitate the return or warranty repair of Procured Equipment; however, Client understands and agrees that (i) the return or warranty repair of Procured Equipment is governed by the terms of the warranties (if any) governing the applicable Procured Equipment, for which Layer 9 will be held harmless, and (ii) Layer 9 is not responsible for the quantity, condition, or timely delivery of the Procured Equipment once the equipment has been tendered to the designated shipping or delivery courier.

Technology Business Review; IT Strategic Planning

Suggestions and advice rendered to Client are provided in accordance with relevant industry practices, based on Client's specific needs and Layer 9's opinion and knowledge of the relevant facts and circumstances. By rendering advice, or by suggesting a particular service or solution, Layer 9 is not endorsing any particular manufacturer or service provider.

VCTO or VCIO Services

The advice and suggestions provided us in our capacity as a virtual chief technology or information officer will be for your informational and/or educational purposes only. Layer 9 will not hold an actual director or officer position in Client's company, and we will neither hold nor maintain any fiduciary realtionship with Client. Under no circumstances shall Client list or place the Layer 9 on Client's corporate records or accounts.

Sample Policies, Procedures.

From time to time, we may provide you with sample (*i.e.*, template) policies and procedures for use in connection with Client's business ("Sample Policies"). The Sample Policies are for your informational use only, and do not constitute or comprise legal or professional advice, and the policies are not intended to be a substitute for the advice of competent counsel. You should seek the advice of competent legal counsel prior to using or distributing the Sample Policies, in part or in whole, in any transaction. We do not warrant or guarantee that the Sample Policies are complete, accurate, or suitable for your (or your customers') specific needs, or that you will reduce or avoid liability by utilizing the Sample Policies in your (or your customers') business operations.

Penetration Testing; Vulnerability Assessment

You understand and agree that security devices, alarms, or other security measures, both physical and virtual, may be tripped or activated during the penetration testing process, despite our efforts to avoid such occurrences. You will be solely responsible for notifying any monitoring company and all law enforcement authorities of the potential for "false alarms" due to the provision of the penetration testing services, and you agree to take all steps necessary to ensure that false alarms are not reported or treated as "real alarms" or credible threats against any person, place or property. Some alarms and advanced security measures, when activated, may cause the partial or complete shutdown of the Environment, causing substantial downtime and/or delay to your business activities. We will not be responsible for any claims, costs, fees or expenses arising or resulting from (i) any response to the penetration testing services by any monitoring company or law enforcement authorities, or (ii) the partial or complete shutdown of the Environment by any alarm or security monitoring device.

No Third Party Scanning

Unless we authorize such activity in writing, you will not conduct any test, nor request or allow any third party to conduct any test (diagnostic or otherwise), of the security system, protocols, processes, or solutions that we implement in the managed environment ("Testing Activity"). Any services required to diagnose or remediate errors, issues, or problems arising from unauthorized Testing Activity is not covered under the Quote, and if you request us (and we elect) to perform those services, those services will be billed to you at our then-current hourly rates.

HaaS

You will use all Layer 9-hosted or Layer 9-supplied equipment and hardware (collectively, "Infrastructure") for your internal business purposes only. You shall not sublease, sublicense, rent or otherwise make the Infrastructure available to any third party without our prior written consent. You agree to refrain from using the Infrastructure in a manner that unreasonably or materially interferes with our other hosted equipment or hardware, or in a manner that disrupts or that is likely to disrupt the services that we provide to our other clientele. We reserve the right to throttle or suspend your access and/or use of the Infrastructure if we believe, in our sole but reasonable judgment, that your use of the Infrastructure is violates the terms of the Quote, this Service Statement, or the Agreement.

Obsolescence

If at any time any portion of the managed environment becomes outdated, obsolete, reaches the end of its useful life, or acquires "end of support" status from the applicable device's or software's manufacturer ("Obsolete Element"), then we may designate the device or software as "unsupported" or "non-standard" and require you to update the Obsolete Element within a reasonable time period. If you do not replace the Obsolete Element reasonably promptly, then in our discretion we may (i) continue to provide the Services to the Obsolete Element using our "best efforts" only with no warranty or requirement of remediation whatsoever regarding the operability or functionality of the Obsolete Element, or (ii) eliminate the Obsolete Element from the scope of the Services by providing written notice to you (email is sufficient for this purpose). In any event, we make no representation or warranty whatsoever regarding

any Obsolete Element or the deployment, service level guarantees, or remediation activities for any Obsolete Element.

Hosting Services

You agree that you are responsible for the actions and behaviors of your users of the Services. In addition, you agree that neither Client, nor any of your employees or designated representatives, will use the Services in a manner that violates the laws, regulations, ordinances, or other such requirements of any jurisdiction.

In addition, Client agrees that neither it, nor any of its employees or designated representatives, will: transmit any unsolicited commercial or bulk email, will not engage in any activity known or considered to be "spamming" and carry out any "denial of service" attacks on any other website or Internet service; infringe on any copyright, trademark, patent, trade secret, or other proprietary rights of any third party; collect, attempt to collect, publicize, or otherwise disclose personally identifiable information of any person or entity without their express consent (which may be through the person or entity's registration and/or subscription to Client's services, in which case Client must provide a privacy policy which discloses any and all uses of information that you collect) or as otherwise required by law; or, undertake any action which is harmful or potentially harmful to Layer 9 or its infrastructure.

Client is solely responsible for ensuring that its login information is utilized only by Client and Client's authorized users and agents. Client's responsibility includes ensuring the secrecy and strength of user identifications and passwords. Layer 9 shall have no liability resulting from the unauthorized use of Client's login information. If login information is lost, stolen, or used by unauthorized parties or if Client believes that any hosted applications or hosted data has been accessed by unauthorized parties, it is Client's responsibility to notify Layer 9 immediately to request the login information be reset or unauthorized access otherwise be prevented. Layer 9 will use commercially reasonable efforts to implement such requests as soon as practicable after receipt of notice.

Licenses

If we are required to re-install or replicate any software provided by you as part of the Services, then it is your responsibility to verify that all such software is properly licensed. We reserve the right, but not the obligation, to require proof of licensing before installing, re-installing, or replicating software into the managed environment. The cost of acquiring licenses is not included in the scope of the Quote unless otherwise expressly stated therein.