SERVICE GUIDE

SECURE VIP SUBSCRIPTION SERVICE

Computer Corner, Inc.

Last Updated: November 2023

Service Guide

Secure VIP Subscription Service

This Services Guide contains provisions that define, clarify, and govern the scope of the services described in the quote that has been provided to you (the "Quote"), as well as the policies and procedures that we follow (and to which you agree) when we provide a service to you or facilitate a service for you. If you do not agree with the terms of this Services Guide, you should not sign the Quote and you must contact us for more information.

This Services Guide is our "owner's manual" that generally describes all managed services provided or facilitated by Computer Corner ("Computer Corner," "we," "us," or "our"); **however, only those services specifically described in the Quote will be facilitated and/or provided to you (collectively, the "Services").**

This Services Guide is governed under our Master Services Agreement ("MSA"). You may locate our MSA through the link in your Quote, online at www.compcorner.com/legal, or, if you want, we will send you a copy of the MSA by email upon request. Capitalized terms in this Services Guide will have the same meaning as the capitalized terms in the MSA, unless otherwise indicated below.

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.

Please read this Services Guide carefully and keep a copy for your records.

Important Contact Information for Computer Corner, Inc.

Company Phone:	(505) 881-2333
Company Fax:	(505) 881-1300
Contact Email:	SecureVIP@compcorner.com
Company Website:	www.compcorner.com

How Can I Get Help or Tech Support?

1. By Sending Us an Email
    a. send an email to help@compcorner.com
2. By Calling Us
    a. call us at 505-881-2333, option 1
3. By Chatting With Us – Coming Soon!
    a. our first priority is your security, so our testing process is rigorous and thorough. We'll let you know when it is available!
4. Billing Help
    a. send an email to SecureVIP@compcorner.com

Table of Contents

Secure VIP Subscription Plan Matrix

The Secure VIP Subscription Plan Matrix is updated regularly and can be viewed on our website at www.compcorner.com/legal.

Onboarding for Secure VIP

In the Onboarding phase of our services, we will prepare your computer(s) for the monthly managed services described in the Quote. During this phase, we will work with you to review the information we need to prepare the targeted environment, and we may also:

- Uninstall any monitoring tools or other software installed by previous IT service providers.
- Uninstall any previous endpoint protection and install our managed security solutions (as indicated in the Quote).
- Install remote support access agents (*i.e.*, software agents) on each managed device to enable remote support.
- Configure Windows® and application patch management agent(s) and check for missing security updates.
- Uninstall unsafe applications or applications that are no longer necessary.
- Optimize device performance including disk cleanup and endpoint protection scans, otherwise known as a Computer Tune-Up Service.
- Review Windows® firewall configuration.
- As applicable, make recommendations for changes that should be considered.

This 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.**

The duration of the onboarding process depends on many factors, many of which may be outside of our control—such as product availability/shortages, required third party vendor input, etc. As such, we can estimate, but cannot guarantee, the timing and duration of the onboarding process. We will keep you updated as the onboarding process progresses.

Ongoing / Recurring Managed 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. Some ongoing/recurring services will begin with the commencement of onboarding services; others will begin when the onboarding process is completed. Please direct any questions about start or "go live" dates to your technician.

The following Services, if listed in the Quote, will be provided to you as part of your Managed Services Agreement. For services provided on a Time and Material basis, please refer to the appropriate Service Guide – Computer Sales & Service located at www.compcorner.com/legal.

ENDPOINT HARDENING

SERVICES	GENERAL DESCRIPTION
Patching & Asset 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 below. • Review and installation of updates and patches for supported software • 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. • Deploy, manage, and monitor the installation of approved service packs, security updates and firmware updates as deemed necessary on all applicable managed hardware. • Review and installation of updates and patches for Windows and supported software.
Remote Monitoring & Remote Desktop	• Endpoint protection agent monitoring, alerting us to potential security vulnerabilities. • Routine operating system inspection and cleansing. • Asset inventory and workstation and software information collection. • Secure remote connectivity to the workstation and collaborative screen sharing.
Next-Generation Endpoint Antivirus & Malware Protection	Primary endpoint security layer. Software agents installed in covered devices protect against malware and prevent intruder access, protect against ransomware encryption, and are supported by a 24x7x365 Security Operations Center. • **Local File Scanning**. Using real-time low-impact file and signature scanning, local files and Windows registry are scanned for changes or malicious behavior. • **Real-time Cloud Scanning**. Any unknown files or potential threats are sent to a cloud server for further inspection. • **Sandbox and Backdoor Inspection**. If scanned files do not appear as malware, they will be isolated in the sandboxing system and examined for malicious behavior. • **Behavior-based Scanning**. Once a file is allowed to execute, the processes will be monitored by Artificial Intelligence to identify malicious behavior. If the process tries to contact an outside source ("Command and Control"), that malicious communication is stopped at its roots. **Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**

ENDPOINT HARDENING

SERVICES	GENERAL DESCRIPTION
Ransomware Encryption Protection	Each day, over 200,000 new ransomware strains are detected, meaning that every minute brings us 140 new ransomware strains capable of evading detection and inflicting irreparable damage. **Ransomware operators will never stop, not even after the victim pays the demanded ransom.** The threat actor could withhold the data, plant spyware on the victim's network or endpoints, and conduct similar attacks. Computers afflicted by ransomware can experience debilitating side-effects such as critical errors and performance issues. **Countering ransomware means stopping the file encryption process. Antivirus is not enough.** Ransomware Encryption Protection by Heimdal is anti-ransomware technology capable of arresting malicious encryption as it unfolds. Owing to Heimdal Security's advanced Intelligence, Ransomware Encryption Protection can distinguish between normal operating system encryption processes and malicious attempts. **Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Threat Hunting & Action Center	The Threat-hunting and Action Center leverages the industry-renowned MITRE ATT&CK techniques to help security teams proactively classify and prioritize security risks, hunt anomalies, and neutralize threats in a secure environment. This takes place behind the scenes, without disrupting users or impacting productivity.
Security Operations Center	A Security Operations Center (SOC) is a centralized unit within an organization responsible for monitoring, detecting, analyzing, and responding to security incidents or events. Its primary function is to ensure the security of an organization's information systems, network infrastructure, and digital assets. The SOC team uses various security tools, techniques, and procedures to identify and prevent cyber threats, vulnerabilities, and attacks. The SOC operates 24/7 and plays a critical role in the organization's overall security posture. The team comprises security analysts, incident responders, forensic experts, and other cybersecurity professionals who work together to protect the organization from potential security breaches. The job roles in a SOC team may vary depending on the organization's size, structure, and security needs. Each role has its particularity, driving ever further the (collective) effort to identify, monitor, respond, mitigate, and hound down cyber threats. Here's what a fully staffed SOC team looks like: • Security Analyst • Incident Responder. • Threat Hunter. • Security Engineer. • SOC Manager. • Compliance Specialist. Source: https://heimdalsecurity.com/blog/security-operations-center-soc/

LOCAL TECH SUPPORT

SERVICES	GENERAL DESCRIPTION
Remote & In-Person Tech Support	Some of our Secure VIP plans include a block of Tech Support hours. These Tech Support hours can be used during business hours throughout the contract year. **Our LOCAL team of tech experts** are available to provide tech support, either remotely or in-person by appointment. Tech support hours can be used for many issues, including, but not limited to: • Windows Operation System issues. • Microsoft Office issues. • Computer Tune-ups. • Malware removal. Standard Malware and Computer Tune-ups are maintenance tasks. Some problems require a reload of the OS, which is not covered by this plan.
Affiliate Product Support	There are some services that we can't provide directly, but our clients ask for recommendations so that they know which product to choose for themselves. We only endorse services we've tested or are highly recommended by industry peers. If you purchase a plan after clicking any of our referral links below, we may receive a small commission. However, there's no extra cost to you. • If you sign up with one of our Affiliate Partners, we are happy to provide basic support for the Affiliate Service, as part of your Tech Support block of hours. • However, the Affiliate Partner is the best source of support for their product. We can help you get access to their Tech Support for the fastest service. Our Affiliate Disclosure can be read here: https://www.compcorner.com/affiliate-disclosure
Items Not Covered by Tech Support	Our Tech Support hours are intended for use for "software" related issues, such as Operation System, Microsoft Office, Tune-Ups, and Malware issues. If we must put "hands on" or "crack open" a computer to perform a repair, the time is billable, and you will be provided a quote. **The good news: all Secure VIP subscribers get 20% off all non-covered services!*** "Hands On" service includes, but is not limited to: • Hard drive replacement. • RAM or battery installation. • Computer re-builds. • OS Reload due to extensive corruption or malware infection. • Data transfers. * Discount applies to all services except training and on-site services; discount does not apply to parts. For additional information about our regular services, please review our Service Guide – Computer Sales & Service, located at https://www.compcorner.com/legal

OTHER SUPPORT ITEMS AND GENERAL TERMS

SERVICES	GENERAL DESCRIPTION
Affiliate Program (applies to all affiliate products referred by Computer Corner, in which Computer Corner may receive a commission for the referral)	There are some services that we can't provide directly, but our clients ask for recommendations so that they know which product to choose for themselves. We only endorse services we've tested or are highly recommended by industry peers. If you purchase a plan after clicking any of our referral links below, we may receive a small commission. However, there's no extra cost to you. • Some of the products for whom we have an Affiliate Partner include: • Password Manager • VPN Service • Data Recovery Service Our current list of Affiliate Partners can be found here: https://www.compcorner.com/resources Our Affiliate Disclosure can be read here: https://www.compcorner.com/affiliate-disclosure
Software Licensing (applies to all software licensed by or through Computer Corner)	All software provided to you by or through Computer Corner's Secure VIP Program is licensed, not sold, to you ("Software"). In addition to any Software-related requirements described in Computer Corner's Master Services Agreement, Software may also be subject to end user license agreements (EULAs), acceptable use policies (AUPs), and other restrictions all of which must be strictly followed by you and any of your authorized users. When installing/implementing software licenses in the managed environment or as part of the Services, we may accept (and you agree that we may accept) any required EULAs or AUPs on your behalf. **You should assume that all Software has an applicable EULA and/or AUP to which your authorized users and you must adhere.** If you have any questions or require a copy of the EULA or AUP, please contact us.

Covered Equipment / Hardware / Software

Managed Services will be applied to the number of devices indicated in the Quote ("Covered Hardware"). The list of Covered Hardware may be modified by mutual consent (email is sufficient for this purpose); however, we reserve the right to modify the list of Covered Hardware at any time if we discover devices that were not previously included in the list of Covered Hardware and which are receiving Services, or as necessary to accommodate changes to the quantity of Covered Hardware.

Unless otherwise stated in the Quote, Covered Devices will only include technology assets (such as computers, servers, and networking equipment) owned by the Client's organization. As accommodation, Computer Corner may provide guidance in connecting a personal device to the Client's organization's technology, but support of personal devices is generally not included in the Scope of Services.

If the Quote indicates that the Services are billed on a "per user" basis, then the Services will be provided for up to **one (1)** Device used by the number of users indicated in the Quote. A "Device" is a device that (i) is owned or leased by Client, and (ii) has installed on it a software agent through which we (or our designated Third Party Providers) can monitor the device.

We will provide support for any software applications that are licensed through us. Such software ("Supported Software") will be supported on a "best effort" basis 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 the Quote and will be provided to you on a "best-effort" basis and a time and materials basis with no guarantee of remediation. Should our technicians provide you with advice concerning non-Supported Software, the provision of that advice should be viewed as accommodation, not an obligation, to you.

If we are unable to remediate an issue with non-Supported Software, then you will be required to contact the manufacturer/distributor of the software for further support. Please note: Manufacturers/distributors of such software may charge fees, some of which may be significant, for technical support; therefore, we strongly recommend that you maintain service or support contracts for all non-Supported Software ("Service Contract"). If you request that we facilitate technical support for non-Supported Software and if you have a Service Contract in place, our facilitation services will be provided at no additional cost to you.

In this Services Guide, Covered Hardware and Supported Software will be referred to as the "Environment" or "Covered Equipment."

Physical Locations Covered by Services

Services will be provided remotely unless, in our discretion, we determine that an in-person or on-site visit is required. Computer Corner in-person or on-site visits are subject to technician availability. Additional fees will apply for onsite visits.

Minimum Requirements / Exclusions

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

- 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.
- 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 Services Guide.
- Client must provide us with exclusive administrative privileges to the Environment.

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 Computer Corner. Without limiting the foregoing, the following services are expressly excluded, and if required to be performed, must be agreed upon by Computer Corner 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.
- Battery backup replacement.
- Equipment relocation.
- The cost to bring the managed environment up to these minimum requirements (unless otherwise noted in the Quote).
- 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 our business hours (currently M-F, 8 AM – 5 PM Mountain Time, excluding legal holidays and Computer Corner-observed holidays as listed below), unless otherwise specifically stated in the Quote or as otherwise described below.

We will respond to problems, errors, or interruptions in the provision of the Services during business hours in the timeframe(s) described below. Severity levels will be determined by Computer Corner in our discretion after consulting with the Client. All remediation services will be provided remotely unless, at our discretion, we determine that an in-person or on-site visit is required. Computer Corner in-person or on-site visits are subject to technician availability. Additional fees will apply for onsite visits.

Trouble / Severity	Response Time
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.
Long Term Project, Preventative Maintenance	Response within four (4) business days after notification.

* All time frames are calculated as of the time that we are notified of the applicable issue / problem by Client through our designated support portal, help desk, or by telephone at the telephone number listed in the Quote. Notifications received in any manner other than described herein may result in a delay in the provision of remediation efforts.

Computer Corner-Observed Holidays: Computer Corner observes the following holidays:

- New Year's Day
- Memorial Day
- Independence Day
- Labor Day
- Thanksgiving Day
- The day following Thanksgiving Day
- Christmas Day

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.

Travel Time. If onsite services are provided, time spent traveling beyond 15 miles or 45 minutes (*e.g.,* locations that are beyond 15 miles or 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, you will be billed 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.

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 Computer Corner'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").

Per Seat/Per Device Licensing: **Regardless of the reason for the termination of the Services, you will be required to pay for all per seat or per device licenses that we acquire on your behalf. Please see "Access Licensing" in the Fees section above for more details.**

Removal of Software Agents; Return of Firewall & Backup Appliances: Unless we expressly direct you to do so, you will not remove or disable, or attempt to remove or disable, any software agents that we installed in the managed environment or any of the devices on which we installed software agents. Doing so without our guidance may make it difficult or impracticable to remove the software agents, which could result in network vulnerabilities and/or the continuation of license fees for the software agents for which you will be responsible, and/or the requirement that we remediate the situation at our then-current hourly rates, for which you will also be responsible. Depending on the particular software agent and the costs of removal, we may elect to keep the software agent in the managed environment but in a dormant and/or unused state.

Within ten (10) days after being directed to do so, Client will remove, package and ship, at Client's expense and in a commercially reasonable manner, all hardware, equipment, and accessories provided to Client by Computer Corner that were used in the provision of the Services. If you fail to timely return all equipment to us, or if the equipment is returned to us damaged (normal wear and tear excepted), then we will have the right to charge you, and you hereby agree to pay, the replacement value of all such unreturned or damaged equipment.

Additional Policies

Sales Returns

If you want to return or exchange your purchase, please know that the time period begins the day you receive your product(s) and applies to new, clearance, open box, refurbished and pre-owned products. Unless noted otherwise below, most un-opened and un-damaged products may be returned within seven (7) days for full credit. Most products may be returned within fifteen (15) days for partial credit, after a 25% restocking fee, and within thirty (30) days for exchange for a similar product if the original product is defective. Bring your receipt, the credit card used to make your purchase, and a valid photo ID to facilitate your available return option. The following additional terms apply to returns:

a. **Computer Systems**. Computer systems that are not custom builds may be returned with fifteen (15) days for partial credit, net of a 25% restocking fee, to cover the cost of reformatting the hard drive and preparing the product for re-sale as a used item to another customer.

b. **Special Orders or Custom Orders are Final.** Special order parts are final. Custom orders made especially for you are nonreturnable.

c. **Software Sales are Final.** All software sales are final, due to strictly imposed copyright laws.

d. **Bundle Discounts and Free Items**. If you received a discount or free item by purchasing multiple items together, you may lose some or all that benefit if part of the bundle is returned.

System and Service Warranty

If a defect is discovered and reported to Computer Corner, Inc. during the applicable warranty period, Computer Corner, Inc. will, AT ITS OPTION, repair or replace the product at no charge to you. If the service performed is deemed to be unrelated to any defects in parts or workmanship, both travel time and service time will be billed to the customer at the current service rate. The warranty applies only to hardware and peripheral products. Software, printers, and manuals are licensed and/or warranted pursuant to separate written statements by the manufacturer/publisher.

a. **Equus System Warranty.** All new Equus computer systems and components are warranted against defects in materials and workmanship for a period of one (1) year or three (3) years from the date of the original invoice, as noted on the invoice. Extended warranties are available for purchase and extend the covered warranty period from the original invoice date.

b. **Computer Corner Reconditioned ("CCR") System and Product Warranty.** All reconditioned or refurbished systems sold by Computer Corner are warranted against defects in materials and workmanship from the date of the original invoice as follows: desktops for six (6) months; laptops, including battery, for ninety (90) days. Extended warranties are available for purchase and extend the covered warranty period from the original invoice date. Unless otherwise stated on the invoice, all used inventory is covered by a limited warranty against parts and labor defects for a period of ninety (90) days from the date of the original invoice.

c. **Original Equipment Manufacturer ("OEM") System Warranty.** All new OEM systems are covered by the terms and conditions of the warranty provided by the manufacturer, including any extended warranties sold by Computer Corner.

d. **Repair and Service Warranty**. All labor, new parts, and used or reconditioned parts are warranted for ninety (90) days from the service date. This warranty applies only to the original purchaser named on the invoice and is not transferable. The warranty begins on the date of the original invoice date, regardless of any repairs or replacement by Computer Corner during the warranty period.

e. **Obtaining Warranty Service**. Before bringing any product to Computer Corner, first call the Service Department at (505) 881-2333. We may be able to fix the problem over the phone or via remote service. **All warranties are Depot Warranties, which require the product to be brought back to the store for warranty service if phone or remote service is unsuccessful**.

Warranty Exclusions

The warranty stated herein is void if the product has been modified without the WRITTEN permission of Computer Corner, Inc. or if any serial number has been removed/altered and/or the warranty seal is broken. Product failures resulting from misuse of product, electrical surges, lightning or other "Acts of God" are not product defects, and the repair or replacement of products under these circumstances is not covered by warranty. Computer Corner, Inc. is not responsible for repairing or replacing system files or other software files on a system on which illegal or "pirated" software has been installed. Computer Corner, Inc. shall have no obligation to enhance or update ANY UNIT once the unit is built and prepped for delivery. Service performed, including travel time, that is not covered by warranty will be billed to you at the current service rate.

Data Integrity

When reloading the Operating System on your computer, Computer Corner will back up the data we reasonably can from your computer and return this data to a folder labeled "OLD HARD DRIVE", located on the desktop, or on external media, as requested by the customer. Computer Corner may not be able to backup all your data, and, in some situations such as a failed hard drive, data backup may not be possible.

COMPUTER CORNER IS NOT RESPONSIBLE FOR YOUR DATA.

Data Backup and Automatic Backup and Disaster Recovery ("BDR") Services

Computer Corner, Inc. is not responsible for damage as a result of accidents, misuse, or abuse of equipment. Computer Corner, Inc. is not responsible for lost data or files. **Data backups should be performed by all computer users on a regular basis.** 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 Computer Corner 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. Computer Corner cannot and does not warrant that data corruption or loss will be avoided, and Client agrees that Computer Corner shall be held harmless if such data corruption or loss occurs. **Client is strongly advised to keep a local backup of all stored data to mitigate against the unintentional loss of data.**

Virus and Malware Removal

After we have removed viruses and/or malware, the utmost care should be taken to prevent reinfection. We strongly recommend the installation of a reputable anti-malware software program. We are happy to install our recommended program with the purchase at time of malware service. *Reinfection virus removal service is not covered under warranty*. Reinfection typically results from the user performing an action such as opening an infected e-mail or attachment or downloading a file that is infected. Please do not operate your computer system without anti-virus protection, open e-mails from unknown sources, or download files without first scanning them with your anti-virus software.

Anti-Virus; Anti-Malware Solution

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. To improve security awareness, you agree that Computer Corner 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 or systems impacted by the incident will be recoverable or remediated. 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 managed environment, or (ii) prevents normal access to the managed environment, or impedes or disrupts the normal functions of the managed environment.

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—including ours. 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 Computer Corner 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. Computer Corner 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 Computer Corner believes, in its discretion, that Client's email account(s) is/are being used in an improper or illegal manner.

Abandoned Property

All articles left for computer service or repair that are not retrieved within thirty (30) days from service date, will be subject to a daily storage fee of $1.50 per day. After three (3) months from service date, abandoned articles will be disposed of according to Computer Corner's discretion, pursuant to Sections 48-3-22 through 48-3-27 NMSA 1978.

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 Guide ("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 Computer Corner, and Client shall not modify these levels without our prior written consent.

Configuration of Third-Party Services

Certain third-party services provided to you under an Order 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 authorization could disrupt the Services and/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 in 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

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" or which are not expressly capped in the number of available usage hours per month. An "unlimited" service designation means that, subject to the terms of this FUP, you may use the applicable 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' availability, 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.

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.

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 are 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.

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.

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.

Acceptable Use Policy

The following policy applies to all hosted services provided to you, including but not limited to (and as applicable) hosted applications, hosted websites, hosted email services, and hosted infrastructure services ("Hosted Services").

Computer Corner does not routinely monitor the activity of hosted accounts except to measure service utilization and/or service uptime, security-related purposes and billing-related purposes, and as necessary for us to provide or facilitate our managed services to you; however, we reserve the right to monitor Hosted Services at any time to ensure your compliance with the terms of this Acceptable Use Policy (this "AUP") and our master services agreement, and to help monitor and ensure the safety, integrity, reliability, or security of the Hosted Services.

Similarly, we do not exercise editorial control over the content of any information or data created on or accessible over or through the Hosted Services. Instead, we prefer to advise our customers of inappropriate behavior and any necessary corrective action. If, however, Hosted Services are used in violation of this AUP, then we reserve the right to suspend your access to part or all of the Hosted Services without prior notice.

Violations of this AUP: The following constitute violations of this AUP:

- **Harmful or illegal uses**: Use of a Hosted Service for illegal purposes or in support of illegal activities, to cause harm to minors or attempt to contact minors for illicit purposes, to transmit any material that threatens or encourages bodily harm or destruction of property or to transmit any material that harasses another is prohibited.
- **Fraudulent activity**: Use of a Hosted Service to conduct any fraudulent activity or to engage in any unfair or deceptive practices, including but not limited to fraudulent offers to sell or buy products, items, or services, or to advance any type of financial scam such as "pyramid schemes," "Ponzi schemes," and "chain letters" is prohibited.
- **Forgery or impersonation**: Adding, removing, or modifying identifying network header information to deceive or mislead is prohibited. Attempting to impersonate any person by using forged headers or other identifying information is prohibited. The use of anonymous remailers or nicknames does not constitute impersonation.
- **SPAM**: Computer Corner has a zero tolerance policy for the sending of unsolicited commercial email ("SPAM"). Use of a Hosted Service to transmit any unsolicited commercial or unsolicited bulk e-mail is prohibited. You are not permitted to host, or permit the hosting of, sites or information that is advertised by SPAM from other networks. To prevent unnecessary blacklisting due to SPAM, we reserve the right to drop the section of IP space identified by SPAM or denial-of-service complaints if it is clear that the offending activity is causing harm to parties on the Internet, if open relays are on the hosted network, or if denial of service attacks are originated from the hosted network.
- **Internet Relay Chat (IRC)**. The use of IRC on a hosted server is prohibited.
- **Open or "anonymous" proxy**: Use of open or anonymous proxy servers is prohibited.
- **Cryptomining.** Using any portion of the Hosted Services for mining cryptocurrency or using any bandwidth or processing power made available by or through a Hosted Services for mining cryptocurrency, is prohibited.
- **Hosting spammers**: The hosting of websites or services using a hosted server that supports spammers, or which causes (or is likely to cause) our IP space or any IP space allocated to us or our customers to be listed in any of the various SPAM databases, is prohibited. Customers violating this policy will have their server

immediately removed from our network and the server will not be reconnected until such time that the customer agrees to remove all traces of the offending material immediately upon reconnection and agree to allow Computer Corner to access the server to confirm that all material has been completely removed. Any subscriber guilty of a second violation may be immediately and permanently removed from the hosted network for cause and without prior notice.

- **Email/message forging**: Forging any email message header, in part or whole, is prohibited.
- **Unauthorized access**: Use of the Hosted Services to access, or to attempt to access, the accounts of others or to penetrate, or attempt to penetrate, Computer Corner's security measures or the security measures of another entity's network or electronic communications system, whether or not the intrusion results in the corruption or loss of data, is prohibited. This includes but is not limited to accessing data not intended for you, logging into or making use of a server or account you are not expressly authorized to access, or probing the security of other networks, as well as the use or distribution of tools designed for compromising security such as password guessing programs, cracking tools, or network probing tools.
- **IP infringement**: Use of a Hosted Service to transmit any materials that infringe any copyright, trademark, patent, trade secret or other proprietary rights of any third party, is prohibited.
- **Collection of personal data**: Use of a Hosted Service to collect, or attempt to collect, personal information about third parties without their knowledge or consent is prohibited.
- **Network disruptions and sundry activity**. Use of the Hosted Services for any activity which affects the ability of other people or systems to use the Hosted Services or the internet is prohibited. This includes "denial of service" (DOS) attacks against another network host or individual, "flooding" of networks, deliberate attempts to overload a service, and attempts to "crash" a host.
- **Distribution of malware**: Intentional distribution of software or code that attempts to and/or causes damage, harassment, or annoyance to persons, data, and/or computer systems is prohibited.
- **Excessive use or abuse of shared resources**: The Hosted Services depend on shared resources. Excessive use or abuse of these shared network resources by one customer may have a negative impact on all other customers. Misuse of network resources in a manner which impairs network performance is prohibited. You are prohibited from excessive consumption of resources, including CPU time, memory, and session time. You may not use resource-intensive programs which negatively impact other customers or the performance of our systems or networks.
- **Allowing the misuse of your account**: You are responsible for any misuse of your account, even if the inappropriate activity was committed by an employee or independent contractor. You shall not permit your hosted network, through action or inaction, to be configured in such a way that gives a third party the capability to use your hosted network in an illegal or inappropriate manner. You must take adequate security measures to prevent or minimize unauthorized use of your account. It is your responsibility to keep your account credentials secure.

To maintain the security and integrity of the hosted environment, we reserve the right, but not the obligation, to filter content, DNS requests, or website access for any web requests made from within the hosted environment.

Revisions to this AUP: We reserve the right to revise or modify this AUP at any time. Changes to this AUP shall not be grounds for early contract termination or non-payment.