Service Statement

This Service Statement contains provisions that define, clarify, and govern the services described in the quote to which it is attached (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 American PCS, Inc. ("American PCS"); 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.

- Uninstall any monitoring tools and other MSP software installed by previous IT consultants.
- Compile a full inventory of all protected devices including servers, workstations, laptops, and networking devices.
- Uninstall any previous security products and install our managed security solutions.
- Install remote support access application on each managed device to enable remote support.
- Configure patch management application and check for missing security updates.
- Uninstall identified unsafe applications and review applications that are no longer necessary.
- Optimize device performance including disk cleanup, virus removal, and security scans.
- Review firewall configuration and other network infrastructure devices.
- Review status of battery backup protection on all servers and networking devices.
- Stabilize network and assure that all applicable devices can securely access the necessary resources.
- Review and document current server configurations and status.
- Determine existing backup strategy and status; prepare backup options for consideration.
- Review password policies and update user and device passwords.
- As applicable, make recommendations for changes that should be considered to the managed environment.

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 completion of onboarding services; therefore, any delays or interruptions to the onboarding services may delay the commencement of ongoing/recurring services.

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

Freedom Services

SERVICES	GENERAL DESCRIPTION
Remote Monitoring and Management	Software agents installed in Covered Equipment (defined below) report status and events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below.
Unlimited Remote Helpdesk / Onsite Support	• Remote support provided during normal business hours for managed devices and covered software • Tiered-level support provides a smooth escalation process and helps to ensure effective solutions. • If remote efforts are unsuccessful then American PCS will dispatch a technician to the Client's premises to resolve covered incidents (timing of onsite support is subject to technician availability and scheduling) • Covered devices may include servers, workstations, laptops, virtual machines, and networking devices
Remote Infrastructure Maintenance	• Configuration, monitoring, and preventative maintenance services provided for the managed IT infrastructure
Remote Workforce Assistance	• Remote workstations will be provided 24/7 monitoring and remote assistance
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 backups • Preventive maintenance and management of backup software • Firmware and software updates of backup appliance • Problem analysis by the network operations team • Monitoring of backup successes and failures 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 8:00 am to 5:00 pm Central time. • Request Method. Requests to restore backed up data should be made through one of the following methods: ○ Email: help@american-pcs.com

	○ Telephone: 712-309-9110 • 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 and internet bandwidth.
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	• Firewalls help to prevent hackers from accessing internal network(s) from outside the network(s), while providing secure and encrypted remote network access; antivirus scanning of traffic, website content filtering, SSL inspection, and application control. • Firewalls will be monitored for uptime and errors with alerts configured to generate trouble tickets • Firmware and security updates will be applied as deemed necessary • Minor configuration changes will be made to resolves issues
Email Support	• Baseline managed email protection from phishing, business email compromise (BEC), SPAM, and email-based malware. • Unusual activity and risky sign-in alerting • E-mail management including the creation, configuration, or deletion of e-mail accounts, shared mailboxes, groups, and distribution lists
Automation	• Automation is a powerful tool to reduce downtime, assist with problem resolution, and even self-heal many issues • When appropriate custom automation policies will be created and implemented
Multi Factor Authentication	• Support will be provided for multi factor authentication to secure on-premises and cloud-based applications. • Support of custom access policies based on role, device, location
Password Manager	• Password Managers provide a secure method for storing passwords and are strongly encouraged Support will be provided to configure and utilize password managers
Wi-Fi Services	• American PCS will maintain, monitor, and manage the wireless system, including hardware and software updates. • American PCS will provide remote support services during normal business hours to assist with device connectivity issues. (Support services will be provided on a “best efforts” basis only, and Client understands that some end-user devices may not connect to the wireless network, or they may connect but not perform well).

vCIO Services	• The Freedom Services solution does not stop with excellent customer service and rapid problem resolution. It includes vCIO services to provide a business minded focus on IT management.
	  • Budget Forecasting
	  • Strategic Planning
	  • Consulting
	  • Asset Tracking
	• This is achieved by striving to fully understand the core-processes of the business and its inner workings. Only then can the client's IT run in accordance with the company's vision

The Freedom Service Plan (above) does not include advanced security-related services. Security-related services are provided through our Freedom Defense Plans, which are described below and which must be purchased separately; please see your Quote to determine which Freedom Defense Plan, if any, you have purchased. If you did not purchase a Freedom Defense Plan then those security-related services described in our Freedom Defense Plans, if requested or required by you, must be agreed upon by us in writing and will be provided to you on a time and materials basis.

Our Freedom Defense Plans offer increasing security options, with Plan 1 being our basic plan, and Plan 4 being our most comprehensive option.

Freedom Defense Plan 1

SERVICES	GENERAL DESCRIPTION
Overview	• Freedom Defense provides a powerful and robust security solution. In addition to the technical features listed below, it includes American PCS labor to restore computer systems to an operational state after a security breach or ransomware attack. • Freedom Defense Plan 1 includes up to 50 hours labor per incident with no more than 70 hours in any one month
End User Security Awareness Training	• Online, on-demand training videos (multi-lingual). • Online, on-demand quizzes to verify employee retention of training content. • Baseline testing to assess the phish-prone percentage of users; simulated phishing email campaigns designed to educate employees about security threats.
Freedom EDR	• Endpoint Detection and Response is a next generation anti-virus that has behavioral AI to stop known and unknown threats by evaluating the behavior in real time • EDR (Endpoint Detection and Response) solution installed, configured, and managed on all workstations, servers, and laptops
BCDR (Business Continuity and Disaster Recovery)	• BCDR takes backups a step further to ensure business continuity in the event of a disaster, hardware failure, ransomware, or data loss • Full image backups that can be restored to the cloud (or local appliance) in minutes ensures that a disaster or security breach does not lead to extended outages

	• Backups can be restored to dissimilar hardware in the event of hardware failure • Nightly automated restore verification ensures every backup can be successfully recovered • Ransomware detection will alert if a protected device has suspicious encrypted data • Freedom Defense Plan 1 includes BCDR on all servers with business-critical data
Microsoft 365 Enhancements	• Enhanced security licensing for each mailbox • Enhanced spam, phishing, and malware protection • Safe Links & Attachments throughout Microsoft 365 Email, SharePoint & Teams • Daily quarantine message digests upon request • Custom security and alerting configured to notify of unusual activity • Conditional access prohibiting access by region and user type • Backup of M365 accounts (1 year retention)
Advanced Network Monitoring	• Detailed network scanning, auditing, reporting, and alerting • Continuous network scanning to identify newly connected devices • Monitor uptime for all network devices • Remote power management and WOL
Advanced Network and Domain Reporting	• Deep network and resource scans • Review of Active Directory and network for security threats and changes • Internal and external vulnerability reports
Penetration Testing	• Also known as pen testing or ethical hacking, a penetration test will simulate a cyberattack to seek out exploitable vulnerabilities in your network • Through regular testing you can identify and resolve any discovered vulnerabilities • Freedom Defense Plan 1 includes a penetration test every 3 years
Documented Disaster Recovery and Incident Response Plan	• To protect your data, reputation, customer trust, and financial resources – you need thoughtful disaster recovery and incident response plans created in advance of an incident. Plans that have clear responsibilities that can be followed when needed. • American PCS will provide templates, research, and resources to create appropriate plans
Firewall Hardening	• Firewalls are the front line of defense from an outside attack. They need to be properly configured and maintained • Regularly scheduled policy reviews • Implementation of advanced security options and custom settings for your environment
Prerequisites	• Approved Next Generation Firewall with active warranty and subscription for advanced security features at all supported locations • All workstations and servers on currently supported operating systems • MFA enabled for all e-mail accounts • MFA enabled for all VPN users • If any prerequisites are not met, a quote will be provided to remedy prior to onboarding

Freedom Defense Plan 2

SERVICES	GENERAL DESCRIPTION
Overview	• **Freedom Defense Plan 2 includes everything in Plan 1 plus the additional items listed below**. • Freedom Defense provides a powerful and robust security solution. In addition to the technical features listed below, it includes American PCS labor to restore computer systems to an operational state after a security breach or ransomware attack. • Freedom Defense Plan 2 includes up to 75 hours labor per incident with no more than 100 hours in any one month
Defense in depth / MDR	• Every solution has weaknesses or blind spots. Even the best EDR is not perfect. A robust security plan requires defense in depth and many overlapping solutions. • MDR (Managed Detection and Response) goes beyond malware protection and looks for legitimate tools or resources being used for nefarious things. It looks for footholds used to gain access later as well as other suspicious activity.
Threat Hunting	• A team of security experts will be reviewing logs and alerts 24/7 to provide rapid response to resolve security issues as quickly as possible.
Annual Penetration Testing	• At this level penetration testing is increased to annually
BCDR (Business Continuity and Disaster Recovery)	• Freedom Defense Plan 2 includes BCDR on one workstation from each department in addition to the servers

Freedom Defense Plan 3

SERVICES	GENERAL DESCRIPTION
Overview	• **Freedom Defense Plan 3 includes everything in Plan 1 and 2 plus the additional items listed below** • Freedom Defense provides a powerful and robust security solution. In addition to the technical features listed below, it includes American PCS labor to restore

	computer systems to an operational state after a security breach or ransomware attack. • Freedom Defense Plan 3 includes up to 120 hours labor per incident with no more than 150 hours in any one month
Zero Trust / Whitelisting	• Zero Trust application whitelisting for endpoints blocks any application that is not explicitly permitted while monitoring and controlling how applications interact with each other. • 24-hour operations center continuously monitors for application and operating system updates to automatically adjust the whitelists when needed. • Sets boundaries around applications to prevent them from interacting with other applications, accessing network resources, registry keys, and files.

Freedom Defense Plan 4

SERVICES	GENERAL DESCRIPTION
Overview	• **Freedom Defense Plan 4 includes everything in Plan 1, 2, and 3 plus the additional items listed below** • Freedom Defense provides a powerful and robust security solution. In addition to the technical features listed below, it includes American PCS labor to restore computer systems to an operational state after a security breach or ransomware attack. • Freedom Defense Plan 4 includes up to 150 hours labor per incident with no more than 180 hours in any one month
Zero Trust / Whitelisting	• Expanded Zero Trust approach trusts zero people, devices, networks, or applications unless they have been preapproved or whitelisted. • The most secure environments are those that restrict access to only the people, devices, networks, and applications that have been explicitly approved
Complete BCDR	• Every server and workstation is covered by a full image backup for rapid restore in the event of ransomware or other data loss

Additional Add-on Products and Services

The following products and services may be provided in addition to, or in lieu of, the Freedom Services and Freedom Defense packages listed above. Please note: Depending on the Freedom Defense Plan you select, one or more of these “add-on” services may already be included your service plan.

BCDR (Business Continuity and Disaster Recovery)

- BCDR takes backups a step further to ensure business continuity in the event of a disaster, hardware failure, ransomware, or data loss
- Full image backups that can be restored to the cloud (or local appliance) in minutes ensures that a disaster or security breach does not lead to extended outages
- Backups can be restored to dissimilar hardware in the event of hardware failure
- Nightly automated restore verification ensures every backup can be successfully recovered
- Ransomware detection will alert if a protected device has suspicious encrypted data
- For more details, see the description of these services in the Freedom Services table, above.

Penetration Testing

- Also known as pen testing or ethical hacking, a penetration test will simulate a cyberattack to seek out exploitable vulnerabilities in your network
- Through regular testing you can identify and resolve any discovered vulnerabilities

Hardware as a Service (HaaS)

HaaS Equipment We will provide you with the HaaS Equipment described in the Quote or, if no hardware is expressly designated as HaaS Equipment in the Quote, then a complete list of HaaS Equipment will be provided to you under separate cover.

Deployment. We will deploy the HAAS Equipment within the timeframe stated in the Quote, provided that you promptly provide all information that we reasonably request from you to complete deployment. This deployment guaranty does not apply to any software, other managed services, or hardware devices other than the HAAS Equipment. If you wish to delay the deployment of the HaaS Equipment, then you may do so provided that you give us written notice of your election to delay no later than five (5) days following the date you sign the Quote. Deployment shall not extend beyond two (2) months following the date on which you sign the Quote. You will be charged at the rate of fifty percent (50%) of the monthly recurring fees for the HaaS-related services during the period of delay. Following deployment, we will charge you the full monthly recurring fee (plus other usage fees as applicable) for the full term indicated in the Quote.

Equipment Hardware Repair or Replacement. American PCS will repair or replace HAAS Equipment by the end of the business day following the business day on which the applicable problem is identified by, or reported to, American PCS and has been determined by American PCS to be incapable of being remediated remotely.

This warranty does not include the time required to rebuild your system, such as the time required to configure a replacement device, rebuild a RAID array, reload the operating system, reload and configure applications, and/or restore from backup (if necessary).

If American PCS fails to meet the warranties in this section and the failure materially and adversely affects your hosted environment ("Hosted System"), you are entitled to a credit in the amount of 5% of the monthly fee per hour of downtime (after the initial one (1) hour allocated to problem identification), up

to 100% of your monthly fee for the affected HaaS Equipment. In no event shall a credit exceed 100% of the applicable month's monthly fee for the affected equipment. The foregoing shall not apply where the service level failure was due to a failure, error, or omission from a third party service provider, third party service, or force majeure event.

Periodic Replacement of HaaS Equipment. From time to time and in our discretion, we may decide to swap out older HaaS Equipment for updated or newer equipment. (Generally, equipment that is five years old or older may be appropriate for replacement). If we elect to swap out HaaS Equipment due to normal, periodic replacement, then we will notify you of the situation and arrange a mutually convenient time for such activity.

Return of HaaS Equipment. 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 HaaS Equipment. Doing so 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. Within ten (10) days after the termination of HaaS-related Services, Client will provide American PCS access to the premises at which the HaaS Equipment is located so that all such equipment may be retrieved and removed by us. If you fail to provide us with timely access to the HaaS Equipment 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.

Covered Equipment / Hardware / Software

Freedom Services will be applied to the equipment listed in the Quote ("Covered Hardware").

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."

.

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 business locations; home networks, mobile networks, and other locations that are not primarily used for Client's business purposes are out-of-scope. Additional fees may apply for onsite visits: 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 American PCS' 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 thirty (30) days nor more than ninety (90) days before the end of the then-current Service Term.

Per Seat Licensing: **Regardless of the reason for the termination of the Services, you will be required to pay for all per seat licenses (such as, if applicable, Microsoft NCE licenses) that we acquire on your behalf. Please see "Per Seat License 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.
- Server file systems and email systems (if applicable) must be protected by licensed and up-to-date virus protection software.
- The Environment must have a currently licensed and approved backup solution that can be monitored.
- Business grade networking equipment that has monitoring and remote access capabilities
- Business grade workstations from major manufacturers such as Dell or HPE.
- All wireless data traffic in the environment must be securely encrypted.
- All servers must be connected to working and networked UPS devices.
- Data recovery assumes data integrity of the backups or the data stored on the backup devices. We do not guarantee the integrity of the backups or the data stored on the backup devices. Server restoration will be to the point of the last successful backup.
- 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
What Is Not Included

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 American PCS. Without limiting the foregoing, the following services are expressly excluded, and if required to be performed, must be agreed upon by American PCS in writing:

"Project / Integration Work" Defined as any service designated to add or increase functionality or capacity; in other words, any work that is not designed to support existing systems or persons. Projects are outside the scope of this agreement and as such will be quoted and invoiced separately. Project / Integration Work will be identified to The Client as such before any work is performed.

"Line of Business Applications" Defined as applications such as custom accounting packages, CRM software, ERP software, etc. that are not specifically mentioned herein fall outside the normal purview of this Agreement. Reasonable attempts will be made to correct connectivity issues to such applications; however problems specific to the application configuration or network problems caused by the applications are excluded.

"Hardware Replacement Cost" Defined as the cost associated with hardware replacement falls outside this agreement. Hardware replacement can take the form of warranty, extended warranty, manufacturer's support contract, on-site spares, or purchases as needed. Hardware replacement options will be discussed as part of the Audit deliverables to be sure an appropriate hardware strategy exists for all critical equipment.

Other Exclusions:

- Customization of third-party applications, or programming of any kind.
- Support for operating systems or applications no longer supported by the manufacturer.
- Data/voice wiring or cabling services of any kind.
- 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 American PCS in our discretion after consulting with the Client. All remediation services will initially be attempted remotely; American PCS will provide onsite service only if remote remediation is ineffective and, under all circumstances, only if covered under the Service plan selected by Client.

Trouble	Priority	Response Time	Resolution Time	Escalation Threshold
Critical Emergency (Service not available all users and functions unavailable).	1	Within 1 business hour	ASAP –Best Effort	2 hours
Urgent (Large number of users or business critical functions affected)	2	3 business hours	ASAP –Best Effort	8 hours
High (Limited degradation of service, limited number of users or functions affected, business process can continue).	3	Within 5 business hours	ASAP –Best Effort	24 hours
Normal (Small service degradation, business process can continue, one user affected).	4	Within 12 business hours	ASAP –Best Effort	48 hours
Low Priority (Maintenance needed, no noticeable degradation to any users).	5	Next Available	Not Applicable	Not Applicable

* All time frames are calculated as of the time that American PCS is notified of the applicable issue / problem by Client through American PCS' designated e-mail, 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.

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 / devices accessing the managed environment changes, then you agree that the fees will be automatically and immediately modified to accommodate those changes. We reserve the right to modify and/or adjust your invoices to reflect changes to the managed environment and/or the number of authorized users accessing the managed environment (retroactively if necessary), and you agree to pay such additional amounts to accommodate the changes.

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 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, 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.

Payment. You may pay your invoices by check and/or by ACH, as described below.

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. These functionalities are guided by Client-designated policies, which may be modified by Client as necessary or desired from time to time. Initially, the policies will be set to a baseline standard as determined by American PCS; however, Client is advised to establish and/or modify the policies that correspond to Client's specific monitoring and notification needs.

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.

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 American PCS 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 American PCS 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. American PCS 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 American PCS 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 American PCS 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. American PCS cannot and does not warrant that data corruption or loss will be avoided, and Client agrees that American PCS 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 American PCS 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, American PCS 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. American PCS is not a warranty service or repair center. American PCS 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 American PCS will be held harmless, and (ii) American PCS 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.

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 American PCS' opinion and knowledge of the relevant facts and circumstances. By rendering advice, or by suggesting a particular service or solution, American PCS 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. American PCS 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 American PCS 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 American PCS-hosted or American PCS-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 American PCS 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. American PCS 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 American PCS immediately to request the login information be reset or unauthorized access otherwise be prevented. American PCS 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.