Services Guide

This Services Guide contains provisions that define, clarify, and govern the services described in the Order that has been provided to you

This Services Guide is our "owner's manual" that generally describes all managed services provided or facilitated by Provider; however, only those Services specifically described in the Order will be facilitated and/or provided to you.

Activities or items that are not specifically described in the Order will be out of scope and will not be included unless otherwise agreed to by us in writing.

Initial Audit / Diagnostic Services

If an Initial Audit / Diagnostic Services is listed in the Order, then we will audit your managed information technology environment (the "Environment") to determine the readiness for, and compatibility with, ongoing managed services. Our auditing services may be comprised some or all of the following:

- Audit to determine general Environment readiness and functional capability
- Review of hardware and software configurations
- Review of current vendor service/warranty agreements for Environment hardware and software
- Basic security vulnerability check
- Basic backup and file recovery solution audit
- Speed test and ISP audit
- Print output audit
- Office telephone vendor service audit
- Asset inventory
- Email and website hosting audit
- IT support process audit

If deficiencies are discovered during the auditing process (such as outdated equipment or unlicensed software), we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of the Services and provide you with options to correct the deficiencies. Please note, unless otherwise expressly agreed by us in writing, auditing 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 auditing process. Issues that are discovered in the Environment after the auditing process is completed may be addressed in one or more subsequent quotes.

Onboarding Services

If onboarding services are listed in the Order, then one or more of the following services may be provided to you.

- Uninstall any monitoring tools or other software installed by previous IT service providers.
- Compile a full inventory of all protected servers, workstations, and laptops.
- Uninstall any previous endpoint protection and install our managed security solutions (as indicated in the Order).
- 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.
- Review firewall configuration and other network infrastructure devices.
- Review the status of battery backup protection on all mission-critical devices.
- Stabilize the network and ensure that all devices can securely access the file server.
- Review and document current server configuration and status.
- Determine existing business continuity strategy and status; prepare backup file recovery and incident response option 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.

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 Order, 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 Services

Ongoing/recurring services are services that are provided to you or facilitated for you on an ongoing basis and, unless otherwise indicated in an Order, 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.

Managed Services

SERVICES	GENERAL DESCRIPTION
Backup and File Recovery	Implementation and facilitation of a top-tier backup and file recovery solution from our designed Third-Party Provider. Features include: • 24/7 monitoring of backup system, including offsite backup, offsite replication, and an onsite backup appliance ("Backup Appliance") • Troubleshooting and remediation of failed backup disks • Preventive maintenance and management of imaging software • Firmware and software updates of backup appliance • Problem analysis by the network operations team • Monitoring of backup successes and failures • Daily recovery verification Backup Data Security: All backed up data is encrypted in transit and at rest in 256-bit AES encryption. All facilities housing backed up data implement physical security controls and logs, including security cameras, and have multiple internet connections with failover capabilities. Backup Retention: Backed up data will be retained on a one (1) year rolling basis. Backup Alerts: Managed servers will be configured to inform of any backup failures. Recovery of Data: If you need to recover any of your backed up data, then the following procedures will apply: • Service Hours: Backed up data can be requested during our normal business hours, which are currently 7:30 AM to 4:30 Pacific Time, excluding Professional IT-observed holidays. • Request Method. Requests to restore backed up data should be made through one of the following methods: ○ Email: help@proitzone.com ○ Telephone: 805-489-2131 • Restoration Time: We will endeavor to restore backed up data as quickly as possible following our receipt of a request to do so; however, in all cases data restoration services are subject to (i) technician availability and (ii) confirmation that the restoration point(s) is/are available to receive the backed up data.
Backup Monitoring	Implementation and facilitation of a top-tier backup monitoring solution from our designed Third-Party Provider. Features include: • Monitors backup status for certain backup applications then-installed in the managed environment,

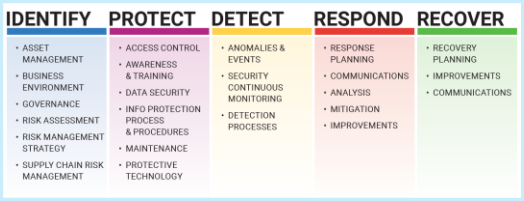
	such as successful completion of backup, failure errors, and destination free space restrictions/limitations. • Helps ensure adequate access to Client's data in the event of loss of data or disruption of certain existing backup applications. • **Note: Backup monitoring is limited to monitoring activities only and is not a backup and file recovery solution.**
Compliance as a Service (CaaS)	We will facilitate a top-tier third-party solution to help meet your compliance needs. The solution will offer the following features: • Audits. Annual audits of your company will identify administrative, technical, and physical gaps in compliance with regulatory standards. • Remediation Plan: A relevant and enforceable remediation plan so you're ready in the event of a breach or ransomware attack. • Policies, procedures, and employee training: The risk of compliance violations will be lowered by having documented and well-developed policies, procedures, and training to meet regulatory HIPAA and PCI standards requirements, with annual (and ongoing) learn-from-experience training tailored for your company's team. • Documentation: A comprehensive toolkit devoted to clearly showing the compliance regulators you are making a concerted effort to improve your network security. • Incident management: Implementation of a system and toolbox for your team to be prepared in the event of a data breach, so you can document the breach and notify those who need to know. • Health and Finance: Compliance training will cover all current HIPAA and PCI standards.
Dark Web Monitoring	Implementation and facilitation of a top-tier Dark Web Monitoring solution from our designed Third-Party Provider. Credentials supplied by Client will be added to a system that continuously uses human and machine-powered monitoring to determine if the supplied credentials are located on the dark web. If compromised credentials are found, they are reported to Help Desk Services staff, who will review the incident and notify affected end-users. 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.
Email Threat Protection	Implementation and facilitation of a trusted email threat protection solution from our designed Third-Party Provider. Features include: • Managed email protection from phishing, business email compromise (BEC), SPAM, and email-based malware. • Friendly Name filters to protect against social engineering impersonation attacks on managed devices. • Protection against social engineering attacks like whaling, CEO fraud, business email compromise, or W-2 fraud. • Protects against newly registered and newly observed domains to catch the first email from a newly registered domain. • Protects against display name spoofing. • Protects against "looks like" and "sounds like" versions of domain names. **Please see Anti-Virus; Anti-Malware, and Breach / Cyber Security Incident Recovery sections below for important details.** **All hosted email is subject to the terms of our Hosted Email Policy and our Acceptable Use Policy.**

Endpoint Antivirus & Malware Protection	Implementation and facilitation of a top-tier endpoint malware protection solution from our designed Third-Party Provider. Features include: • Utilizes artificial intelligence and machine learning to provide a comprehensive and adaptive protection paradigm to managed endpoints. • Detects unauthorized behaviors of users, applications, or network servers. • Blocks suspicious actions before execution. • Analyzes suspicious app activity in isolated sandboxes. • Antivirus and malware protection for managed devices such as laptops, desktops, and servers. • Protects against file-based and fileless scripts, as well as malicious JavaScript, VBScript, PowerShell, macros, and more. • Allows whitelisting for legitimate scripts. • Allows for blocking of unwanted web content. • Detects advanced phishing attacks. • Detects / prevents content from IP addresses with low reputation. *** Please see Anti-Virus; Anti-Malware, and Breach / Cyber Security Incident Recovery sections below for important details.**
Extended Detection & Response (XDR)	Implementation and facilitation of a top-tier endpoint malware protection solution with extended functionalities from our designed Third-Party Provider. Features include: • Automated correlation of data across multiple security layers*—email, endpoint, server, cloud workload, and the managed network, enabling faster threat detection. • Provides extended malware sweeping, hunting, and investigation. • Allows whitelisting for legitimate scripts. • Next-generation deep learning malware detection, file scanning, and live protection for the workstation operating system. • Web access security and control, application security and control, intrusion prevention system. • Data loss prevention, exploit prevention, malicious traffic detection, disk and boot record protection. • Managed detection, root cause analysis, deep learning malware analysis, and live response. • On-demand endpoint isolation, advanced threat intelligence, and forensic data export. * Requires at least two layers (*e.g.*, endpoint, email, network, servers, and/or cloud workload.) **Please see Anti-Virus; Anti-Malware, and Breach / Cyber Security Incident Recovery sections below for important details.**
End User Security Awareness Training	Implementation and facilitation of a security awareness training solution from an industry-leading third-party solution provider. Features include: • 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. **Please see Anti-Virus; Anti-Malware, and Breach / Cyber Security Incident Recovery sections below for important details.**

Firewall as a Service **(firewall appliance provided by Professional IT)**	• Provide a FIPS 140-2 compliant firewall configured for your organization's specific bandwidth, remote access, and user needs. • Helps to prevent hackers from accessing internal network(s) from outside the network(s), while providing secure and encrypted remote network access; provides antivirus scanning for all traffic entering and leaving the managed network; provides website content filtering functionality. • Firewall appliance is subject to "Hardware as a Service" terms and conditions located in this Guide. • Firewall appliance must be returned to Professional IT upon the termination of service. Client will be responsible for missing or damaged (normal wear and tear excepted) appliance.
Firewall Solution **(firewall appliance provided / purchased by Client)**	• Monitors, updates (software/firmware), and supports Client-supplied firewall appliance. • Helps to prevent hackers from accessing internal network(s) from outside the network(s), while providing secure and encrypted remote network access; provides antivirus scanning for all traffic entering and leaving the managed network; provides website content filtering functionality.
Hardware as a Service (HaaS)	The provisions and descriptions below apply to all hardware, devices, and accessories that are provided to you on a "hardware as a service" basis. • Scope. Provision and deployment of hardware and devices listed in the Order or other applicable schedule ("HaaS Equipment"). • Deployment. We will deploy the HaaS Equipment within the timeframe stated in the Order, provided that you promptly provide all information that we reasonably request from you to complete deployment. This deployment guarantee 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 if you give us written notice of your election to delay no later than five (5) days following the date you sign the Order. Deployment shall not extend beyond two (2) months following the date on which you sign the Order. 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 Order. • Repair/replacement of HaaS Equipment. Professional IT 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, Professional IT and has been determined by Professional IT 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). • Technical Support for HaaS Equipment. We will provide technical support for HaaS Equipment in accordance with the Service Levels listed in this Services Guide. • In-Warranty Repair. Professional IT 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,

	Professional IT and has been determined by Professional IT to be incapable of being remediated remotely. • Periodic Replacement of HaaS Equipment. From time to time and in our discretion (at no additional charge), 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. • Usage. You will use all HaaS Equipment for your internal business purposes only. You shall not sublease, sublicense, rent, or otherwise make the HaaS Equipment available to any third party without our prior written consent. You agree to refrain from using the HaaS Equipment 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 HaaS Equipment if we believe, in our sole but reasonable judgment, that your use of the HaaS Equipment violates the terms of the Order, this Services Guide, or the Agreement. • Credits/Remedies. If Professional IT fails to meet the warranties in this section and the failure materially and adversely affects your hosted environment, 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. • Return of HaaS Equipment. Unless we expressly direct you to do so, you shall 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 Professional IT 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.

Labor for New / Replacement Workstations	Includes all labor charges for the setup of new workstations or the replacement of existing workstations.
	
	• Labor covers:
	  ○ New computers / additional computers added during the term of the Order;
	  ○ Replacement of existing computers that are four (4) or more years old (as determined by the manufacturer's serial number records);
	  ○ Replacement of existing computers that have been lost/stolen, or irreparably damaged and/or out of warranty but not yet four years old;
	  ○ Operating systems upgrades – subject to hardware compatibility.
	
	The following restrictions apply:
	
	• Upgrades or installs of new or replacement computers are limited to four (4) devices per month unless otherwise approved in advance by Professional IT;
	• This service is not available for used or remanufactured computers; and,
	• New/replacement computers must be business-grade machines (not home) from a major

	manufacturer like HPE, or Lenovo.
Managed Detection & Response (MDR)	Implementation and facilitation of a top-tier MDR solution from our designed Third-Party Provider. Features include: • 24x7 Managed network detection and response. • Real time and continuous (24x7) monitoring and threat hunting. • Real-time threat response. • Alerts are handled in accordance with our Alert Notification table, below. • Security reports, such as privileged activities, security events, and network reports, are available upon request. • 24x7x365 access to a security team for incident response* * **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware, and Breach / Cyber Security Incident Recovery sections below for important details.**
NIST Risk Assessment	• Perform a cybersecurity assessment under NIST CSF using the NIST Risk Management Framework & NIST 800-53. • Identifies how Client currently assesses, mitigates, and tracks its cybersecurity requirements. • Identifies authorized and unauthorized devices in the managed network. • Identifies gaps or deficiencies in the Client's operations that would prevent compliance under NIST CSF. The assessment will cover the following five core areas of the NIST framework:  The results of the assessment will be provided in a report that will identify detected risks and your organization's current maturity levels (*i.e.*, indicators that represent the level of capabilities within your organization's security program) and will propose actionable activities to help increase relevant maturity levels and augment your organization's security posture.

	Please Note: This service is limited to an assessment/audit only. Remediation of issues discovered during the assessment, as well as additional solutions required to bring your managed environment into compliance, are not part of this service. After the audit is complete, we will discuss the results with you to determine what steps, if any, are needed to bring your organization into full compliance.
Password Manager	Implementation and facilitation of an industry-leading password management protection solution from our designed Third-Party Provider. Features include: • Password Vault: Securely store and organize passwords in a secure digital location accessed through your browser or an app. • Password Generation: Generate secure passwords with editable options to meet specific criteria. • Financial Information Vault: Securely store and organize financial information such as bank accounts and credit card information in a secure digital location accessed through your browser or an app. • Contact Information Vault: Store private addresses and personal contact information within your vault, accessed through your browser or an app. • Browser App: Browser extension permits easy access to all of your information, including the vaults, financial information, contact information, and single sign-on through the app. • Smart-Phone App: Mobile phone app enables access to your vault and stored information on your mobile device.
Penetration (Pen) Testing	**External Pen Testing:** exposes vulnerabilities in your internet-facing systems, networks, firewalls, devices, and/or web applications that could lead to unauthorized access. **Internal Pen Testing:** Validates the effort required for an attacker to overcome and exploit your internal security infrastructure after access is gained. **PCI Pen Testing:** Using the goals set by the PCI Security Standards Council, this test involves both external and internal pen testing methodologies. **Web App Pen Testing:** Application security testing using attempted infiltration through a website or web application utilizing PTES and the OWASP standard testing checklist. Please see additional terms for Penetration Testing below.

Commented [A1]: At what frequency is this happening?

Remote Helpdesk

- 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.

Remote Infrastructure Maintenance & Support

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

Remote Monitoring and Management

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

- Includes capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD and SSD partitions, not external devices such as USB or mapped drives)
- Includes routine operating system inspection and cleansing to help ensure that disk space is increased before space-related issues occur.
- Review and installation of updates and patches for supported software.

In addition to the above, our remote monitoring and management service will be provided as follows:

Event	Server	Workstation
Hardware Failures	Yes	No
Device Offline	Yes	No
Failed/Missing Backup	Yes	Yes
Failed/Missing Updates	Yes	Yes
Low Disk Space	Yes	Yes
Agent missing/misconfigured	Yes	Yes
Excessive Uptime	Yes	No

Security Incident & Event Monitoring (SIEM)

Implementation and facilitation of an industry leading SIEM from our designed Third-Party Provider.

The SIEM service utilizes threat intelligence to detect threats that can exploit potential vulnerabilities against your managed network.

- Initial Assessment. Prior to implementing the SIEM service, we will perform an initial assessment of the managed network at your premises to define the scope of the devices/network to be monitored (the "Initial Assessment").
- Monitoring. The SIEM service detects threats from external facing attacks as well as potential insider

	threats and attacks occurring inside the monitored network. Threats are correlated against known baselines to determine the severity of the attack. • Alerts & Analysis. Threats are reviewed and analyzed by third-party human analysts to determine true/false positive dispositions and actionability. If it is determined that the threat was generated from an actual security-related or operationally deviating event (an "Event"), then you will be notified of that Event. Events are triggered when conditions on the monitored system meet or exceed predefined criteria (the "Criteria"). Since the Criteria are established and optimized over time, the first thirty (30) days after deployment of the SIEM services will be used to identify a baseline of the Client's environment and user behavior. During this initial thirty (30) day period, Client may experience some "false positives" or, alternatively, during this period not all anomalous activities may be detected. Note: The SIEM service is a monitoring and alert-based system only; remediation of detected or actual threats are not within the scope of this service and may require Client to retain Professional IT's services on a time and materials basis.
Server Monitoring & Maintenance	As part of our RMM service, we will monitor and maintain managed servers as follows: • Software agents installed in covered servers report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below. • Online status monitoring, alerting us to potential failures or outages • Capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD and SSD partitions, not external devices such as USB or mapped network drives) • Performance monitoring, alerting us to unusual processor or memory usage • Server essential service monitoring, alerting us to server role-based service failures • Endpoint protection agent monitoring, alerting us to potential security vulnerabilities • Routine operating system inspection and cleansing • Secure remote connectivity to the server and collaborative screen sharing • Review and installation of updates and patches for Windows and supported software • Asset inventory and server information collection
Two Factor Authentication	Implementation and facilitation of a two-factor authentication solution from our designed Third-Party Provider. Features include: • Advanced two-factor authentication with advanced admin features. • Secures on-premises and cloud-based applications. • Permits custom access policies based on role, device, and location. • Identifies and verifies device health to detect "risky" devices
Server Next-	Implementation and facilitation of a top-tier, next-generation antivirus protection solution from our

Generation Antivirus	designed Third-Party Provider. Software agents installed in covered server devices protect against malware and prevents intruder access. Used in coordination with other endpoint security layers and security solutions to form a comprehensive defense strategy. • Next-generation deep learning malware detection, file scanning, and live protection for Server OS • Web access security and control, application security and control, intrusion prevention system • Data loss prevention, exploit prevention, malicious traffic detection, disk and boot record protection
Software Licensing (applies to all software licensed by or through Professional IT)	All software provided to you by or through Professional IT is licensed, not sold, to you ("Software"). In addition to any Software-related requirements described in Professional IT'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.
Updates & Patching	• Remotely deploy updates (e.g., x.1 to x.2), as well as bug fixes, minor enhancements, and security updates as deemed necessary on all managed hardware. • Perform minor 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.
Technology Strategy	Act as the main point of contact for certain business-related IT issues and concerns. • Assist in the creation of information/data-related plans and budgets. • Provide strategic guidance and consultation across different technologies. • Create company-specific best standards and practices. • Provide education and recommendations for business technologies. • Participate in scheduled meetings to maintain goals. • Maintain technology documentation. • Assess and make recommendations for improving technology usage and services.
Security Optimization	Act as the main point of contact for certain business-related IT security and risk mitigation issues and concerns.

	• Provides leadership on risk, governance, incident response, disaster recovery and business continuity processes and procedures. • Assesses operational and strategic procedures to mitigate security risks • Provides consultation to build effective cybersecurity & resiliency programs • Facilitates the integration of security into Client's overall business strategies, processes, and culture • Assist with integration and interpretation of information security program controls.
Voice Over IP (VoIP) Services	Implementation and facilitation of an industry-recognized VoIP solution from our designed Third-Party Provider. Features include: • Scalable VoIP-based telephone service with call transferring, voicemail, caller ID, call hold, conference calling, and call waiting functionalities. • Central control panel provides access to VoIP-related configurations, including physical address registration, call routing, updating greetings, and ability to turn on/off service features. • Ability to use mobile app dialing **Important**: There are additional terms related to the VoIP service, including your use of E911 features, toward the end of this Services Guide. Please read them carefully. You may be required to sign an additional consent form indicating your understanding and acceptance of the limitations of 911 dialing using the VoIP services.
Vulnerability Scanning	Implementation and facilitation of an industry-recognized vulnerability scanning solution from our designed Third-Party Provider. Vulnerability scanning identifies holes in the managed network that could be exploited. Professional IT runs external vulnerability scans monthly and internal vulnerability scans annually. External scans pertain to the IP address assigned to each customer location through the Client's ISP. Internal scans look at all systems inside the managed network. Vulnerability results will be discussed during business review meetings with Client. Vulnerability reports will be made available on request. Please see additional terms for vulnerability scanning below.
Website Hosting	Our designated Third-Party Provider will provide sufficient space and bandwidth to host your designated website ("Website") which, except for scheduled downtime or force majeure events, will be available on a 24x7 basis. The Website will be hosted on a server that may be shared between many customers; however, the Website will be given a unique address (Professional IT). • Migration of Servers. As a normal course of business, we or our Third-Party Provider, as applicable, may migrate the servers on which the Website is hosted. This process will not interfere with the Hosting Services, however, due to the potential for migration, you are not

	guaranteed a permanent or dedicated IP address. • Administration. You will be provided with access to a dashboard through which you may make configuration adjustments to the hosted environment; however, we strongly advise you to refrain from making changes to the hosted environment without our guidance or direction. We will not be responsible for remediating issues caused by your adjustments to the hosted environment unless those adjustments were made pursuant to our written directions or under our supervision. • Resource/Load Balancing. The bandwidth made available to your website is shared and allocated among all of our customers. You must comply with all bandwidth and Professional IT-imposed limitations on the hosting services as established by Professional IT from time to time. We reserve the right to load-balance applicable bandwidth to ensure that your activity will not restrict, inhibit, or diminish any other user's use of the bandwidth or create an unusually large burden on the bandwidth. We reserve the right to restrict your access to your hosted website in the event that your activities create a disproportionate burden on our network or our Third-Party Providers' networks (if applicable), or any other crucial resources reasonably needed to ensure the functionality, integrity, and/or security of the hosting services. • Backup. Data in the hosted environment will be backed up daily ("Standard Backup Service"); however, the Standard Backup Service is not, and should not be regarded as, a backup and disaster recovery solution. Although the Standard Backup Service is a part of the hosting services, it is only a basic backup service, and it does not provide data integrity verification services or other advanced backup or recovery options. We strongly recommend that you implement a separate backup and disaster recovery solution to protect the security and integrity of, and accessibility to, the data in the hosted environment. • Storage and Security. We and/or our Third-Party Providers will take reasonable steps to prevent unauthorized access to the Website and the hosted environment; however, you understand and agree that no security solution is 100% effective, and we do not warrant or guarantee that the hosted environment will be free from unauthorized access or malware at all times. **Client, as well as any visitors to the Website, must comply with our Acceptable Use Policy which is located at the end of this Services Guide.**
Wi-Fi Services	• Professional IT will install at the Client's premises Wireless Access Points) in all areas requiring wireless network coverage, as agreed upon by Professional IT and Client. • Professional IT will maintain, supervise, and manage the wireless system at no additional cost. • Installed equipment, if provided by Professional IT, will be compatible with the then-current industry standards. • Professional IT 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). Please note: Any Wi-Fi devices, such as access points or routers, that are supplied by Client cannot be older than five (5) years from the applicable device's original date of manufacture, and in all cases must be supported by the manufacturer of the device(s).
Workstation Next-	Implementation and facilitation of an industry-recognized, next generation workstation malware

Generation Malware Solution	protection solution from our designed Third-Party Provider. Software agents installed in covered devices protect against malware and prevent intruder access. Used in coordination with other endpoint security layers and security solutions to create a comprehensive defensive strategy. • Next-generation deep learning malware detection, file scanning, and live protection for Workstation OS. • Web access security and control, application security and control, intrusion prevention system. • Data loss prevention, exploit prevention, malicious traffic detection, disk, and boot record protection.
Workstation Monitoring & Maintenance	Software agents installed in covered workstations report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below. • Online status monitoring, alerting us to potential failures or outages. • Capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD and SSD partitions, not external devices such as USB or mapped network drives). • Performance monitoring, alerting us to unusual processor or memory usage. • Endpoint protection agent monitoring, alerting us to potential security vulnerabilities. • Routine operating system inspection and cleansing. • Secure remote connectivity to the workstation and collaborative screen sharing. • Review and installation of updates and patches for Windows and supported software. • Asset inventory and workstation information collection.

Covered Environment

Managed Services will be applied to the number of devices indicated in the Order ("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.

If the Order indicates that the Services are billed on a "per user" basis, then the Services will be provided for up to two (2) Business Devices used by the number of users indicated in the Order. A "Business Device" is a device that (i) is owned or leased by Client and used primarily for business, (ii) is regularly connected to Client's managed network, and (iii) 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 Order 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 an 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, then 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 on-site visit is required. Professional IT 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 the Client's primary business location. Additional fees may apply for onsite visits: Please review the Service Level section below for more details.

Minimum Requirements / Exclusions

In addition to the Minimum Standards identified in the Service Attachment for Managed Services, the scheduling, fees, and provision of the Services are based upon the following assumptions and minimum requirements, all of which must be provided/maintained by Client at all times:

- Server file systems and email systems (if applicable) must be protected by licensed and up-to-date virus protection software.
- The managed environment must have a currently licensed, vendor-supported server-based backup solution that can be monitored.
- All servers must be connected to working UPS devices.
- Recovery coverage 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 Services Guide.
- 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.

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, 7:30 AM – 4:30 PM Pacific Time, excluding legal holidays and Professional IT-observed holidays as listed below), unless otherwise specifically stated in the Order or as otherwise described below.

We will strive to 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 Professional IT in our discretion after consulting with the Client. All remediation services will initially be attempted remotely; Professional IT will provide onsite service only if remote remediation is ineffective and, under all circumstances, only if covered under the Service plan selected by Client. **There is a one (1) hour minimum for all on-site support.**

Trouble / Severity	Response Time
Critical / Service Not Available (*e.g.,* all users and functions unavailable)	Response within two (2) business hours after notification.
Significant Degradation (*e.g.,* large number of users or business critical functions affected)	Response within four (4) business hours after notification.
Limited Degradation (*e.g.,* limited number of users or functions affected, business process can continue).	Response within eight (8) business hours after notification.
Small Service Degradation (e.g., business process can continue, one user affected).	Response within two (2) business days after notification.
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 Order. Notifications received in any manner other than described herein may result in a delay in the provision of remediation efforts.

Support During Off-Hours/Non-Business Hours: Technical support provided outside of our normal business hours is offered on a case-by-case basis and is subject to technician availability. If Professional IT agrees to provide off-hours/non-business hours support ("Non-Business Hour Support"), then that support will be provided on a time and materials basis (which is not covered under any Service plan), and will be billed to Client at the following increased hourly rates:

- After-Hours & Weekends: $300 Per Hour (1 Hour Minimum)

- Holidays (listed below): $400 Per Hour (1 Hour Minimum)

All hourly services are billed in 15-minute increments, and partial increments are rounded to the next highest increment. A one (1) hour minimum applies to all Non-Business Hour Support.

Professional IT-Observed Holidays: Professional IT observes the following holidays:

- New Year's Day
- Martin Luther King Jr. Day
- President's Day
- Cesar Chavez Day
- Good Friday – All Day
- Memorial Day
- Juneteenth
- Independence Day
- Labor Day
- Columbus Day
- Veterans Day
- Thanksgiving Eve – All Day
- Thanksgiving Day
- The day following Thanksgiving Day
- Christmas Eve
- Christmas Day
- New Year's Eve

Service Credits: Our service level target is 90% as measured over a calendar month ("Target Service Level"). If we fail to adhere to the Target Service Level and Client timely brings that failure to our attention in writing (as per the requirements of our Master Services Agreement), then Client will be entitled to receive a pro-rated service credit equal to 1/30 of that calendar month's recurring service fees (excluding hard costs, licenses, etc.) for each day on which the Target Service Level is missed. Under no circumstances shall credits exceed 30% of the total monthly recurring service fees under an applicable Order.

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.

Off Boarding

Subject to the requirements in the MSA, Professional IT will off-board Client from Professional IT's services by performing one or more of the following:

- Removal/disabling of monitoring agents in the Environment
- Removal/disabling of endpoint software from the Environment
- Removal/disabling of Microsoft 365 from the Environment (unless the licenses for Microsoft 365 are being transferred to your incoming provider; please speak to your technician for details.)
- Termination of SQL or Remote Desktop licenses provided by Professional IT
- Removal of credentials from the Environment
- Removal of backup software from the Environment

Additional Terms & Policies

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 an Order or this Services Guide ("Minimum Requirements") must be implemented and maintained as an ongoing requirement of our providing the Services to you.

Monitoring Services; Alert Services

Unless otherwise indicated in the Order, all monitoring and alert-type services are limited to detection and notification functionalities only. Monitoring levels will be set by Professional IT, 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.

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 Order. 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.

Anti-Virus; Anti-Malware

Our anti-virus / anti-malware solution will generally protect the Environment from becoming infected with new viruses and malware ("Malware"); however, Malware that exists 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 Malware will be detected, avoided, or removed, or that any data erased, corrupted, or encrypted by Malware will be recoverable. To improve security awareness, you agree that Professional IT 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 Order, 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.

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 Order, 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.

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 Professional IT 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. Professional IT 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 Professional IT 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 Professional IT 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. Professional IT cannot and does not warrant that data corruption or loss will be avoided, and Client agrees that Professional IT 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 Professional IT on the Client's behalf ("Procured Equipment") may be covered by one or more manufacturer warranties, which will be passed through to the Client to the greatest extent possible. By procuring equipment or software for Client, Professional IT 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. Professional IT is not a warranty service or repair center. Professional IT 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 Professional IT will be held harmless, and (ii) Professional IT 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 Meetings

We strongly suggest that you participate in business review/strategic planning meetings as may be requested by us from time to time. These meetings are intended to educate you about recommended (and potentially crucial) modifications to your IT environment, as well as to discuss your company's present and future IT-related needs. These reviews can provide you with important insights and strategies to make your managed IT environment more efficient and secure. You understand that by suggesting a particular service or solution, we are not endorsing any specific manufacturer or service provider.

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 Scanning

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 and/or vulnerability scanning processes, 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 or vulnerability scanning 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 or vulnerability scanning 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 are not covered under the Order, 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 Order 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").

Professional IT 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**: Professional IT 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 Professional IT 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, Professional IT'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 performances 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, Professional IT 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.