Services Guide

NetIntegration LLC "Net-I" Services Guide

Updated 07-17-2024

https://www.net-i.com/net-i-service-guide/

SERVICES GUIDE

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

This Services Guide is our "owner's manual" that generally describes all services and products provided or facilitated by NetIntegration LLC ("Net-I," "we," "us," or "our"); 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 Services Guide contains important provisions pertaining to the auto-renewal of the Services in the Quote, as well as fee increases that may occur from time-to-time. Please read this Services Guide carefully and keep a copy for your records.

This Services Guide also discusses certain provisions of the Master Services Agreement (the "Master Services Agreement"), which governs our business relationship with you.

REQUESTS FOR SERVICE:

Requests for any type of service from Net-I should be initiated by using one of the following methods:

NET-I Agent (Preferred Method): Right Click on our NI icon on the taskbar of your computer and select Create Service Request. Filling out this form will give us a standard set of information and will lessen the need for us to ask follow-up question will improve our responsiveness to your request. You are also able to easily attach a screenshot of any errors you may be seeing on your display.

Please provide a Priority from the list below to help us process the request in a timely fashion. Follow up with a phone call for RED priority issues immediately and ORANGE priority issues as necessary.

Email: Help@net-i.com

Please provide the phone number you wish at which you wish to be reached and as detailed description of the problem as possible.

Please provide a Priority from the list below to help us process the request in the proper order.

Service Line phone: 901.309.4642

When initiating a phone call to us be prepared to provide the correct callback number at which yourself or the person needing assistance can be reached.

Please provide as much detail as possible regarding the issue.

Please provide a Priority from the list below to help us process the request in the proper order.

Other Information regarding service request initiation:

Business Critical Issues: Please open a request if possible and follow up with a phone call to our service line.

Priority: Please provide the priority of your request or incident you are requesting for which you are requesting service regardless of initiation method:

RED: Critical / Service Not Available (e.g., all users and functions unavailable)

ORANGE: Significant Degradation (e.g., large number of users or business critical functions affected, single user completely unable to access system)

YELLOW: Small Service Degradation (e.g., business process can continue, one user affected) Small Service Degradation (e.g., business process(es) can continue.

PREBOARDING SERVICES:

PREBOARDING SERVICES-INITIAL AUDIT / DIAGNOSTIC SERVICES

If an Initial Audit / Diagnostic Services are listed in the Quote, 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 are comprised of:

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:

ONBOARDING SERVICES FOR NEW CLIENT/SERVICE PLAN UPGRADE

If onboarding services are listed in the Quote, then one or more of the following services will 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 Quote).

Install remote support access agents (i.e., software agents) on each managed device to enable remote support.

Configure Windows® and application patch management agent(s) and check for missing security updates.

Uninstall unsafe applications or applications that are no longer necessary.

Optimize device performance including disk cleanup and endpoint protection scans.

Review firewall configuration and other network infrastructure devices.

Review status of battery backup protection on all mission critical devices.

Stabilize network and assure 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 Quote, onboarding-related services do not include the remediation of any issues, errors, or deficiencies ("Issues"), and we cannot guarantee that all Issues will be detected during the onboarding process.

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

ONGOING AND RECURRING SERVICES:

The following Service(s), if listed in the Quote, will be provided to you.

Ongoing and recurring services are services that are provided to you on an ongoing basis and, unless otherwise indicated in a Quote, are billed to you monthly. Some ongoing and 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.

Ongoing and recurring services do not include service fees for Professional Services associated with activities that are deemed a Project.

Unless otherwise provided in the Quote clients are considered "Time and Material" meaning all provided services and deliverables whether requested or not, are deemed billable at our current hourly billing rates. This includes communications with the client regarding any service requests, or resolving any backend issues that may arise from any third-party hardware or software.

PROFESSIONAL SERVICES / PROJECT MANAGEMENT SERVICES:

The following Service(s), if listed in the Quote, will be provided to you.

All requested services are billable and will be provided on a time and materials basis under our then-current hourly labor rates unless otherwise provided in the Quote.

If an estimated fee for Professional Services is provided in the Quote we will make our best effort to meet the fee as detailed by the Statement of Work in the Quote. We cannot guarantee the amount quoted will not be exceeded based on the actual times and rates of the work required to complete said Services.

Project Management Services are provided via the Quote task involves multiple stages and varied Net-I resources to complete.

A Project is defined as any task that requires five (5) hours or more hours to complete.

A Project is defined as "Out of Scope" for Clients with Ongoing and/or Recurring Service Agreement whether provided in the Quote or not.

Professional Services are billed at our current Rate Scheduled by technician skill level as detailed in the Quote.

PREPAID/FEE BASED ALLOCATED PROFESSIONAL SERVICES:

The following Service(s), if listed in the Quote, will be provided to you.

If you purchase one or more blocks of professional services or consulting hours from NetIntegration LLC, then we will provide our professional information technology professional services to you from time to time on an ongoing, "on demand" basis ("Services").

The specific scope, timing, term, and pricing of the Services (collectively, "Specifications") will be determined between you and us at the time that you request the Services from us.

You and we may finalize the Specifications (i) by exchanging emails confirming the relevant terms, or (ii) by you agreeing to an invoice, purchase order, or similar document we send to you that describes the Specifications (an "Invoice"), or in some cases, (iii) by us performing the Services or delivering the applicable deliverables in conformity with the Specifications.

If we provide you with an email or an Invoice that contains details or terms for the Services that are different than the terms of than the Quote, then the terms of the email or Invoice (as applicable) will control for those Services only.

A Service will be deemed completed upon our final delivery of the applicable portions of Specifications unless a different completion milestone is expressly agreed upon in the Specifications ("Service Completion"). (For example, sales of hardware will be deemed completed when the hardware is delivered to you; licensing will be completed when the licenses are provided to you, etc.) Any defects or deviations from the Specifications must be pointed out to us, in writing, within ten (10) days after the date of Service Completion. After that time, any issues or remedial activities related to the Services will be billed to you at our then-current hourly rates.

Unless we agree otherwise in writing, Services will be provided only during our normal business hours, which are currently 8-5 Central Time. Services provided outside of our normal business hours are subject to increased fees and technician availability and require your and our mutual consent to implement.

The priority given to implementing the Services will be determined our reasonable discretion, considering any milestones or deadlines expressly agreed upon in an invoice or email from Net-I. If no specific milestone or deadline is agreed upon, then the Services will be performed in accordance with your needs, the specific requirements of the job(s), and technician availability

Business Review / IT Strategic Planning Meetings:

The following Service(s), if listed in the Quote, will be provided to you.

Review existing technical environment to access possible improvements

Review Client business needs that may benefit from automation and/or improved efficiency through technology

Review upcoming technology upgrades

Annual Budget and Review as requested

Review existing Technology Security Standards and potential improvements

MANAGED BACKUP SERVICE(S):

The following Service(s), if listed in the Quote, will be provided to you.

24/7 monitoring of backup system, including offsite backup, offsite replication, and an onsite backup appliance ("Backup Appliance")

Troubleshooting and remediation of failed backup and cloud replication jobs

Troubleshooting and remediation of issues related to the Backup Appliance

Preventive maintenance and management of imaging software

Firmware and software updates of backup appliance

Problem analysis by the network operations team

Daily recovery and automated boot screen verification

Coordination of troubleshooting and remediation of failing backup jobs with Third-party backup service provider.

Backup Data Security: Backup data encryption varies by client. To ascertain that information Client may refer to the original Quote for Backup services, the Backup

Service fee detail on the monthly invoices, or by opening a service request by one of the means listed in

Backup Retention: Backed up data will be retained for up to 1 year in the cloud. Local Retention is based on device capacity and varies by client. Refer to the Quote for details on retention schedules.

Backup Alerts: Backup Jobs 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:

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. Note: Backup monitoring is limited to monitoring activities only and is not a backup and file recovery solution.

FIREWALL MANAGEMENT AND MONITORING SERVICE:

The following Service(s), if listed in the Quote, will be provided to you.

Scope of Work Inclusions:

24/7 external monitoring and alerting

Internet uptime monitoring with reporting (External monitoring of public facing WAN Interface on the firewall, System monitors ping response time and uptime. Alerts generated off consecutive failed ping times)

Administrator brute force monitoring (Monitor and alerting setup to monitor failed admin login attempts)

VPN brute force monitoring (Monitoring and alerting setup to monitor failed VPN login attempts)

Firewall temperature monitoring (Monitor and alerting setup to monitor system temp)

Memory usage monitoring (Monitor and alerting setup to monitor system memory usage / conserve mode activation)

License Expiration Monitoring

Configuration change alerts

Patch and Vulnerability Management

Firmware Updates

Bi-Annual Security Audits

Emergency Vulnerability Patching

Business related Web filtering whitelisting

Scope of Work Exclusions:

System Administration, VPN configuration, Non-Business related Web filtering whitelisting requests

This fee does not include the mandatory software and subscriptions contracts from the manufacturer upon initial expiration which is typically 36 months. These subscriptions are mandatory. Effective January 1, 2023 we no longer provide support to any client with a firewall that is not under an active security subscription.

Required Subscriptions:

Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, URL, DNS & Video Filtering, Antispam Service, and FortiCare Premium)

Cloud Management, Analysis and 1 Year Log Retention, Configuration backup and Device Configuration

REMOTE HELP DESK SUPPORT:

The following Service(s), if listed in the Quote, will be provided to you.

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

Microsoft 365 or Google Workspace Email and Application Support

Printing Support

Line of Business Access and Login Assistance

Password Lockout Resets

ONSITE DESKTOP AND PRINTER SUPPORT:

The following Service(s), if listed in the Quote, will be provided to you.

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

The following Service(s), if listed in the Quote, will be provided to you.

Onsite support provided for End User Endpoint and Printer during normal business hours for managed devices and covered software

REMOTE AND ONSITE INFRASTRUCTURE MAINTENANCE & SUPPORT:

The following Service(s), if listed in the Quote, will be provided to you.

Configuration, monitoring, and preventative maintenance services provided for the managed IT infrastructure, including Servers, UPS units, Network Switches and other infrastructure.

If remote efforts are unsuccessful, then Net-I 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:

The following Service(s), if listed in the Quote, will be provided to you.

Software agents installed in Covered Equipment (defined below) report status and IT-related events on a 24×7 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 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.

Software agents allow for support access by our technicians and can also be extended to client's staff or internal IT personnel for remote access and support.

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

Hardware Failures:

Yes – Server

No – Workstation

Device Offline:

Yes – Server

No – Workstation

Failed/Missing Updates:

Yes – Server

Yes – Workstation

Low Disk Space:

Yes – Server

No – Workstation

Excessive Uptime:

Yes – Server*

No – Workstation

Post Patching Scheduled Reboots (weekly)

Yes – Server

Yes – Workstation

Endpoint Security Service Failure/Missing Updates:

Yes-Server

Yes-Workstation

Internet Connectivity:

27x7x365 Internal and External ICMP with alerting

*Note-Not all servers can be scheduled for an automated reboot after patching due to application and Windows services startup issues that must be manually verified. In these cases, we will reach out to the Client and schedule a time to perform said task.

SERVER MONITORING AND AUTOMATED MAINTENANCE:

The following Service(s), if listed in the Quote, will be provided to you.

Software agents installed on covered servers report status and IT-related events on a 24×7 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

Automated routine operating system inspection and cleansing

Secure remote connectivity to the endpoint and collaborative screen sharing

Review and installation of updates and patches for Windows and supported software

Asset inventory and server information collection

ENDPOINT MONITORING AND AUTOMATED MAINTENANCE:

The following Service(s), if listed in the Quote, will be provided to you.

Software agents installed in covered Endpoints report status and IT-related events on a real time 24×7 basis; alerts are generated and responded to in accordance with the Service Levels described below.

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

Automated routine operating system inspection and optimization

Secure remote connectivity to the Endpoint and collaborative screen sharing

Review and automated delivery of updates and patches for Windows Desktop Operating Systems

Updates for support third-party applications such as Chrome

Asset inventory and server information collection

Automated post-update scheduled reboot with Notification Banner

ENDPOINT NEXT-GEN ANTIVIRUS & MALWARE PROTECTION:

The following Service(s), if listed in the Quote, will be provided to you.

Antivirus and malware protection for managed devices such as laptops, desktops, and servers.

Blocks suspicious actions before execution.

Malware detection and prevention – Blocks viruses, malware, Trojans, phishing, ransomware, spyware, browser-based attacks, cryptojacking, credential-stealing malware, script-based, and fileless attacks, and a wide range of other threats.

Multi-shield protection –multi-shield protection includes Real-Time, Behavior, Core System, Web Threat, Identity, Phishing, Evasion, and Offline shields for detection, prevention and protection from complex attacks.

Malicious script protection –Evasion Shield technology detects, blocks, and remediates (quarantines) evasive script attacks, whether they are file based, fileless, obfuscated, or encrypted, and prevents malicious behaviors from executing in PowerShell, JavaScript, and VBScript.

User identity and privacy protection – The Identity Shield (browser and application isolation) is trusted by the world's leading banks to stop attacks like DNS poisoning, keylogging, screen grabbing, cookie scraping, clipboard grabbing, and browser and session hijacking by malicious software.

White and blacklisting – Offers direct control over application execution. • Intelligent firewall – The system-monitoring and application-aware outbound firewall augments the built in Windows® firewall to protect users both on and off corporate networks.

* Please see Anti-Virus; Anti-Malware and Breach/Cyber Security Incident Recovery sections below for important details.

ENDPOINT DETECTION & RESPONSE (EDR):

The following Service(s), if listed in the Quote, will be provided to you.

24×7 network detection by Net-I technicians with response during normal business hours.

Real time and continuous (24×7) monitoring and threat hunting.

Real time threat response.

Alerts handled in accordance with our Alert Notification table, below.

Security reports, such as privileged activities, security events, and network reports, available upon request.

* 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.

MANAGED DETECTION & RESPONSE (MDR):

The following Service(s), if listed in the Quote, will be provided to you.

24×7 network detection and response by third-party Security Operations Center

Real time and continuous (24×7) monitoring and threat hunting.

Real time threat response.

Alerts handled in accordance with our Alert Notification table, below.

Security reports, such as privileged activities, security events, and network reports, available upon request.

24x7x365 access to a security team for incident response*

Next-generation deep learning malware detection, file scanning, and live protection for workstation operating system.

Web access security and control, application security and control, intrusion prevention system.

Detection and Response managed by Third-party provider.

Please see Anti-Virus; Anti-Malware and Breach/Cyber Security Incident Recovery sections below for important details.

DARK WEB MONITORING:

The following Service(s), if listed in the Quote, will be provided to you.

Credentials supplied by Client will be added into a system that continuously uses human and machine-powered monitoring to determine of 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:

The following Service(s), if listed in the Quote, will be provided to you.

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.

Held Mail Notification

Email Queuing

Please see Anti-Virus; Anti-Malware and Breach/Cyber Security Incident Recovery sections below for important details.

Advanced Email Threat Protection:

The following Service(s), if listed in the Quote, will be provided to you.

Includes all of the features of Email Threat Protection along with advanced threat prevention through the use of sandboxing and removal of suspicious code within common attachments. Additionally, the solution integrates on-demand email remediation to remove messages previously delivered to O365 employee mailboxes that were later determined to be malicious or violated internal email use policies.

All hosted email is subject to the terms of our Hosted Email Policy and our Acceptable Use Policy.

END USER SECURITY AWARENESS TRAINING:

The following Service(s), if listed in the Quote, will be provided to you.

Online, on-demand training videos (multi-lingual).

Proven educational approach for reducing risky employee behaviors that can lead to security compromise.

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.

HARDWARE AS A SERVICE (HAAS):

The following Service(s), if listed in the Quote, will be provided to you;

Scope. Provision and deployment of hardware and devices listed in the Quote or other applicable schedule ("HaaS Equipment").

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 if 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.

Repair/replacement of HaaS Equipment. Net-I 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, Net-I and has been determined by Net-I 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. Net-I 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, Net-I and has been determined by Net-I to be incapable of being remediated remotely.

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.

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 Quote, this Services Guide, or the Master Services Agreement.

Credits/Remedies. If Net-I 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 (2) 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 Net-I 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.

Term. When added any hardware added to a Master Services Agreement provided follows the term outlined in the Quote. The minimum term for a PC or Laptop is 36 Months. The minimum term for Server Hardware is 60 Months. Hardware returned prior to the terms will be billed at Net-I's discretion for the remainder of the term of the original Quote on which the hardware was provided.

NIST RISK ASSESSMENT:

The following Service(s), if listed in the Quote, will be provided to you.

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:

Cybersecurity Framework Functions Wheel

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:

The following Service(s), if listed in the Quote, will be provided to you.

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:

The following Service(s), if listed in the Quote, will be provided to you.

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 under Terms and Policies.

TWO FACTOR AUTHENTICATION

The following Service(s), if listed in the Quote, will be provided to you.

Advanced two factor authentication with advanced admin features.

Secures on-premises and cloud-based applications.

Permits custom access policies based on role, device, location.

Identifies and verifies device health to detect “risky” devices

SOFTWARE LICENSING (APPLIES TO ALL SOFTWARE LICENSED BY OR THROUGH NET-I)

The following Service(s), if listed in the Quote, will be provided to you.

All software provided to you by or through Net-I is licensed, not sold, to you (“Software”). In addition to any Software-related requirements described in Net-I’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

The following Service(s), if listed in the Quote, will be provided to you.

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.

Email Archiving / Information Archiving

The following Service(s), if listed in the Quote, will be provided to you.

Information Archiving Features and Benefits:

Unlimited cloud-based storage

eDiscovery for 50+data sources

Data Triplication across Three Geo-Redundant Datacenters

WORM-Compatible Storage (compliant with SEC and FINRA storage requirements)

Journal to Anywhere Technology

Attachment OCR Scanning and Content Indexing

Message Activity History (tracks all user activity at the message level, including exports, views, tagging, comments, and legal holds)

Software as a Service (SAAS) Protection

The following Service(s), if listed in the Quote, will be provided to you.

Information Archiving Features and Benefits:

Comprehensive backup and recovery solution for Microsoft 365 and Google Workspace

Automated, Continuous backups

Simple, Per User licensing

Provide independent backup copy outside of provider's platform for enhanced security

Provides longer retention of data than the standard retention times provided by provider's platforms

VOICE OVER IP (VOIP) SERVICES

The following Service(s), if listed in the Quote, will be provided to you.

Scalable VoIP-based with traditional telephone functionality including call transferring, voicemail, caller ID, call hold, conference calling, and call waiting functionalities.

Modern Enterprise functionality:

Softphone App: Turn any computer or mobile phone into your desk phone giving you the same on-the-go functional as you would have at your office

Call, Fax, Chat with coworkers, and check your Voicemail in a single application

Automate your business with tight integrations across many applications

Contact Center Capabilities, call recording and Agent Routing are available as add-on services.

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.

WI-FI MANAGEMENT SERVICES

The following Service(s), if listed in the Quote, will be provided to you.

Net-I will install at the Client's premises Wireless Access Points to provide a bandwidth of at least 10Mbps (download) in all areas requiring wireless network coverage, as agreed upon by Net-I and Client.

Net-I will maintain, supervise, and manage the wireless system at no additional cost.

Installed equipment, if provided by Net-I, will be compatible with the then-current industry standards.

Net-I 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).

Covered Equipment / Hardware / Software:

The following Service(s), if listed in the Quote, will be provided to you.

Managed Services will be applied to the devices on which we install software monitoring agents ("Covered Hardware"). You will be provided with an updated list of Covered Hardware once all software agents have been installed. 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. We will provide technical support for Covered Devices; however, all Covered Devices must be covered, at all times and at your cost, under a then-current manufacturer's service plan.

We will provide support for any software applications that are licensed through us. Such software ("Supported Software") will be supported on a "best effort" basis only, and any support required beyond Level 2-type support will be facilitated with the applicable software vendor/producer. Coverage for non-Supported Software is outside of the scope of the Quote and, if provided to you, will be provided to you on a "best effort" basis only with no guarantee of remediation.

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.

Should our technicians provide you with general advice concerning non-Supported Software, the provision of that advice should be viewed as an accommodation to you, and not as a continuing obligation or guarantee by Net-I to continue to provide such support or advice to you.

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

We provide the Services on a "per user" basis. As such, our managed services will be provided for up to two (2) Business Devices used by the number of users indicated in the Quote. 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 our software agent and end-point security (fee will apply) through which we (or our designated Third-party providers) can monitor the device. In this Services Statement, covered Business Devices are referred to as "Covered Hardware."

Physical Locations Covered by Services

Services will be provided remotely unless, in our discretion, we determine that an onsite visit is required. Net-I visits will be scheduled in accordance with the priority assigned to the issue (below) and are subject to technician availability. Unless we agree otherwise, all onsite Services will be provided at Client's primary business location. 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 Net-I's satisfaction.

The Services will continue through the Initial Term until terminated as provided in the Master Services 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 (45) 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.

Removal of Software Agents; Return of Firewall & Backup Appliances:

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

Within ten (10) days after being directed to do so, Client will remove, package and ship, at Client's expense and in a commercially reasonable manner, all hardware, equipment, and accessories provided to Client by Net-I that were used in the provision of the

Services. If you fail to timely return all equipment to us, or if the equipment is returned to us damaged (normal wear and tear excepted), then we will have the right to charge you, and you hereby agree to pay, the replacement value of all such unreturned or damaged equipment.

MINIMUM REQUIREMENTS / EXCLUSIONS:

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

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

Ø Customization of Third-party applications, or programming of any kind.

Ø Support for operating systems, applications, or hardware no longer supported by the manufacturer.

Ø Data/voice wiring or cabling services of any kind.

Ø Battery backup replacement.

Ø Equipment relocation.

Ø The cost to bring the managed environment up to these minimum requirements (unless otherwise noted in the Quote).

Ø 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 (SLA):

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 AM – 5 PM Central Time, excluding legal holidays and NetIntegration LLC -observed holidays as listed below), unless otherwise specifically stated in the Quote or as otherwise described below.

We will respond to problems, errors, or interruptions in the provision of the Services during business hours in the timeframe(s) described below. Severity levels will be determined by Net-I in our discretion after consulting with the Client. All remediation services will initially be attempted remotely; Net-I will provide onsite service only if remote remediation is ineffective and, under all circumstances, only if covered under the Service plan selected by Client.

Critical / Service Not Available (e.g., all users and functions unavailable, VIP/Owner unable to function)

Response within two (2) business hours after notification

Next available qualified technician will be assigned

Resolution Effort: Highest

Significant Degradation (e.g., large number of users or business critical functions affected)

Response within four (4) business hours after notification.

Resolution Effort: Medium to High

Limited Degradation (e.g., limited number of users or functions affected, business process can continue).

Response within eight (8) business hours after notification.

Resolution Effort: Medium

Small Service Degradation (e.g., business process can continue, no users affected).

Response within sixteen (16) business hours after notification.

Resolution Effort: Medium to Low

Long Term Project, Preventative Maintenance (e.g., no business user affected)

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 RMM Agent, 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.

Service Level response times do not apply to Time and Material Clients.

NON-BUSINESS HOUR SUPPORT:

The following Service(s), if listed in the Quote, will be provided to you.

Support for after-hours, Weekends and Holidays must be included in your Master Services Agreement. We reserve the right to refuse service any client who is not on a Service Plan that includes provisions for after-hours support.

Technical support provided outside of our normal business hours is offered on a case-by-case basis and is subject to technician availability. If Net-I 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 by default under any Service plan where it is not specifically quoted), and will be billed to Client at the following increased hourly rates:

Project Professional Level 1: 2x normal rate

Project Professional Level 2: 2x normal rate

Project Professional Level 3: 2x normal rate

Support Technician, Level 1: 2x normal rate

Support Technician, Level 2: 2x normal rate

Support Technician, Level 2: 2x normal rate

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

Business Hour Support Remote Support and a minimum of (2) hours minimum fee applies to Onsite Support.

Net-I-Observed Holidays:

Net-I observes the following holidays:

New Year’s Day

Good Friday (partial)

Memorial Day

Independence Day

Labor Day

Thanksgiving Day

The day following Thanksgiving Day

Christmas Eve (partial)

Christmas Day

New Year's Eve (partial)

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 the MSA), 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 Quote.

FEES:

The fees for the Services will be as indicated in the Quote. We reserve the right to charge for applicable non-quoted fees for unexpected events or client initiated projects that Net-i was not aware of in sufficient time to provide a quote. As an example a client contracting another provider to implement equipment such as printers, plotters, manufacturing equipment, offboarding services, and premise security systems such as access systems or cameras would not be covered under any service agreement.

Changes to Environment. Initially, you will be charged the monthly fees indicated in the Quote. Thereafter, if the managed environment changes, or if the number of authorized users accessing the managed environment changes, then you agree that the fees will be automatically and immediately modified to accommodate those changes.

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 and, if applicable, our data recovery-related 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.

In addition to the foregoing, we reserve the right to pass through to you any increases in the costs and/or fees charged by Third-party providers for the Third-party services ("Pass Through Increases"). Since we do not control Third-party providers, we cannot predict whether Pass Through Increases will occur, however, should they occur, we will endeavor to provide you with as much advance notice as reasonably possible.

Pass Through Increases are independent of any increases to our monthly recurring fees and will not be included in the five percent calculation described in the paragraph above.

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.

Automated Payment. You may pay your invoices by ACH, as described below.

ACH. When enrolled in an ACH payment processing method, you authorize us to electronically debit your designated checking or savings account, as defined and configured by you in our payment portal, for any payments due under the Quote. This authorization will continue until otherwise terminated in writing by you. We will apply a $35.00 service charge to your account for any electronic debit that is returned unpaid due to insufficient funds or due to your bank's electronic draft restrictions.

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 may 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. 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 & Policies

Endpoints

Endpoints are physical devices that connect to and exchange information with a computer network. Some examples of endpoints are mobile devices, desktop computers, virtual machines, embedded devices, and servers.

Authenticity

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

Monitoring Services; Alert Services

Unless otherwise indicated in the Quote, all monitoring and alert-type services are limited to detection and notification functionalities only. 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 Net-I; however, Client is advised to establish and/or modify the policies that correspond to Client's specific monitoring and notification needs.

Unless otherwise indicated in the Quote, all monitoring and alert-type services are limited to detection and notification functionalities only. Monitoring levels will be set by Net-I, 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 this Services Guide 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 in an efficient and effective manner; however, (a) we will not be responsible for the acts or omissions of Co-Managed Providers, or the remediation of any problems, errors, or downtime associated with those acts or omissions, and (b) in the event that a Co-managed Provider's determination on an issue differs from our position on a Service-related matter, we will yield to the Co-Managed Provider's determination and bring that situation to your attention

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. To improve security awareness, you agree that Net-I or its designated Third-party affiliate may transfer information about the

results of processed files, information used for URL reputation determination, security risk tracking, and statistics for protection against spam and malware. Any information obtained in this manner does not and will not contain any personal or confidential information.

Breach/Cyber Security Incident Recovery

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

Environmental Factors

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

Fair Usage Policy

Our Fair Usage Policy ("FUP") applies to all services that are described or designated as "unlimited" or which are not expressly capped in the number of available usage hours per month. An "unlimited" service designation means that, subject to the terms of this FUP, you may use the applicable service as reasonably necessary for you to enjoy the use and benefit of the service without incurring additional time-based or usage-based costs. However, unless expressly stated otherwise in the Quote, all unlimited services are provided during our normal business hours only and are subject to our technicians' 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—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 Net-I 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. Net-I 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 Net-I 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 Net-I 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. Net-I cannot and does not warrant that data corruption or loss will be avoided, and Client agrees that Net-I shall be held harmless if such data corruption or loss occurs. Client is strongly advised to keep both local and cloud backups of all of stored data to mitigate against the unintentional loss of data.

Procurement

Equipment and software procured by Net-I 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, Net-I 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. Net-I is not a warranty service or repair center. Net-I 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 Net-I will be held harmless, and (ii) Net-I 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 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.

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. Net-I will not hold an actual director or officer position in Client's company, and we will neither hold nor maintain any fiduciary relationship with Client. Under no circumstances shall Client list or place Net-I 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.

No Third-party Scanning

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

Obsolescence

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

Licenses

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

VOIP – Dialing 911 (Emergency) Services

The following terms and conditions apply to your use of any VoIP service that we facilitate for you or that is provided to you by a Third-party provider of such service. Please note, by using VoIP services you agree to the provisions of the waiver at the end of this section. If you do not understand or do not agree with any of the terms below, you must not subscribe to, use, or rely upon any VoIP service and, instead, you must contact us immediately.

There is an important difference in how 9-1-1 (i.e., emergency) services can be dialed using a VoIP service as compared to a traditional telephone line. Calling emergency services using a VoIP service is referred to as "E911."

Registration: You are responsible for activating the E911 dialing feature by registering the address where you will use the VoIP service. This will not be done for you, and you must take this step on your own initiative. To do this, you must log into your VoIP control panel and provide a valid physical address. If you do not take this step, then E911 services may not work correctly, or at all, using the VoIP service. Emergency service dispatchers will only send emergency personnel to a properly registered E911 service address.

Location: The address you provide in the control panel is the location to which emergency services (such as the fire department, the police department, etc.) will respond. For this reason, it is important that you correctly enter the location at which you are using the VoIP services. PO boxes are not proper addresses for registration and must not be used as your registered address. Please note, even if your account is properly registered with a correct physical address, (i) there may be a problem automatically transmitting a caller's physical location to the emergency responders, even if the caller can reach the 911 call center, and (ii) a VoIP 911 call may go to an unstaffed call center administrative line or be routed to a call center in the wrong location. These

issues are inherent to all VoIP systems and services. We will not be responsible for, and you agree to hold us harmless from, any issues, problems, incidents, damages (both bodily- and property-related), costs, expenses, and fees arising from or related to your failure to register timely and correctly your physical location information into the control panel.

Address Change(s): If you change the address used for E911 calling, the E911 services may not be available and/or may operate differently than expected. Moreover, if you do not properly and promptly register a change of address, then emergency services may be directed to the location where your services are registered and not where the emergency may be occurring. For that reason, you must register a change of address with us through the VoIP control panel no less than three (3) business days prior to your anticipated move/address change. Address changes that are provided to us with less than three (3) business days notice may cause incorrect/outdated information to be conveyed to emergency service personnel. If you are unable to provide us with at least three (3) business days notice of an address change, then you should not rely on the E911 service to provide correct physical location information to emergency service personnel. Under those circumstances, you must provide your correct physical location to emergency service dispatchers if you call them using the VoIP services.

If you do not register the VoIP service at your location and you dial 9-1-1, that call will be categorized as a "rogue 911 call." If you are responsible for dialing a rogue 911 call, you will be charged a non-refundable and non-disputable fee of $250/call.

Power Loss: If you lose power or there is a disruption to power at the location where the VoIP services are used, then the E911 calling service will not function until power is restored. You should also be aware that after a power failure or disruption, you may need to reset or reconfigure the device prior to utilizing the service, including E911 dialing.

Internet Disruption: If your internet connection or broadband service is lost, suspended, terminated or disrupted, E911 calling will not function until the internet connection and/or broadband service is restored.

Account Suspension: If your account is suspended or terminated, then all E911 dialing services will not function.

Network Congestion: There may be a greater possibility of network congestion and/or reduced speed in the routing of E911 calls as compared to 911 dialing over traditional public telephone networks.

INDEMNIFICATION: Client hereby agree to release, indemnify, defend, and hold Net-I and its officers, directors, representatives, agents, and any Third-party service provider that furnishes VoIP-related services to Client, harmless from any and all liabilities, claims, demands, causes of action, expenses, damages, fines, and assessments, including, without limitation, costs, attorneys' fees, and expenses (collectively, "Claims") whatsoever arising out of, based upon, occasioned by or in connection with the Services, VoIP services, including but not limited to any failure or outage of the VoIP services, incorrect routing or use of, or any inability to use, E911 dialing features. The foregoing waiver and release shall not apply to Claims arising from Net-I's gross negligence, recklessness, or willful misconduct.

DEFAULT: Client is responsible for all costs and expenses incurred by Net-I in collection of payments from Client, including reasonable attorneys' fees. Client's failure to make payment when due shall entitle Net-I to suspend its Services under the Master Services Agreement until all past-due amounts are paid, plus any late fees or interest, and the price of Services (as detailed in the Quote) shall be increased by any costs incurred by Net-I arising out of suspension of the Master Services Agreement, including, without limitation, deactivation and reactivation of the Services. In the event that Client fails to pay any sums due and payable or perform any duties stated herein, refuses to upgrade or update to Net-I's latest Services offerings, or otherwise fails to comply with any of the

covenants, conditions and agreements contained herein or in any other agreement, the Master Services Agreement, document or instrument executed by Client and Net-I in connection herewith (a "Default"), and fails to cure such Default within thirty (30) days from the date payment was due or notice of Default given by Net-I to Client, Net-I shall have the right to terminate the Master Services Agreement, and in such event, Client shall be liable to Net-I for all damages, costs, and expenses, including attorneys' fees arising out of the Client's Default.

LIMITATION OF LIABILITY: Net-I's liabilities to you shall be limited to direct actual damages. In no event shall Net-I be liable to you for any amount exceeding the price of Services (as detailed in the Quote). Net-I will not be liable to you for consequential, incidental, punitive, special, exemplary, or indirect damages. These limitations apply without regard to the cause of any liability or damage. There are no third-party beneficiaries to this Services Guide or your Quote.

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").

Net-I 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: Net-I 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. v

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.

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 Net-I 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. The guidelines for Marketing Email are provided by the FTC at CAN SPAM ACT.

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, Net-I’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, DNS requests, or website access for any web requests made from within the hosted environment.

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