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 <u>all</u> managed services provided or facilitated by Forum Info-Tech, Inc. ("Forum Info-Tech," "we," "us," or "our"); however, only those services specifically described in the Quote (collectively, the "Services"). will be facilitated and/or provided to you ("Customer," "you," or "your").

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.

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 ERP, CRM and other SaaS applications
- Review of overall business and application workflow
- 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
- Office Telephone, Wireless, Print and Internet Service 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If deficiencies are discovered during the auditing process (such as outdated equipment or unlicensed software), we will bring those issues to your attention and discuss the impact of the deficiencies on our provision of the Services and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 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 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.
- Onboard and transfer licensing management through partner agreements with Microsoft, AWS, and other applicable tools.

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 <u>not</u> 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, .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.

Off Boarding

- Subject to the Customer's payment of any and all fees and charges due through the date of expiration or termination and if Customer is not in breach or default of any of its obligations hereunder, Forum Info-Tech will perform the following tasks for offboarding:
- Removal of monitoring agents from Servers
- Removal of Endpoint Protection software from Servers
- Removal of monitoring agents from Workstations
- Removal of Endpoint Protection software from Workstations
- Removal of Microsoft 365 Licenses from client's account
- Removal of SQL or Remote Desktop licenses provided by Forum Info-Tech
- Removal of credentials from Network devices
- Removal of Backup software from Servers
- Removal of Microsoft 365 Backup
- Removal of FIT Security Care products
- Removal of all client data from internal systems, including documentation and passwords
- Instruct and advise client on removal of consolidated billing on all cloud platforms

Ongoing / Recurring Services

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

The following Services/Service Plans, if listed on the Quote, will be provided to you.

Workstation Care

8x5 Proactive Monitoring

This product monitors the health of a workstation, proactively warning us about possible hardware failures and application errors. It also allows tech support or the end user to remotely connect to the workstation through LogMeIn Pro.

Antivirus Licensing & Monitoring

This product provides basic malware protection. Our system administrators will receive alerts about threats found and remediate any problems remotely. Advanced Endpoint Protection is available as an upgrade, and it includes behavior detection, firewall and web filtering.

Proactive Patching Services

When Microsoft releases patches, our NOC team will test the patches for one week to mitigate possible issues. Once patches are tested, they may be whitelisted or blacklisted for deployment. Whitelisted patches are deployed on a scheduled decided by the customer.

Operating System Support

We provide technical support for the Operating System installed on the workstation. This includes troubleshooting error messages, device drivers, feature updates and system health.

Remote Hardware Diagnostics

We offer remote assistance in diagnosing hardware problems. Onsite visits are available at an extra cost.

User Care

Technical Support – Microsoft Applications

We will assist users with applications developed by Microsoft, such as Microsoft Office, Teams, Planner, etc.

Technical Support – Corporate Email Security

We will assist with set up of multi-factor authentication for email accounts and assist users identifying threats sent by email messages (phishing, malicious payloads, etc.)

Technical Support – Cloud Connectivity

We will assist users with cloud connectivity problems on authorized workstations. This includes problems with credentials, multi-factor authentication or issues with the LevelCloud Dashboard.

Technical Support – Current Application

We will provide technical support only for Current line-of-business ("LOB") applications. A Current LOB Application is an application that has not been discontinued or retired by the developer or distributor of the application, that the developer or distributor offer standard support and maintenance services for and has a valid and current maintenance agreement between the client and the developer or distributor.

If we are unable to remediate an issue with a Current LOB Application, 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 Current LOB Applications ("Service Contract").

On occasion and in our discretion, we may provide you with advice or suggestions concerning support for non-Current LOB Applications. Please note, if such advice or suggestions are provided, they are on a "best efforts" basis with no guarantee of remediation whatsoever. If you request that we work with a vendor/manufacturer to diagnose or remediate issues with non-Current LOB Applications, then that service, if provided to you, will be billed to you at out then-current hourly rates. In addition, the vendor/manufacturer may charge service fees to provide such support, and those fees will be passed through to you.

Vendor Management - Current Application

If problems cannot be solved by basic support, Forum Info-Tech will be the interface between the Customer and the vendor. We will contact the company responsible for application and work with them, on behalf of the Customer, until the problem is resolved. Please note: We do not warrant or guarantee that any particular issue or problem can or will be resolved by the applicable vendor, nor do we guarantee that the issue(s) or problem(s) will be fully remediated in a particular time period.

Multi Factor Authentication

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.

Server Care

24x7 Proactive Monitoring

This product monitors the health of a server, proactively warning us about possible hardware failures and application errors. It also provides information about failed services, disk space and performance.

24x7 Emergency Technical Support

If servers are not working or reporting offline, our team will provide 24x7 support for your critical workloads.

Antivirus Licensing & Monitoring

This product provides basic malware protection. Our system administrators will receive alerts about threats found and remediate any problems remotely.

Proactive Patching Services
When Microsoft releases patches, our NOC team will test the patches for one week to mitigate possible issues. Once patches are tested, they may be whitelisted or blacklisted for deployment. Whitelisted patches are deployed on a scheduled decided by the customer.

Remote / In-House / On Site Hardware Diagnostics

In case servers have problems that cannot be fixed remotely, we provide in-house and onsite support for critical workloads until functionality is restored.

Database Care Services

For applications that use database services like Microsoft SQL Server, Progress, Pervasive, Oracle and others, our team provides database maintenance services following industry best practices.

Vendor Management - Warranty Services

If physical components of a server should fail, our team works directly with the manufacturer to obtain replacement parts and install them as fast as possible. We also monitor warranty of servers and work with our customers to plan for server replacements before warranty expires.

Data Care

Server Backup Monitoring & Maintenance

We will monitor your server backup jobs 24/7, including offsite backups and provide maintenance on backup chains and backup retention to meet the customers' needs. We will also provide data restoration services in case of disaster or human error.

Offsite Replication & Retention

Backups will be replicated to a second and third locations depending on customers' needs and compliance requirements. Backed up data will be retained at a minimum on a rolling 7 day basis.

Backup Testing

We will test restoring backups from the current backup set every 30 days or less, depending on customers' needs. This ensures backups are healthy and can be restored from.

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 6:00am – 6:00pm PST Monday through Friday, excluding Forum Info-Tech observed holidays
- Request Method. Requests to restore backed up data should be made by creating a support ticket. Requests made by any other method may delay our response to you.
- 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.

Network Care

Network Switch Monitoring & Maintenance

We will provide basic switch monitoring (basic status as online / offline and system hardware load load) or advanced switch monitoring (traffic insights, VLANs, security, etc.), along with remediation in case of failure and firmware upgrades.

Firewall / Router Monitoring & Maintenance

We will provide basic firewall / router monitoring (basic status as online / offline and system hardware load) or advanced firewall monitoring (traffic insights, VLANs, security, etc.), along with remediation in case of failure and firmware upgrades.

Wireless Infrastructure Monitoring & Maintenance

We will provide wireless infrastructure monitoring and maintenance. This service includes wireless surveys, optimization of access point placement, creation / removal / maintenance of wireless SSIDs and wireless security.

Quality of Service Monitoring & Maintenance

We will advise and assist with Quality-of-Service configurations for sensitive services such as video conferencing and VoIP.

Virtual CIO Service (vCIO Service)

Forum Info-Tech will act as the main point of contact for certain business-related IT issues and concerns. For example, we will:

- Assist in 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.

FIT Secure Care

Please see "[Anti-Virus; Anti-Malware"](#) and "[Breach / Cyber Security Incident Recovery"](#) sections below for important details.

Microsoft Security Essentials

Built on the robust foundation of the Microsoft 365 platform and fortified with security features from our cutting-edge automation engine, Secure Care Microsoft Security Essential services are designed to provide your users with a stable and user-friendly environment. Please note Microsoft Security Essentials requires a minimum of M365 Business Premium Licenses from Microsoft.

Our Baseline Security comes with all these benefits:
- Entra ID risk remediation
- Customized Exchange rules
- Guest access limitations
- Compliance policies ensure company data is accessible only from registered devices
- Microsoft Secure Score of over 80%
- Permanent Single Sign-On (SSO)
- Automated application deployment

- Automatic device enrollment (sign-in on any new computer, and it will be enrolled with all settings and applications)
- Windows Tweaks and optimizations
- Windows and Edge ads/news blocker
- Phish and Spam Protection Policies
- Synced Edge profile
- OneDrive auto sign-in and backup of user documents
- Windows Sign-In with MFA (Bluetooth, face recognition, fingerprint, or YubiKey) [Optional]
- Mobile phone security policies, extra encryption and authentication layer
- Defender for Endpoint Cloud Protection (EDR)

Endpoint Security as a Service

SOC (Security Operations Center) analyst supported endpoint protection & next generation anti-virus solution utilizing behavioral AI for workstations and servers.

- Single Solution: Combining Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) capabilities into a single platform.
- Proactive Protection: Our solution delivers enterprise-class prevention, threat detection, response, and hunting.
- End-to-End Coverage: Our solution works to find threats across enterprise environments, including endpoint, cloud and IoT.
- Integrated intelligence: We ensure up-to-date threat detection with the latest information from third-party and proprietary sources.

Email Threat Protection

Email Security protects against business email compromise and extends protection to your company's vital data-sharing hubs such as Email and Messaging Protection, Collaboration Protection and File Sharing Protection platforms.

Key Features:
- Anti-Malware and Ransomware: Our multilayer security detects zero-day threats and malicious behavior, quarantining harmful files in real-time.
- Anti-Phishing Software: To catch advanced attack, we leverage AI/ML analyzes every aspect of an email, including trusted senders, to identify fraud.
- Account Takeover Protection: We use historical ML analysis to identify past breaches, filter false positives and prevent future account takeover.
- Smart Data Loss Prevention: Our platform identifies confidential files, prevents accidental sharing, and limits the ability to print, copy, paste or screen captures.
- Incident Response as a Service: IRaaS provides expert management of end-user reports of suspicious content and request to release quarantined emails.

- Incoming outgoing and internal emails are easily archived for reference, ensuring business continuity and compliance.

SaaS Monitoring

SOC (Security Operations Center) supported SaaS Alerts monitor your SaaS applications and send real-time alerts for any unusual activities including data breaches, configuration changes, and access violations across your SaaS stack, including Microsoft 365, Google, Workspace, Salesforce, Slack, Dropbox, and others.

Vulnerability Scanning

Secure care Vulnerability Scanning utilizes advanced vulnerability scanning tools to identify potential weaknesses in your systems, applications, and network devices.
- Vulnerability scanning covers a wide range of assets, including servers, workstations, firewalls, routers, and web applications.
- Vulnerability scanning can discover and identify potential vulnerabilities in systems, applications, and network infrastructure.

Vulnerability Management

Secure Care Vulnerability Management combines people power with data mining and machine learning technology to uncover, prioritize, and block the holes in your defense continuously – 24/7/365, taking defense from "reactive' to "adaptive" to stay ahead of evolving threats.

- DETECT: Our automated AI engine provides state-of-the-art vulnerability detection and continuous assessment of your security posture.
- IDENTIFY: Our solution identifies known and unknown assets present in the network and sends immediate alerts of critical threats and new vulnerabilities.
- PROTECT: Our solution leverages AI machine learning to accurately identify, rate, and prioritize the most at-risk assets in your environment.
- RECOVER: Our action plans help remediate vulnerabilities quickly by patching systems and applying configuration hardening easily and efficiently.
- COMPLY: Our solution monitors your environment for cyber-hygiene and compliance with regulatory or industry data privacy and security mandates.

Phishing and Training

Secure Care Phishing and Training is a solution to keep your users sharp and well trained to protect your most valuable data, and to help identify potential malware and phishing attacks before they can infiltrate your organization's network.

- 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.

Dark Web Monitoring Service

Credentials supplied by the Client will be added into 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.

MXDR – Critical Servers

SOC Supported Managed Extended Detection and Response (MXDR) is a is a vendor-agnostic XDR solution that consolidates multiple security products into a single platform to better corelate, detect, and respond to threats. This centralized platform empowers security teams to identify threats and breaches, and provides context around incidents that can bolster and speed up response and remediation more quickly and easily. This solution requires an agent to be installed on the most critical assets.

Key Security Benefits:
- Protects entire attack surface
- Enhances existing infrastructure with superpowered AI
- Delivers best-in-class intelligence regardless of existing security products and services
- Deploys across network, cloud, and endpoint infrastructure
- Generates exponential improvements in detection (MTTD) & response (MTTR) times
- 24/7 SOC Team

Key Features:
- Built-in integrated with FIT Email Threat Protection, FIT SaaS Protection, FIT Managed Endpoint Security as a Service
- Comprehensive, automatic sensor-based data collection
- Physical (on-premises) and cloud visibility
- Integrated IDS/IPS paired with AI to reduce false positives

    Additional Asset(s): Secure Care XDR with 1 year log storage

MXDR _ Firewall

SOC Supported Managed Extended Detection and Response (MXDR) – Firewall is a device that will passively collect network traffic information, check for known IDS signature events, provide an on-premise malware sandbox, and act as a syslog server for the XDR platform to collect logging information from on-prem assets. The device has 250Mb/s of network logging throughput and

includes the yearly IDS security sensor license for the XDR platform.

Key Security Benefits:
- Protects entire attack surface
- Enhances existing infrastructure with superpowered AI
- Delivers best-in-class intelligence regardless of existing security products and services
- Deploys across network, cloud, and endpoint infrastructure
- Generates exponential improvements in detection (MTTD) & response (MTTR) times
- 24/7 SOC Team

Key Features:
- Built-in integration with FIT Email Threat Protection, FIT SaaS Protection, FIT Managed Endpoint
- Comprehensive, automatic sensor-based data collection
- Physical (on-premises) and cloud visibility
- Integrated IDS/IPS paired with AI to reduce false positives
- Security as a Service

Additional Asset(s): Secure Care XDR with 1 year log storage

MXDR – Network
SOC Supported Managed Extended Detection and Response (MXDR) – Network provides firewall syslog and network traffic ingestion from small networks (less than 8 GB/day). MXDR Network includes network traffic analysis with Suricata IDS. Firewall response actions and SOAR (Security Orchestration Automation Response) included.

Key Security Benefits:
- Protects entire attack surface
- Enhances existing infrastructure with superpowered AI
- Delivers best-in-class intelligence regardless of existing security products and services
- Deploys across network, cloud, and endpoint infrastructure
- Generates exponential improvements in detection (MTTD) & response (MTTR) times
- 24/7 SOC Team

Key Features:
- Built-in integrated with FIT Email Threat Protection, FIT SaaS Protection, FIT Managed Endpoint Security as a Service
- Comprehensive, automatic sensor-based data collection
- Physical (on-premises) and cloud visibility
- Integrated IDS/IPS paired with AI to reduce false positives

Additional Asset(s): Secure Care XDR with 1 year log storage

Please see "[Anti-Virus; Anti-Malware"](#) and "[Breach / Cyber Security Incident Recovery"](#) sections below for important details.

Additional Available Services

The following services are available on an ad-hoc, by-request basis, and will be provided to or facilitated for you only if specifically listed in the Quote. Additional fees will apply for these services unless they are expressly included in one of our Service Plans listed above.

FIT Vulnerability Assessment
Our Vulnerability Assessment are done by scanning your Public IP address. Our team inspects the client's network for known vulnerabilities or weaknesses, while the Pen Test attempts to gain access to the clients network. Both are done in accordance with highest security standards and best practices, keeping the client compliant with any industry or state/federal regulations. The Summary and Technical Report will identify & grade vulnerabilities or weaknesses that need to be addressed and remedied, and you and your team can of course charge separately for that service. (We are also available for remediation work if necessary, at an additional cost.)

FIT Penetration Testing
A penetration test is the process of identifying and exploiting vulnerabilities, trying to use the most diverse methods from the perspective of an attacker. This process is a key part of the information security, allowing quickly and effectively identify vulnerabilities and their proper risk.

The vulnerability assessment process aims at identifying and reporting on observed vulnerabilities. A penetration test attempts to exploit vulnerabilities of existing systems to determine whether unauthorized access and / or malicious code execution is possible. The test includes testing the network and application layers and can be performed externally (run external to the customer's network, for example via the Internet) and / or internally (performed within the customer's network).

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.

Security Incident and Event Monitoring (SIEM)

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 Forum Info-Tech's services on a time and materials basis.

Updates and Patching

Please refer to FIT Patching Policy on definitions of various types of patching, frequency and other details

Labor for New / Replacement Workstations

Includes all labor charges for setup of new workstations, or replacement of existing workstations.

- Labor covers:
  - New computers / additional computers added during the term of the Quote
  - Replacement of existing computers that are four (4) or more years old (as determined by the manufacturer's serial number records)
  - Replacement of existing computers that lost/stolen or irreparably damaged and/or out of warranty but not yet four years old
  - Operating systems upgrades – subject to hardware compatibility

Digital Signage Service

This services is for clients that need to display things on their TV's This service includes the cloud Software Licensing and Support and is billed per TV.

Marketing4WiFi Dashboard

A service that provided a collection of services to provide a WiFi Landing page for guests. This service is usually charged per Wireless Access Point.

<u>Software Licensing</u>

(applies to all software licensed by or through Forum Info-Tech)

All software provided to you by or through Forum Info-Tech is licensed, not sold, to you ("Software"). In addition to any Software-related requirements described in Forum Info-Tech's Master Services Agreement, Software may also be subject to end user license agreements (EULAs), acceptable use policies (AUPs), and other restrictions all of which must be strictly followed by you and any of your authorized users. When installing/implementing software licenses in the managed environment or as part of the Services, we may accept (and you agree that we may accept) any required EULAs or AUPs on your behalf. **You should assume that all Software has an applicable EULA and/or AUP**

to which your authorized users and you must adhere. If you have any questions or require a copy of the EULA or AUP, please contact us.

Covered Hardware

Unless otherwise stated in the Quote, Managed Services will be applied to the technology assets such as computers, servers, and networking equipment owned by the Customer. Forum Info-Tech will assist connecting from a personal device to the organization's technology at the Customer's discretion, but **support of any personal devices is not included**. Forum Info-Tech may exclude specific devices not under a maintenance and support agreement from the applicable hardware manufacturer or beyond typical useful life for such hardware ("Covered Hardware").

Physical Locations Covered by Services

Services will be provided remotely unless, in our discretion, we determine that an onsite visit is required. Forum Info-Tech 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 Forum Info-Tech's satisfaction.
The Services will continue through the Initial Term until terminated as provided in the Agreement, the Quote, or as indicated in this section (the "Service Term").

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 Forum Info-Tech 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:

- Server hardware must be under current warranty coverage.
- All equipment with Microsoft Windows® operating systems must be running then-currently supported versions of such software and have all of the latest Microsoft service packs and critical updates installed.
- All software must be genuine, licensed, and vendor-supported.
- Server file systems and email systems (if applicable) must be protected by licensed and up-to-date virus protection software.
- The managed environment must have a currently licensed, vendor-supported server-based backup solution that can be monitored.
- All wireless data traffic in the managed environment must be securely encrypted.
- 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 provide us with exclusive administrative privileges to the Environment.
- Client must not affix or install any accessory, addition, upgrade, equipment, or device on to the firewall, server, or NAS appliances (other than electronic data) unless expressly approved in writing by us.

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

- Customization of third party applications, or programming of any kind.
- Support for operating systems, applications, or hardware no longer supported by the manufacturer.
- Data/voice wiring or cabling services of any kind.
- Battery backup replacement.
- Equipment relocation.
- The cost to bring the managed environment up to these minimum requirements (unless otherwise noted in the Quote).
- The cost of repairs to hardware or any supported equipment or software, or the costs to acquire parts or equipment, or shipping charges of any kind.

Service Levels

Automated monitoring is provided on an ongoing (*i.e.*, 24x7x365) basis. Response, repair, and/or remediation services (as applicable) will be provided only during our business hours (currently M-F, 6 AM – 6 PM Pacific Standard Time, excluding legal holidays and Forum Info-Tech 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 Forum Info-Tech in our discretion after consulting with the Client. All remediation services will initially be attempted remotely; Forum Info-Tech will provide onsite service only if remote remediation is ineffective and, under all circumstances, only if covered under the Service plan selected by Client.

Trouble	Priority	Response time (in hours) *
Service not available (all users and functions unavailable).	1	Within 1 hour
Significant degradation of service (large number of users or business critical functions affected)	2	Within 2 hours

Limited degradation of service (limited number of users or functions affected, business process can continue). Small service degradation (business process can continue, one user affected).	3	Within 2 hours

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

<u>Rates</u>

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 Forum Info-Tech 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:

Business Hours Remote Support Monday-Friday, 8am PST to 5pm PST excluding holidays	Included
Business Hours Onsite Support Monday-Friday, 8am PST to 5pm PST excluding holidays	$175/hour
Emergency* After Hours Remote Support All other times and on observed holidays	$250/hour
Emergency* After Hours Onsite Support All other times and on observed holidays	$250/hour
Non-Emergency After Hours Remote Support All other times and on observed holidays (subject to availability)	$250/hour

Non-Emergency After Hours Onsite Support All other times and on observed holidays (subject to availability)	$250/hour

*Emergency shall be defined as a Priority 1 event.

Note:

- All hourly services are billed in 15-minute increments, and partial increments are rounded up to the next highest increment.
- A one (1) hour minimum applies to all Non-Business Hour Support.
- A four (4) hour minimum, in addition to travel time, applies to all on-site service calls. Billing and Technician travel time are calculated based upon the table above.
- The above-listed rates are subject to change from time to time.

<u>**Forum Info-Tech-Observed Holidays**</u>: Forum Info-Tech observes the following holidays:

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

<u>Fees</u>

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

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

Travel Time. If onsite services are provided, it will be billed to you at our current hourly rates, portal to portal and roundtrip. 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.

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 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 Forum Info-Tech; 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 Forum Info-Tech, 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 Forum Info-Tech 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, or (iv) declining to work with the technician we select to work on your particular issue or problem.

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 Forum Info-Tech 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. Forum Info-Tech 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 Forum Info-Tech 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 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 Forum Info-Tech 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. Forum Info-Tech cannot and does not

warrant that data corruption or loss will be avoided, and Client agrees that Forum Info-Tech 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 Forum Info-Tech 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, Forum Info-Tech 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. Forum Info-Tech is not a warranty service or repair center. Forum Info-Tech 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 Forum Info-Tech will be held harmless, and (ii) Forum Info-Tech 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 by us in our capacity as a virtual chief technology or information officer will be for your informational and/or educational purposes only. Forum Info-Tech 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 Forum Info-Tech on Client's corporate records or accounts.

Sample Policies, Procedures.

From time to time, we may provide you with sample (*i.e.*, template) policies and procedures for use in connection with Client's business ("Sample Policies"). The Sample Policies are for your informational use only, and do not constitute or comprise legal or professional advice, and the

policies are not intended to be a substitute for the advice of competent counsel. You should seek the advice of competent legal counsel prior to using or distributing the Sample Policies, in part or in whole, in any transaction. We do not warrant or guarantee that the Sample Policies are complete, accurate, or suitable for your (or your customers') specific needs, or that you will reduce or avoid liability by utilizing the Sample Policies in your (or your customers') business operations.

Penetration Testing; Vulnerability Assessment

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

No Third Party Scanning

Unless we authorize such activity in writing, you will not conduct any test, nor request or allow any third party to conduct any test (diagnostic or otherwise), of the security system, protocols, processes, or solutions that we implement in the managed environment ("Testing Activity"). Any services required to diagnose or remediate errors, issues, or problems arising from unauthorized Testing Activity 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."

<u>Registration</u>: 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.**

<u>Location</u>: 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 <u>not</u> where the emergency may be occurring. **For that reason, you <u>must</u> register a change of address with us through the VoIP control panel no less than three (3) business days <u>prior</u> 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 **<u>must</u>** 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.

WAIVER: You hereby agree to release, indemnify, defend, and hold us and our officers, directors, representatives, agents, and any third party service provider that furnishes VoIP-related services to you, harmless from any and all claims, damages, losses, suits or actions, fines, penalties, costs and expenses (including, but not limited to, attorneys' fees), whether suffered, made, instituted or asserted by you or by any other party or person (collectively, "Claims") arising from or related to the 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 our gross negligence, recklessness, or willful misconduct.

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").

Forum Info-Tech 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**: Forum Info-Tech 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.

- **Crypto mining.** 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 Forum Info-Tech 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, Forum Info-Tech'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.