STATEMENT OF WORK

This Statement of Work ("SOW") is governed under the Master Service Agreement located at https://www.itsupportri.com/terms-and-conditions/ (the "Agreement"), and further describes and governs the provisions of the quote that incorporates this SOW by reference (the "Quote"). If you do not have a copy of the Agreement or cannot access the Agreement, or if you do not agree with the terms of this SOW, please do not accept the Quote and contact us for further information. This SOW is effective as of the date that you accept the Quote ("Effective Date").

Scope of Services

The following services (collectively, "Services") will be provided to you based on the plan you selected in the Quote ("Selected Plan"):

Office Solutions (Service Scope):

Office Solutions will consist of maintaining all servers and workstations with the following:

- Included Service & Support Outlined Below
- Offsite & Local Backups (**Servers Only**)
- 24/7 Server & Desktop Monitoring
- Cloud Antivirus & Malware Protection
- Microsoft Windows Patch Management
- Client Payment Portal and Ticket Access
- Security Firewall - Includes support for device, IPS, and VPN (**Firewalls Only**)

Included Services (within Hours of Operation):

- Remote PC Management/Help Desk Support
- Remote Network Management
- Remote Server Management
- Network Monitoring
- Onsite Labor

Billable Services:

- Remote Labor *(outside Hours of Operation)*
- On-Site Labor *(outside Hours of Operation)*
- Any services referenced in "Excluded Services" section

- If devices are added and/or removed from the Selected Plan, billing will be adjusted based on current count of services provided.
- If a device is removed after the first day of the month, no refund will be given for said computer/device.
- All computers and other devices on or attached to the managed environment ("Environment") must be covered under a SNECS service plan.
- Client must notify us of any changes to the Environment. Failure to alert us of Environment changes may result in downtime or issues that will require remediation at our then-current hourly rate.
- Support will be provided to all computers/devices as per your Selected Plan.
- Unless otherwise stated in writing, if a computer is offline, we may continue to bill for it unless Client requests removal of offline device.
- Client cannot reduce devices covered below 75% of the number of devices initially indicated in the Quote.
- Any future additions to the Service Scope will extend all currently billed services to the newest Service Scope term and Agreement signed upon.

Hosted Exchange (Service Scope):

Hosted Exchange (Only Available for Maintained Computers)

- Full versions of Office applications: Word, Excel, PowerPoint, Outlook, Publisher, and OneNote
- Cloud Hosted Exchange – Emails, Calendars, and Contacts
- Microsoft Teams - Includes IM and HD video conferencing.
- Employee Access Controls – Including "Remote Wipe"
- Spoof, Spam, and Phishing Protection for Emails
- Standard Email Management & Support – Includes Adding/Removing Users

Employee Productivity Package (Service Scope):

Employee Productivity Package (Only Available for Maintained Computers)

- Remote Workstation Screenshots with Real-Time Activity Monitoring
- Alarms for Specific Programs/Websites, Customize Based on User/Group
- Log Every Activity for Compliance & HIPAA Compliant Options
- Block Unproductive Activity Automatically
- Workflow and Productivity Insight

Password Manager (Service Scope):

Password Manager (Only Available for Maintained Computers)

- Manage login/payment credentials
- Encrypt saved credentials
- Share credentials securely

Quick Restore Server (Service Scope):

Quick Restore Server (Only Available if on Office Solutions Plan)

- Redundant Business Server Failover System
- Complete Server Backups Done Nightly
- Estimated Server Restoration in 3 Hours or Less
- Ability to Run Business While Main Server Is Repaired
- Required for Compliance in Many Business Continuity Plans

Backup Internet Service (Service Scope):

Backup Internet Service (Only Available if on Office Solutions Plan)

- Redundant Internet Service Provider **(ISP)** Failover System
- Cloud Based Internet Service for When Main ISP Goes Down
- Ability to Run Business While Main ISP Service Is Restored
- Avoid Downtime & Lost Productivity Due to ISP Failure
- Perfect for Businesses That Rely on Cloud Computing to Work

VoIP Telephone Services (Service Scope):

VoIP Telephone Services (Only Available if on Office Solutions Plan)

- Customizable Phone Services That Can Scale with Your Business
- Connect Multiple Extensions Together with Ring Groups
- Call Forwarding, Call Parking, Hold Music, and Voicemail Services
- Phone Number Porting Available (Transfer Existing Number)
- Alternative Failover Phone Destination (In Case of Local Outage)

Security Bundle (Service Scope):

Security Bundle (Only Available for Maintained Computers)

- Email Account
- Workstation and Email MFA
- Email Fraud and Forgery Protection / Email Spam Protection

Cloud Hosted Server (Service Scope):

Cloud Hosted Server (Only Available for Maintained Computers)

- Cloud Hosted Server
- Custom Specifications Based on Client Needs
- Regulated Functionality for Security Purposes

Projects. The following services are considered to be projects (collectively, "Projects") and will be provided to Client only if expressly indicated in the Quote.

Office Solutions Onboarding Phase (Projects Scope):

- During onboarding, multiple SNECS techs will be scheduled for the Projects, working on-site and/or remotely.
- The main server at each location will be supplied with/connected to a battery backup (UPS) in case of a surge and an external hard drive for local backups.
- SNECS will attempt to install & configure a Security Firewall to prevent unauthorized network intrusion at this time (may be done at later date, depending on Client and applicable third party vendor or OEM needs)
- SNECS will also configure the Antivirus policy on each Security Firewall
- SNECS techs will login to each computer and perform the following:
    - Remove any installed old/expired anti-virus
    - Remove any installed old/unauthorized remote access software
    - Install SNECS's new anti-virus/anti-malware software
    - Install SNECS's remote access support software
    - Install SNECS's 24x7 management software
    - Document each user associated with each computer and label systems accordingly
    - Document additional Client information provided related to IT needs, including but not limited to vendors, emergency contacts, security protocol, and business practices.

Additional Projects and Installations ('Default' Projects Scope):

- SNECS will provide the Client with a quote for Projects requested to meet Client's needs.
- Once we receive a 50% deposit on the Project quote from the Client, SNECS will proceed to order hardware and/or software (the "**Parts**") required for the Project.
- Once all Parts are received, we will begin configuration and perform tests to ensure the stability of all Parts. This testing phase can take up to 72 hours.
- Depending on the Project, we may request the following from the Client:
    - User Names and Passwords
    - Software list and licensing
    - Hardware requirements and/or documentation
    - Vendors, support agreements, and contact information for software/hardware relating to Projects scope
    - Third Party contact information if working with an external contractor (such as electrician, building manager, alarm company, etc.) for the Project
- If a Project includes a Server in the quote, the Project may include setting up the following:
    - Domain
    - Active Directory
    - Mapped Network Drives
    - User Permissions (based on Client's request)
    - Password Policies (based on Client's request)
    - Server-Dependent Software and Hardware (based on Client's request)
    - Configuring existing workstations to be converted to the new domain.
    - Performing user profile migrations to the new domain users.
    - Performing an onsite "data sync" to an external hard drive and transferring data to the new Server as needed. We will perform another "data sync" the day of install to ensure the new Server has the most up-to-date files.
- Project Estimated Timeframes are as follows (timeframes are rough estimates only):
    - Week 1 – Deposit and Ordering Parts
    - Week 2 – Assembly, Configuration, and Testing Parts
    - Week 3 – Preliminary Setup and Documentation
    - Week 4 – Scheduling and Installation

Term; Termination

The Services will commence on the date indicated in the Quote ("Commencement Date").

The Services will continue for an initial term of three (3) years from the Commencement Date. After the expiration of the initial term, the applicable Order will automatically renew for contiguous one (1) year terms unless either party notifies the other of its intention to not renew the Order no earlier than one-hundred and eighty (180) days and no less than thirty (30) days before the end of the then-current term.

Projects (if any) will commence on the date indicated in the applicable Order ("Project Commencement Date"), provided, however, that a 50% deposit payment must be received by SNECS prior to the Project Commencement Date. We reserve the right to delay the Project Commencement Date until the applicable deposit has been received by SNECS. After the initial deposit payment of a Project is processed, the Client may not cancel the Project unless the Client notifies SNECS of its intention to not proceed with the Project, in which event Client will automatically forfeit any deposit paid for the cancelled Project.

Locations Covered by Services and Projects

The Services will be provided at all current and future business locations of the Client. The Projects will be provided to any business location of the Client that is covered by an Office Solutions plan.

Exclusive Vendor Requirement

Client agrees that all current and future business locations opened, acquired, or operated during the term of this Agreement shall be serviced exclusively by SNECS, LLC (d/b/a IT Support RI) under the terms of this Statement of Work and the Master Services Agreement.

This exclusivity applies to all IT services covered under the Selected Plan, including but not limited to network management, workstation support, server maintenance, cybersecurity, and backup solutions.

Client shall notify SNECS in writing at least thirty (30) days prior to the opening of any new location to allow for proper onboarding and service provisioning. Failure to comply with this clause may be considered a material breach of the Agreement, subject to termination and applicable remedies.

Assumptions / Minimum Requirements / Exclusions

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

- All servers and workstations with a Microsoft Windows operating system must be running a Microsoft currently supported operating system, and have all the latest Microsoft service packs and critical updates installed. Any operating systems past their Microsoft "End of Support" date will not be supported.
- All servers and workstations with a Macintosh operating system (MacOS) must be running the latest version of MacOS or a supported operating system (within the 4 latest released versions), and have all the latest MacOS service packs and critical updates installed. Any operating systems older than the 4th latest MacOS will not be supported.
- Any device that require support but is considered "End of Support" or end of life is subject to an "Out of Date" cost, billable monthly per device.
- All server and desktop software must be genuine, licensed and vendor-supported.
- All wireless data traffic in the environment must be securely encrypted.
- The environment must have a currently licensed, up-to-date and vendor-supported server-based antivirus solution protecting all servers, desktops, notebooks/laptops, and email.
- The environment must have a currently licensed, vendor-supported server-based backup solution that can be monitored, and send notifications on job failures and successes.

- The environment must have a currently licensed, vendor-supported hardware firewall between the internal network and the Internet.
- All VoIP hardware must be on a segregated network from all other IT networked devices. Segregated network is defined as a Separate Static IP address and Separate Route dedicate to VoIP services.
- The Client must have a dedicated land (copper) line for failover/fax services & an outside static IP address from main Internet Service Provider for VoIP services.
- Internet speeds must be at a minimum of 10MB Upload and Download for the location or 1MB Upload and Download per device on the System, whichever is greater, to ensure network stability and backup reliability.
- Client understands and accepts any cost associated with additional Static IPs and/or bringing ISP services up to minimum standards (or best available speeds within reasonable costs to the Client) to keep System in operation.

Exclusions. The following services are expressly excluded under this SOW, and if required to be performed, will be billed to Client at SNECS's then-current hourly rate:

- Onsite and Travel Time not specifically covered under your Selected Plan.
- 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 and/or equipment relocation not purchased from SNECS.
- Digital Video Recorders (DVRs) and/or surveillance cameras
- 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.
- Parts, equipment or software not covered by vendor/manufacturer warranty or support.
- The cost of any software, licensing, or software renewal or upgrade fees of any kind.
- The cost of any 3rd party vendor or manufacturer support or incident fees of any kind.
- The cost to bring Client's environment and/or System up to "Minimum Standards" or "Minimum Requirements" as defined by SNECS.
- Any services required that require SNECS to maintain and/or setup software and/or hardware not purchased through SNECS (e.g., email support & migration, printer support & setup, computer/device setup & install, etc.)
- Services, installations, and repairs made by altering or modifying the Environment, software and/or equipment by others than those authorized by SNECS. This includes the Client making deliberate and unauthorized changes that requires SNECS to remediate.
- Service of non-vendor supported applications and/or software packages, whether acquired from SNECS or any other source unless otherwise specified. This also includes all DOS-based software.
- System-wide Virus and Security remediations
- Employee Productivity Package licensing is limited to a specific device on the System. Licenses may not be moved between devices. One user may require multiple licenses depending on total of monitored devices.
- Services on Holidays (or Holiday observance) in which SNECS is closed for business. Services on these dates and times will be billed at Emergency Rates with a 4 hour minimum.
- All Projects are billable and are quoted and billed separately from recurring and/or managed Services.
- Training services of any kind.

Authorized Contact(s)

A party may designate one or more Authorized Contacts to the other party by providing the other party, in writing, with each contact's name and contact information. In addition to the foregoing, the parties agree that any person who routinely or consistently provides direction and guidance on a party's behalf under this SOW shall be an Authorized Contact for such party (an "Authorizing Party"), unless the party receiving the direction and guidance is notified, in writing, that the person is not authorized to act on behalf of the Authorizing Party.

Fees

The fees for the Services will be invoiced to Client, payable by the due date of invoice. The fees for the Projects will be invoiced to the Client, with a 50% deposit due on Commencement Date and the remaining balance payable by the due date of the invoice. Refer to the Quote for additional details.

The initial fees indicated in the Order ("Initial Fees") is the minimum monthly recurring revenue that you agree to pay during the term of the Quote. If during the term of a Quote the amount of managed hardware or software 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. Under no circumstances will the fees charged to you under an Order drop below the Initial Fees (or thereafter be revised downward) without our consent.

For any billable services, please reference our rates listed at https://www.itsupportri.com/terms-and-conditions/.

Service Levels

Automated monitoring services will be provided on a 24x7x365 basis; remediation and technical support will be provided only during our normal business hours. SNECS will respond to problems, errors or interruptions in the provision of the Services in a timeframe commensurate with the severity of the problem, taking into account Client's needs and technician availability. If a request for support is submitted outside of SNECS's normal business hours, the request will be placed in queue for the following business day. Emergency Support is available via an after-hours tech support telephone call by the Client. Client automatically accepts billable charges associated with service requests outside our Hours of Operation.

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

Additional Terms

General Services

Unless otherwise provided in this SOW, general services will be applied in accordance with the recommended practices of the managed services industry. Client understands and agrees that general services are not intended to be, and will not be, a warranty or guaranty of the functionality of any particular device, or a service plan for the repair or remediation of any particular managed hardware or software. Repair and/or device remediation services are not covered under SNECS's service plan, and shall be provided on an hourly basis to Client.

Monitoring Services; Alert Services

Unless otherwise indicated in this SOW, 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 SNECS;

however, Client is advised to establish and/or modify the policies that correspond to Client's specific monitoring and notification needs.

Anti-Virus; Anti-Malware

SNECS's anti-virus / anti-malware solution will generally protect the Client's system from becoming infected with new viruses and malware ("Viruses"); however, Viruses that exist on the Client's system 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.

You understand and agree that no security solution is one hundred percent effective, and any security paradigm may be circumvented and/or rendered ineffective by certain Viruses or malware, such as ransomware or rootkits, that were previously unknown to the manufacturers of the software solution, and/or which are purposely or intentionally downloaded or installed onto your System. You are strongly advised to refrain from downloading files that are sent by unknown users, and/or users or files whose origination cannot be verified. SNECS does not warrant or guarantee that all Viruses and malware will be capable of being removed, or that all forms of Viruses and malware will be timely detected or removed, or that any data corrupted or encrypted by Viruses or malware will be recoverable. Should the Client's network and/or System become infected with a type of trojan, worm, cryptographic, self-replicating, or any other type of malware/virus that brings the business to a critical security breach, we may require the business limit operations while remediation is performed. Client shall hold SNECS harmless for any and all losses resulting in related virus activity, including if business shutdown is required to completed remediation. Client will be responsible for all costs associated with remediation, including but not limited to hardware, software, services, and billable rates.

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

Declination of Backup / Recovery Service

If you did not select a Quick Restore Server, then you have declined SNECS's complete data backup and recovery service; accordingly, you understand and agree that SNECS may be incapable of recovering your data if your data is lost, corrupted, or damaged for any reason. Only if requested to do so by you, SNECS may attempt to recover lost, corrupted, or damaged data; however, SNECS does not warrant or guarantee that its efforts will be successful. Regardless of the outcome, SNECS's recovery services will be billed to you at SNECS's then-current hourly rates, including the costs associated with the use of any 3rd party recovery and/or deletion services.

Hosted Exchange / Email

Client is solely responsible for the security, confidentiality and integrity of all email, and the content of all email, received, transmitted or stored through the hosted email service ("Hosted Email").

Client shall not upload, post, transmit or distribute (or permit any of its 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 SNECS or the services of any third party, or (v) contains Viruses, trojan horses or any other malicious code or programs.

In addition, Client shall not use the Hosted Email for the purpose of sending unsolicited commercial electronic messages ("SPAM") in violation of any federal or state law.

SNECS 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 if SNECS believes, in its discretion, that Client's email account is being used in an improper or illegal manner. We recommend that Client enable Two-Factor Authentication (2FA) services on all email accounts, as well as any other sensitive logins (ex; payroll websites, financial institutions, etc…) to increase overall security for the business and System.

Client shall hold SNECS harmless for any and all losses resulting in (but not limited to); wire transfers, payroll changes, banking or financial account changes initiated by email or other digital transmission. It is understood that the Client has procedures in place within their company to verify these changes with the intended parties via in-person or vocal approval.

SPAM / Junk Mail Filtering

SNECS's service provides email scanning for incoming unsolicited commercial email. Using proprietary algorithms and other technologies, the service scans incoming email for designated keywords, attachments and known blacklisted sites, and filters the email accordingly. From time to time the service may filter email that is not SPAM or junk mail, or may block email from legitimate sources. Client is advised to periodically search the filtered email folder to ensure that relevant emails are not being filtered improperly, and will notify SNECS in the event that the SPAM filter settings require adjustment.

VoIP / Phone System

911 Dialing / Emergency Dialing – Limitations

The VoIP Service ("VoIP Service") does not support traditional 911 or E911 access to emergency services in all locations. The 911 dialing feature of the VoIP Service is not automatic; Client must take affirmative steps to register the address where the VoIP Service will be used in order to activate the 911 Dialing feature. Client understands that Client must inform any users of the VoIP Service of the non-availability of traditional 911 or E911.

When a VoIP calling device is registered in a particular location, it cannot be moved without re-registering the device in the new location. Client agrees that it will not move any VoIP calling device without SNECS's written consent. Client shall hold SNECS harmless for any and all claims or causes of action arising from or related to Client's inability to use traditional 911 or E911 services.

When an emergency call is made, one or more third parties use the address of Client's registered location to determine the nearest emergency response location, and then the call is forwarded to a general number at that location. When the emergency location receives Client's call, the operator will not have Client's address and may not have Client's phone number. Client understands and agrees that users of the VoIP System must provide their address and phone number in order to get help. Client hereby authorizes SNECS to disclose Client's name and address to third-party service providers, including, without limitation, call routers, call centers and public service answering points, for the purpose of dispatching emergency services personnel to Client's registered location.

Client understands and agrees that 911 dialing does not and will not function in the event of a power failure or disruption. Similarly, the hosted VoIP Services will not operate (i) during service outages or suspensions or terminations of service by

Client's broadband provider or ISP, or (ii) during periods of time in which Client's ISP or broadband provider blocks the ports over which the VoIP Services are provided. Client further understands and agrees that 911 Dialing will not function if Client changes its telephone number, or if Client adds or ports new telephone numbers to Client's account, unless and until Client successfully register its location of use for each changed, newly added or newly ported telephone number.

Patch Management

SNECS recommends keeping all managed equipment and software current with critical patches and updates ("Patches") as such Patches are released generally by the manufacturers of the applicable hardware or software. Patches and updates are developed by third party vendors and, on rare occasions, may make the System, or portions of the System, unstable, or cause the managed equipment or software to fail to operate properly even when the Patches are installed correctly. SNECS shall not be responsible for any downtime or losses arising from or related to the installation or use of any Patch, provided that the Patch was installed in accordance with manufacturer's instructions. SNECS reserves the right, but not the obligation, to refrain from installing a Patch if SNECS is aware of technical problems caused by a Patch, or believes that a Patch may render the System, or any portion of the System, unstable.

Data Deletion

Upon written request from you, we will cause all managed systems (laptops, workstations, and servers) and devices (smartphones, USB drives) storing personally identifiable or protected health information to be securely overwritten or wiped using an approved secure file deletion utility or third party company that maintains industry certifications such as ISO-27001, ISO-14001, ISO-9001. This service is outside the scope of a SOW, and you will be responsible for any charges associated with this service, including but not limited to additional 3rd party services to complete required service.

Data Retention

A document listing what Client considers to be "all critical data" and the location of that data (the "Critical Data Report") must be provided to SNECS at time of onboarding. Client shall be responsible for updating the Critical Data Report as necessary to reflect any changes to the type, scope, or location of the information described in the Critical Data Report. Please note, if changes to Client's critical data (or the location of that data) requires additional or unique backup schedules, then Client may be required to purchase additional hardware as needed to accommodate the changes and, further, Client acknowledges that additional monthly charges may apply. If Client does not submit or update its Critical Data Report, then SNECS will apply a "Default Policy" in line with the SNECS then-standard backup policy.

Quick Restore Server (QRS) Services

SNECS's Quick Restore Server ("QRS") solution uses industry-recognized products and software to help ensure the security and integrity of Client's data. However, Client understands and agrees that 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 SNECS nor its designated affiliates will be responsible for the outcome or results of such activities. Data recovery time will depend on the speed and reliability of Client's Internet connection.

QRS services require a reliable, always-connected Internet solution. Internet and telecommunications outages will prevent the QRS services from operating correctly. In addition, all computer hardware is prone to failure due to equipment malfunction, telecommunication-related issues, etc., for which SNECS shall be held harmless. Client is strongly advised to use data verification functionality (if available) to ensure the integrity of Client's stored data. Client is further advised to take all verification errors seriously, and agrees to contact SNECS immediately if verification errors are repetitive and/or cannot be remedied.

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. As such, Client understands and agrees

that any data sent to or stored by SNECS may become corrupted or lost due to communication or hardware-related failures. SNECS cannot and does not warrant that such data corruption or loss will be avoided, and Client agrees that SNECS shall be held harmless if such data corruption or loss occurs. **Client is strongly advised to keep a backup of all of stored data to mitigate against the unintentional loss of data.** Unless otherwise expressly stated in this SOW, QRS services do not permit archiving or retrieval of prior document or file versions; only the latest version of a stored document or file is recoverable.

Procurement

Equipment and software procured by SNECS 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, SNECS does not make any warranties or representations regarding the quality, integrity or usefulness of the Procured Equipment. Certain equipment or software, once purchased, may be 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.

SNECS is not a warranty service or repair center. SNECS will facilitate the return or warranty repair of Procured Equipment; however, Client understands and agrees that 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 SNECS shall be held harmless. Client will be responsible for all repairs and shipping costs associated with Procured Equipment.

Business Review; IT Strategic Planning

Suggestions and advice rendered to Client are provided in accordance with relevant industry practices, based on Client's specific needs. By suggesting a particular service or solution, SNECS is not endorsing any particular manufacturer or service provider. SNECS is not a warranty service or repair center, and does not warrant or guarantee the performance of any third party service or solution.

Virtual CTO or CIO Services

The advice and suggestions provided by the VCIO will be for Client's informational and/or educational purposes only. The VCIO will not hold an actual director or officer position with Client, and the VCIO will neither hold nor maintain any fiduciary realtionship or position with Client. Under no circumstances shall Client list or place the VCIO on Client's corporate records or accounts. At all times the VCIO will be an independent contractor of Client.

Diagnostic / Auditing Services

Any diagnostic or auditing services performed by SNECS may require SNECS to install a small amount of code and/or software ("Diagnostic Code") on one or more of the devices attached to the System. No personal information or personal data reviewed or copied by SNECS at any time during the testing process. No files will be erased, modified, opened, reviewed or copied at any time during the testing process. The Diagnostic Code will not install or create any disabling device, or any backdoor or hidden entryway into the System. The results of the diagnostic testing will be kept confidential by SNECS.

You grant SNECS permission to access the System for the purpose of conducting the diagnostic testing, and agree to hold SNECS harmless from and against any and all incidents or damages that may occur during or as a result of the testing process, regardless of the cause of such damages including but not limited to data loss due to events beyond SNECS's reasonable control, network or communication outages, and deficiencies or errors in any of hardware or equipment that may interrupt or terminate the diagnostic testing process. The testing process is for diagnostic purposes only. The process is not intended, and will not be used, to correct any problem or error in the System. SNECS does not warrant or represent that the testing process will result in any particular outcome, or that any particular issue, hardware or software configuration will be correctly detected or identified.

Sample Policies, Procedures.

From time to time, SNECS may provide Client with sample (*i.e.*, template) policies and procedures for use in connection with Client's business ("Sample Policies"). The Sample Policies are for Client's informational use only, and do not constitute or comprise legal or professional advice. The Sample Policies are not intended to be a substitute for the advice of competent counsel. Client should seek the advice of competent legal counsel prior to using the Sample Policies, in part or in whole, in any transaction. SNECS does not warrant or guaranty that the Sample Policies are complete, accurate, or suitable for Client's specific needs, or that Client will reduce or avoid liability by utilizing the Sample Policies in its business operations.

Penetration Testing; Vulnerability Assessment

Client understands and agrees that security devices, alarms or other security measures, both physical and virtual, may be tripped or activated during the penetration testing process, despite SNECS's efforts to avoid such occurrences. Client shall be 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 shall 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 Client's System, causing substantial downtime and/or delay to Client's business activities. SNECS shall not be responsible for, and shall be held harmless and indemnified by Client against, any claims, costs, fees or expenses incurred by Client that arise or result 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 Client's System by any alarm or security monitoring device.

IaaS

Client shall use all SNECS-hosted equipment and hardware (collectively, "Infrastructure") for Client's internal business purposes only. Client shall not sublease, sublicense, rent or otherwise make the Infrastructure available to any third party without SNECS's prior written consent. Client agrees to refrain from using the Infrastructure in a manner that unreasonably or materially interferes with SNECS's other hosted equipment or hardware, or in a manner that disrupts or which is likely to disrupt the services that SNECS provides to its other clientele. Notwithstanding any provision to the contrary, SNECS reserves the right to throttle or suspend Client's access and/or use of the Infrastructure if SNECS believes, in its sole but reasonable judgment, that Client's use of the Infrastructure is violating, or is likely to violate, the foregoing terms or any other provision on the Agreement.

Data Replication

If Client purchases any services that involve data replication at a geographically diverse site, then the following applies to Client's use of that service: The rate by which the data at the primary site can be transferred to the secondary site will vary depending on the amount and type of data, constraints inherent in Client Hosted System, and fluctuations in bandwidth availability. Therefore, at any given time, the secondary site may not be completely up to date. In the event of a failover to the secondary site, the data that has not yet completed the transfer from the primary site will be lost. SNECS may provide Client with some guidelines on latency times based on its understanding of Client's data and system constraints, but these guidelines are not guaranties.

Domain Name Services

If Client registers, renews or transfers a domain name through SNECS, SNECS will submit the request to its domain name services provider (the "Registrar") on Client's behalf. SNECS's sole responsibility is to submit the request to the Registrar. SNECS is not responsible for any errors, omissions or failures of the Registrar. Client is responsible for timely making all registration and renewal payments to the applicable Registrar directly. Client's use of domain name services is subject to the applicable legal terms of the Registrar. Client is responsible for closing any account with any prior reseller of or registrar for the requested domain name, and Client is responsible for responding to any inquiries sent to Client by the Registrar.

Unsupported Configuration Elements Or Services

If Client requests a configuration element (hardware or software) or hosting service in a manner that is not customary at SNECS, or that is in "end of life" or "end of support" status, SNECS may designate the element or service as "unsupported," "non-standard," "best efforts," "reasonable endeavor," "one-off," "EOL," "end of support," or with like term in the service description (an "Unsupported Service"). SNECS makes no representation or warranty whatsoever regarding any Unsupported Service, and Client agrees that SNECS will not be liable to Client for any loss or damage arising from the provision of an Unsupported Service. Deployment and service level guaranties shall not apply to any Unsupported Service.

IP Addresses

Any IP addresses provided to Client by SNECS during the term of the Agreement are managed by SNECS and SNECS will retain these IP addresses after termination of the agreement, meaning that they may not be transferred or utilized by Client after termination of the Agreement.

Hosting Services

Client agrees that it is responsible for the actions and behaviors of its users of the Services. In addition, Client agrees that neither it, nor any of its employees or designated representatives, will use the Services in a manner that violates the laws, regulations, ordinances or other such requirements of any jurisdiction. Client warrants and represents that all hosted applications will be properly licensed, and that all such licenses shall be maintained by Client throughout the entire term of this SOW.

In addition, Client agrees that neither it, nor any of its employees or designated representatives, will: transmit any unsolicited commercial or bulk email, will not engage in any activity known or considered to be "spamming" and carry out any "denial of service" attacks on any other website or Internet service; infringe on any copyright, trademark, patent, trade secret, or other proprietary rights of any third party; collect, attempt to collect, publicize, or otherwise disclose personally identifiable information of any person or entity without their express consent (which may be through the person or entity's registration and/or subscription to Client's services, in which case Client must provide a privacy policy which discloses any and all uses of information that you collect) or as otherwise required by law; or, undertake any action which is harmful or potentially harmful to SNECS or its infrastructure.

Client is solely responsible for ensuring that its login information is utilized only by Client and Client's authorized users and agents. Client's responsibility includes ensuring the secrecy and strength of user identifications and passwords. SNECS shall have no liability resulting from the unauthorized use of Client's login information. If login information is lost, stolen, or used by unauthorized parties or if Client believes that any hosted applications or hosted data has been accessed by unauthorized parties, it is Client's responsibility to notify SNECS immediately to request the login information be reset or unauthorized access otherwise be prevented. SNECS will use commercially reasonable efforts to implement such requests as soon as practicable after receipt of notice.

SPLA Licensing

As part of the Services, SNECS will acquire certain licenses from Microsoft under a services provider license agreement ("SPLA"). The SPLA incorporates the terms and conditions of another Microsoft document, called the Service Provider Use Rights (or "SPUR"). SNECS's licensing of Microsoft software, and Client's use of such software, must always comply with the terms of the SPLA and SPUR. In the event that Microsoft modifies the terms of the SPLA or the SPUR, SNECS may be required, and will be permitted without prior notice to you, to modify the Services to comply with the modified terms of the SPLA or SPUR, as applicable.