solutions IT

Effective October 17, 2023. These Service Descriptions supersede and replace all prior versions.

Schedule of Services

The Total Solution

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a new Order including those Services.

The Total Solution includes: - Technical Standards / Alignment Process - Business Alignment / vCIO - Managed Services (User / Device Security, Device Mgmt.) - Service Desk

Service Description: A managed IT technical support service that provides Services to Client on a per user basis. Services include:

- Technology Alignment is facilitated through periodic reviews of client’s IT environment for conformance with SolutionsIT’s evolving library of Technical Standards and best practices. Some misalignments may require additional capital investment or professional service expense by Client.

- Business Alignment is facilitated through periodic meetings between Client and SolutionsIT. Client will help SolutionsIT understand its future business plans and SolutionsIT will consult on how to align Client's technology environment to pursue those plans.

- Centralized Technology Management includes the software applications, tools and processes utilized and provided by SolutionsIT to manage and maintain the Client's company-owned workstations, servers, and network devices. The combination of these tools and processes are proprietary to SolutionsIT and are subject to change at any time. They can be broadly categorized into availability monitoring; user security (SPAM filtering, and alert management); device security (anti-virus, thread detection, URL filtering); and device management (patching, remote access).

- The Service Desk provides Client with an "Unlimited Support" help desk for licensed end users. Support is limited to "Routine Support Tasks" during Regular Business Hours.

- VCIO Steering Meetings are periodic meetings following Technology Alignment to report findings and make recommendations.

- One-time Tasks:

  - Installation and configuration of SolutionsIT’s Centralized Managed Services tool stack. Customer Requirements:

  - Client agrees to comply with SolutionsIT Technical Standards and adopt SolutionsIT recommendations for IT Security and hardware refresh within a reasonable timeframe. For purposes of this service, a reasonable timeframe is defined as 12 months.

o Unlimited Support is limited to devices running SolutionsIT monitoring agent. Devices must meet the Minimum Standards Required for Services.

o Line of Business Software is defined as the specific applications that Client uses in the normal operation of their business that are in addition to the applications SolutionsIT provides. To be eligible for support under The Total Solution, Client must maintain an ongoing support and maintenance agreement with the software vendor that would allow SolutionsIT to open support tickets with the software vendor on Client's behalf.

o Client agrees to assign one employee to be the primary contact person to SolutionsIT to handle basic onsite tasks including: 1) training users when and how to contact SolutionsIT for technical support, 2) onsite helping hands to assist with troubleshooting, and 3) other miscellaneous functions related to helping you improve your efficiency concerning computer systems. This role is not expected to consume more than an average of a few minutes each day.

• Assumptions and Exceptions:

o ◦ When (in SolutionsIT sole discretion) Remote Support is not sufficient to resolve the issue, SolutionsIT will also provide Onsite Support at your primary business addresses (excluding residences) for devices running our management agent.

o ◦ The Total Solution support outside of Regular Business Hours or at a location other than your primary business address will be billed to you based upon SolutionsIT prevailing time and material rates.

o ◦ Routine support includes items such as: helping users connect to network resources; answering basic "how to" questions for common Microsoft Windows applications; helping users connect their peripherals devices such as keyboards, mice, printers, scanners and cameras (additional software, drivers or devices may be needed); and resolving application performance issues. SolutionsIT reserves the right to restrict the scope of Unlimited Support as needed to prevent abuse.

o ◦ Unlimited Support does not include end user support for questions related to the use of your specific Line of Business Software.

o ◦ Unlimited Support does not include Projects. Projects are defined as new equipment provisioning and setup as well as support tasks taking more than 5 hours to accomplish.

o ◦ Users are defined as specifically named employees of Client. Each user utilizing the Service within the billing period requires a User License.

o ◦ The security services provided with The Total Solution are not a guarantee against a security event.

The Total Solution – Co-Managed

CoManaged IT Support Plan (per user) includes:

- Technical Standards / Alignment Process

- Business Alignment / vCIO

- Managed Services (User / Device Security, Device Mgmt.)

Service Description: A Co-managed IT technical support service that provides Services to Client on a per user basis. Services include:

• Technology alignment is facilitated through periodic reviews of client's IT environment for conformance with SolutionsIT's evolving library of Technical Standards and best practices. Misalignments are addressed by either 1) SolutionsIT self-initiating minor adjustments or 2) SolutionsIT requesting approval from Client. Some misalignments may require additional capital investment or professional service expense by Client.

• Business alignment is facilitated through periodic meetings between Client and SolutionsIT. Client will help SolutionsIT understand its future business plans and SolutionsIT will consult on how to align Client's technology environment to pursue those plans.

• Centralized managed services include the software applications, tools and processes utilized and provided by SolutionsIT to manage and maintain the Client's company-owned workstations, servers, and network devices. The combination of these tools and processes are proprietary to SolutionsIT and are subject to change at any time. They can be broadly categorized into availability monitoring; user security (SPAM filtering, and alert management); device security (anti-virus,thread detection, URL filtering); and device management (patching, remote access).

• One-time Tasks:

o Installation and configuration of SolutionsIT Centralized Managed Services tool stack.

• Customer Requirements:

o Client agrees to comply with SolutionsIT Technical Standards and adopt SolutionsIT recommendations for IT Security and hardware refresh within a reasonable timeframe. For purposes of this service, a reasonable timeframe is defined as 12 months.

o Client agrees to assign one employee to be the primary contact person to SolutionsIT to handle basic onsite tasks including: 1) training users when and how to contact SolutionsIT for technical support, 2) onsite helping hands to assist with troubleshooting, and 3) other miscellaneous functions related to helping you improve your efficiency concerning computer systems. This role is not expected to consume more than an average of a few minutes each day.

- Assumptions and Exceptions:

  o Support outside of Regular Business Hours or at a location other than your primary business address will be billed to you based upon SolutionsIT prevailing time and material rates.

  o Users are defined as specifically named employees of Client. Each user utilizing the Service within the billing period requires a User License.

  o Co-managed support means that the Client retains responsibility for day-to-day end user support. Should SolutionsIT Centralized Managed Services detect a hardware, security or other performance issue, SolutionsIT will alert Client so that Client can decide upon the appropriate remedial action. Labor for other support requests, as well as the time to mitigate any alerts, virus infections or any other situation is provided on a time and material basis at SolutionsIT then current rates.

  o SolutionsIT is not engaged in supporting end users beyond the limits of maintaining the resources utilized in the delivery of Centralized Services and Technical Alignment. Any additional services or support will be provided on a time and material basis at SolutionsIT then current rate.

ENSO Statement of Service

The Essential Network Service Offering can be characterized as a partial managed service. You maintain full ownership and responsibility of your network while SolutionsIT provides daily hygiene tasks that reduce the frequency of reactive tickets while enhancing security. ENSO is positioned as an intermediate service by SolutionsIT that satisfies the needs of small businesses that are more budget-conscious compared to fully managed services. It is designed using industry best practices and cyber security thresholds, to provide the essential elements necessary to protect your business. The framework of the service includes the following elements:

- Capturing the critical information of the network during the onboarding process and securing this documentation in a repository. This repository is critical to the success of efficient remote service. It also builds in an element of continuity as critical network information is stored outside of your organization.
- Deployment of Cyber Security Suite of Professional Tools. Examples may include:
  - Monitoring; can detect security and performance issues like brute-force attacks, keylogging, outdated OS and various thresholds like CPU usage, hard drive space limitations, etc. It is not uncommon for alerts to appear and be addressed on a daily basis. Our HelpDesk technicians review these issues daily. You are also receiving alerts as they are generated 24/7 and you can ask to have issues addressed as you see fit.
  - Patch Management addresses outdated performance and security patches developed by Microsoft for your operating system. This scheduled task enhances server and

    workstation operation. It is your responsibility to ensure reboots have been performed on all workstations in order for the patches to be fully updated.
    - The anti-virus product will be updated regularly as the manufacturer releases updates.
    - Other optional tools, depending on complexity and compliance requirements.
- Direct access to our HelpDesk remote service team.
- Dispatch onsite technicians as requested/required.
- An assigned Account Manager for professional consultation, continuity and advice.
- Flexibility as to how you allocate your block-time technical hours.
- Reports, alerts and documents to evaluate the health of your network.
- Ticketing system to provide clarity of progress of services provided.
- Quotes on network hardware and installation services.
- An introduction to preventative service via multi-point inspection (STA, optional):
    - The frequency of this service is solely at your discretion.
    - This service will be scheduled by our Customer Care team in advance.
    - This onsite inspection will uncover performance and security issues that would otherwise be undetectable with remote service.

At times, outside parties may require certain measures to be implemented for compliance to continue to use or provide a service or product. In these cases, SolutionsIT can assist you with direction and/or configuration to ensure your business can continue to operate within these parameters (i.e. PIPEDA).

ENSO is positioned to be an enhancement compared to call and dispatch level of service. Service ticket frequency is dependent upon your network's design, age, and inherited maintenance. Your Account Manager will often advise on the design of your network but ultimately it is your choice as to what is and is not implemented.

BASE Statement of Service

The Basic Active Service Experience can be characterized as a partial managed service. You maintain full ownership and responsibility of your network while SolutionsIT provides daily hygiene tasks that reduce the frequency of reactive tickets while enhancing security. BASE is positioned as an intermediate service by SolutionsIT that satisfies the needs of small businesses that are more budget-conscious compared to fully managed services. It is designed using industry best practices and cyber security thresholds, to provide the essential elements necessary to protect your business. The framework of the service includes the following elements:

- Capturing the critical information of the network during the onboarding process and securing this documentation in a repository. This repository is critical to the success of efficient remote service. It also builds in an element of continuity as critical network information is stored outside of your organization.
- Deployment of Cyber Security Suite of Professional Tools. Examples may include:
    - Monitoring; can detect security and performance issues like brute-force attacks, keylogging, outdated OS and various thresholds like CPU usage, hard drive space limitations, etc. It is not uncommon for alerts to appear and be addressed on a daily basis. Our HelpDesk technicians review these issues daily. You are also receiving alerts as they are generated 24/7 and you can ask to have issues addressed as you see fit.

    - Patch Management addresses outdated performance and security patches developed by Microsoft for your operating system. This scheduled task enhances server and workstation operation. It is your responsibility to ensure reboots have been performed on all workstations in order for the patches to be fully updated.
    - The anti-virus product will be updated regularly as the manufacturer releases updates.
    - Other optional tools, depending on complexity and compliance requirements.
- Direct access to our HelpDesk remote service team.
- Dispatch onsite technicians as requested/required.
- An assigned Account Manager for professional consultation, continuity and advice.
- Flexibility as to how you allocate your block-time technical hours.
- Reports, alerts and documents to evaluate the health of your network.
- Ticketing system to provide clarity of progress of services provided.
- Quotes on network hardware and installation services.

At times, outside parties may require certain measures to be implemented for compliance to continue to use or provide a service or product. In these cases, SolutionsIT can assist you with direction and/or configuration to ensure your business can continue to operate within these parameters (i.e. PIPEDA).

BASE is positioned to be an enhancement compared to call and dispatch level of service. Service ticket frequency is dependent upon your network's design, age, and inherited maintenance. Your Account Manager will often advise on the design of your network but ultimately it is your choice as to what is and is not implemented.

MANAGED SECURITY SERVICES

Provider, through its Third-Party Services Providers will make its best effort to ensure the security of Client's information through third-party security software ("Security Software"). Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this Service is subject to the applicable Third-party Service Providers agreements regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client acknowledges that Third-Party Service Providers and their licensors own all intellectual property rights in and to the Security Software. Client will not engage in or authorize any activity that is inconsistent with such ownership. Client acknowledges and agrees to be bound by any applicable Third-Party Service Provider agreements regarding terms or use or end user licensing terms, and Client understands that any applicable agreement regarding terms of use or end user licensing is subject to change without notice.

Network Discovery - generates a visual map of all nodes on your network, making it easy to see where you may be at risk.

Password Management – Provider will provide the application for end users to securely store, maintain and share application passwords.

Spam Prevention - Real-time, continuous, and highly reliable protection from spam and phishing attempts.

Application Control – Provides the ability to allow, block, or restrict access to applications based on a user's department, job function, and time of day.

Data Loss Prevention – works to enforce compliance by scanning text and files to detect sensitive information attempting to exit your network, whether it is transferred via email, web, or FTP.

DNS Filtering - detects and blocks malicious DNS requests, redirecting users to a safe page with information to reinforce security best practices.

Anti-malware - Provider will provide and install anti-malware software of Provider's choosing for each Device covered by the Order. While Provider will make reasonable effort to ensure Client Devices and Client's network are safe from viruses, malware, bugs, hacking, phishing schemes or defective or malicious files, programs or links ("Harmful Content"), of any kind whether now known or hereinafter invented, Provider does not guarantee that Client computers or network cannot be infected by Harmful Content. Where this does happen, Provider will provide commercially reasonable Services to mitigate the Harmful Content. Additional Services will be available upon mutual agreement of the parties.

Security Awareness Training & Phishing Simulations - Provider will acquire and will assign an appropriate number of licenses to support the client environment. The Service will schedule phishing campaigns to send at random times during a specified period. The campaigns are trackable and fully customizable designed to keep track of every user's participation, making all cybersecurity education accountable and measurable.

Multi-Factor Authentication Services / Password Credential Management Services – Provider will configure two-factor authentication for compatible software applications, institute single sign-on services for compatible software applications and customized security policies and procedures. After performing a security assessment and assessing the state of Client's existing policies and procedures pertaining to network security (if any), Provider will work with Client to prepare a new or revised set of policies and procedures that incorporate cutting edge best practices and that take advantage of the other Services delivered by Provider.

Managed Detection and Response (MDR) – The Services include:

- Advanced Malware Protection supported by Security Operations Center (SOC).
- Deployment of advanced malware protection applications to all Windows based devices on customer network.
- 24x7 SOC service analyzes quarantined applications and files, reducing false positives.
- Immediate risk identification – Provides rapid recognition of thousands of viruses and malware attack variants, including cryptomining attacks, as well as the root causes of these malicious behaviors, by quickly identifying and diagnosing corrupt source processes and system settings.
- Ransomware rollback - quickly rollback files to previous safe versions through tracking changes in your devices and restoring them to an acceptable risk state.

Security Log Management – Provider will configure log sources to capture and retain information without creating excessive logging, limit user access to log files, avoid logging sensitive or protected information, secure the processes that generate logs, identify and resolve logging errors, and analyze log entries, prioritize entries, and respond to those requiring action.

Security Incident Event Management (SIEM) Services supported by SOC – Provider will deploy SIEM monitoring probes to monitor all critical network devices including; domain controller, firewalls, network switches and routers. When meeting compliance requirement deployment will include all Windows devices as well.

Incident Response - Provider will assist Client in the hours immediately following a data breach to identify the likely source of the breach and to begin formulating an appropriate response to the breach. However, any assistance with data breach-remediation efforts past the first twenty-four (24) hours following a breach – including but not limited to breach-notification planning, in-depth forensic examinations of the source of a breach, and significant, post-breach systems reconfiguration – are not within the scope of this Service Attachment. If Client requests Provider's assistance with such activities, Provider will prepare a separate Service Attachment for Project Services that will specify what the charges will be for such assistance.

DATA BACKUP SERVICE

The Services to be performed for Client by Provider are set forth in the Order. Additional Services may be added only by entering into a separate Order including those Services.

Local Backups - Using customer provider hardware and software (backup software), backups will be performed on the basis specified in the Order. Client owns the hardware and software agents (backup software) used to perform the backups. If Client subscribes to periodic Server Maintenance, Provider will review the backups during Maintenance and notify Client of backup failures. Client will notify the Provider of any failures, and upon request, perform simple on-site tasks (e.g., powering down and rebooting hardware).

Remote Backups - Provider, through its Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. Data files are backed up via a third-party client-side desktop/server software application (the "Application"), encrypted, and then sent to a storage server at third-party vendor's data center facility. There is no local copy of the backed-up data. Data files can be restored from the cloud but the server itself cannot be recovered or "booted" in the cloud. Therefore, this service is not considered a disaster recovery solution. All data is backed up via a third-party client-side desktop/server software application (the "Application"). Provider will monitor the backups daily, notify Client of any failures, and work with third-party to resolve backup failures.

Cloud Backup - Provider, through its Third-Party Service Providers will make its best effort to ensure the protection and recovery of Client's information. Data is backed up via a third-party client-side desktop/server application, encrypted, stored locally on a Provider-owned storage device ("Provider Owned Storage"), and then sent to a third-party owned storage server at the Third-Party Services Provider's data center facility. Provider will monitor the status of all scheduled backup jobs, notify Client of Provider-owned storage failures and corrective actions. Provider will also provide remote administrative services of Data Backup Service as requested by Client. Offsite Backup copies will have one-year retention unless specified in Order. Upon termination of these Services, Provider will request return of the backup hardware and remove the Application from Client systems.

CLOUD AND HOSTING SERVICES

Public Cloud - Provider will move all Client’s data to a cloud computing platform, allow Client to have access to data via virtual desktop from Client’s own devices or device provided by Provider, and manage the cloud environment for Client.

Hybrid Cloud - Provider will move some of Client’s data to a cloud computing platform, and upon Client’s request, place a server on premises at Client’s location. Any Client data being moved shall be agreed to by the parties in writing prior to moving with specific instructions as to identify which data will be moved, managed or unmanaged by Provider. Any Client data being moved or managed shall be specifically identified as to the location of the data on a particular server. Any Client data not being moved, or that is not specifically identified by Client will be considered not managed. Provider shall not be responsible for the identification, classification, or location of the data. Client is solely responsible for its data up to the outermost point of Provider’s firewall with the public internet (the “Demarcation Point”). Once data has been identified, classified, its final location determined, and moved past the Demarcation Point, Provider shall then become responsible for Client data. Provider will also manage the cloud environment for client and provide hardware that will be owned by Provider and will be licensed using an appropriate license agreement.

Private Cloud or Software Subscriptions - Provider will maintain all Client’s data on premise at Client’s location, manage the cloud environment and software subscriptions for Client, provide unmanaged cloud environment and software subscriptions for Client, and provide hardware that will be owned by Provider and will be licensed using an appropriate license agreement.

Third-Party Cloud & SaaS Vendors - Provider will provide, install, and support the Third-Party Cloud or software-as-a-service vendors listed on the Order, including but not limited to Microsoft. Client designates Provider as its agent to provide the Service to Client, and to enter into any third-party relationship to provide the Service to Client. Use of this software is subject to the applicable third-party cloud or software-as-a-service vendor’s agreement regarding terms of use, which Client and Provider agree has been provided by Provider to Client. Client agrees to be bound by any applicable third-party cloud or software-as-a-service vendor’s agreements regarding terms or use or end user licensing, and Client understands that any applicable agreement regarding terms of user or end user licensing is subject to change by any Third-Party vendor or software-as-a-service provider without notice.

CYBER TRAINING SERVICES

Provider will implement and managed a managed cybersecurity awareness training platform ordered through a third party on Client’s behalf. The program features:

- Enrolling all technology-facing workforce members in the program
- Access to a curriculum of industry-leading cybersecurity awareness education which can be customized to meet the unique needs and regulatory requirements of Client
- Management reporting and visibility into workforce participation and progress in the training
- Regular campaigns to test each workforce member’s ability to recognize and effectively respond to cyberattacks which typically target individuals

- Automated enrollment in remedial training for individual workforce members, when appropriate
- Management reporting and visibility into workforce performance on testing campaigns
- Management reporting and visibility into the improvement in workforce awareness and performance over time
- Lowered risk to (Client) from cyberattacks which target unaware and untrained individuals

Voice Services

Provider will provide Voice access

- □ No charge for labor on all set moves and changes (excluding wiring)*
- □ No charge for service labor within the scope of this agreement
- □ No charge repair/replacement on all defective parts per SYSTEM DETAILS above
- □ No charge for implementing Annual software update
- □ No charge for no fault found calls
- □ No charge telephone support during business hours
- □ No charge remote programming changes as required
- □ Line contract/VoIP cost audits – recommendations upon request
- □ Initial backups of original system settings

*”*moves” denotes moving existing phone sets to different locations within the existing premises*

EXEMPTIONS

- □ Acts of Nature such as fire, flooding and lightning strikes are not covered
- □ Malicious, intentional, or accidental damage is not covered
- □ Installation of equipment not purchased from SolutionsIT is not covered
- □ System moves are excluded from our no charge labor
- □ Cabling jobs are excluded from our no charge labor
- □ Any equipment or licensing required to support any software upgrades are billable

Hosting Services

Domain Name Registration – Provider provide domain name registrations at the request of customers

Website Hosting – Provider will provide DNS hosting as well as server space and bandwidth.

THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY TIME WITHOUT NOTICE.