Effective March 25, 2023. This Description of Services supersedes and replaces all prior versions.

Description of Services

MANAGED IT SERVICES

To the extent ordered by Client, Provider will perform for Client the IT Infrastructure Monitoring and Management Services included below.

24X7 NOC Monitoring & Management:

- Included items:
  - 24X7 alert monitoring & management of servers/desktop/laptops provided by our Network Operations Center
  - Quarterly reporting and performance tuning
  - Prioritization of alerts to identify high priority incidents.
  - Microsoft Patch Management, Failure Resolution and Rollbacks.
  - 3rd Party Applications Patch Management as specified in sales order.
  - Remote Monitoring and Management Agent
  - Antivirus Software Management
  - Removal of viruses, malware, and spyware.
  - Backup software monitoring and management.
  - Recovery of data via backup software as required.
  - Onsite remediation services as needed (Servers Only)
- Excluded items:
  - Major hardware / software upgrades or replacements
  - Hardware and/or Software warranties or licenses, unless specified in order.
  - New equipment installations.

24X7 Firewall/ISP Monitoring & Management:

- Included items:
  - 24X7 alert monitoring & management of managed devices
  - Prioritization of alerts to identify high priority incidents.
  - Escalation to carrier or designated customer contact if carrier services appear to be offline.
  - Remote & Onsite remediation services as needed
  - Quarterly configuration backups
  - Quarterly firmware updates as required by manufacture
  - Quarterly updates and performance tuning
- Excluded items:
  - Hardware replacement
  -
  - Hardware and/or Software warranties or licenses, unless specified in order.
  - New equipment installations.

Help Desk Services:

- Included items:
  - During normal business hours unless otherwise specified on order, Help Desk support via email, phone & chat on Microsoft applications or other 3rd Party applications, software and input/output devices specified in sales order, unless explicitly excluded in contract.
  - Unless otherwise included in an order, all help desk services will include unlimited remote support as required.
  - Remote software installations on covered devices and software.
  - Active Directory/Group Policy Management and support.
  - Password resets on supported applications
  - New / terminated employee setup and configuration. Does not include new devices or image reloads.
- Excluded items:
  - Major hardware / software upgrades or replacements to include image reloads for new/terminated employees unless specified on order.
  - Onsite/Deskside Support, unless specified in order.
  - New equipment installations.

MANAGED SECURITY SERVICES

To the extent ordered by Client, Provider will deliver to Client the Managed Security Services ("Service") listed below. Unless otherwise indicated in the Order, Provider will deliver the Services on an ongoing basis.

- 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.

The Service includes the following:

Firewall and Intrusion Detection

- Installation and configuration of firewall traffic policies.
- Apply updated firmware when applicable.
- Configuration changes when needed.
- Software services included on firewall:
    - Intrusion Prevention - provides real-time protection against network threats, including spyware, SQL injections, cross-site scripting, and buffer overflows.
    - URL Filtering - blocks known malicious sites, and delivers granular content and URL filtering tools to block inappropriate content.
    - Gateway Antivirus - continuously updated signatures, identify and block known spyware, viruses, trojans, worms, rogueware and blended threats – including new variants of known viruses.
- Reputation-Based Threat Prevention - Cloud-based web reputation service that aggregates data from multiple feeds to provide real-time protection from malicious sites and botnets, while dramatically improving web processing overhead.
- 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.
- Threat Detection & Response - Security data collected from the firewall is correlated by enterprise-grade threat intelligence to detect, prioritize and enable immediate action against malware attack.
- SonicOS Capture ATP Sandboxing and Deep Packet Inspection
- DNS Filtering - detects and blocks malicious DNS requests, redirecting users to a safe page with information to reinforce security best practices.
- Cloud Management and Reporting

Managed Endpoint Protection

- Advanced Next Generation AI End Point Protection MDR (managed detection and response) Solution supported by a third-party Security Operations Center (SOC).
- Deployment of advanced malware protection, threat hunting and SEIM technology 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.

Office 365 Email Security

- Protect - Tier One
    - Advanced API deployed AI-enabled Anti-spam, Anti-phishing email security solution includes known malware prevention, unauthorized application detection, account takeover preventions and URL protection.
- Advanced Protect - Tier Two
    - Includes everything in Tier One plus zero-day malware prevention, attachment sanitations and threat extraction and additional SaaS app protection (Teams, One Drive and Google)
- Complete Protect - Tier Three
    - Includes everything in Tier One and Two plus advanced deployment of Azure Information Protection for data loss prevention and Encryption for M365.

Security Awareness Training & Phishing Simulations

Provider will acquire and will assign an appropriate number of licenses to support the client environment.

The Service includes the following:

- Darkweb monitoring.
- Scheduled phishing campaigns with associated training courses sent at random times during a specified period.
- Post-campaign reporting can be used for some Security Awareness Training compliance requirements.

Security Operations Center – 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.

Managed Voice Services

To the extent ordered by Client, Provider will perform for Client the Voice Infrastructure Management Services included below.

24X7 Support & Escalation Management:

- Included items:
  - 24X7 Emergency Support & management of servers/hosted instance provided by our Network Operations Center for system down emergencies.
  - 24x7 Response and Escalation support to carriers as needed
  - 24x7 Remote and Onsite Remediation services as needed
  - Prioritization of alerts to identify high priority incidents.
  - Monthly Patch Management and performance tuning.
  - Annual review of carrier services and system version update.

Remote Programing Services and Help Desk:

- Included items:
  - During normal business hours unless otherwise specified on order, Help Desk support via email, phone & chat on unified communications applications.
  - Remote software installations on covered devices and software.
  - Password resets on supported applications
  - New / terminated employee setup and configuration.
  - Programming changes for users, call groups, auto attendants and business hours performed remotely and during normal business hours.
  - Programing changes to resolve emergency operations needs and dial plans performed remotely and 24/7.
  - Unless otherwise included in an order, all help desk services will include unlimited remote support as required.

Excluded items:

- Major hardware / software upgrades or replacements.
- New equipment installations.

Requirements:

- Servers must be under manufacture warranty and software support.
- Operating System no older than one (1) generation behind current.
- Change control procedures must always be followed.

DATA BACKUP AND RECOVERY SERVICE

To the extent ordered by Client, Provider will perform the following services relate to backup and disaster recovery:

General Description

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.

Hardware and software

There is no additional hardware required.
All data is backed up via a third-party client-side desktop/server software application (the "Application")

Provider responsibility

Monitor the backups daily
Notify the Client of any failures
Work with third-party to resolve backup failures

Client responsibility

If requested, perform simple on-site tasks (e.g., powering down and rebooting hardware).

Summary of Back-up Types

Microsoft Stand-alone and Hyper-V VM Server Back-up

Includes full image (up to 2TB) back-up of all data stored in the cloud with Monthly Backup Recovery Testing. A test VM is spun up in a cloud environment provided by N-able, the backup is restored, and a screen shot is captured to verify successful recovery.

Window 10/11 Desktop/Laptop Back-up

Includes full image (up to 500GB) back-up of all data stored in the cloud.

Window 10/11 Document Back-up

Document Backup includes (up to 500GB) back-up of all documents listed in attachment. Does not include pictures and video files. Files are stored in the cloud.

CLOUD AND HOSTING SERVICES

To the extent ordered by Client, Provider will perform for Client the Cloud and Hosting Services included below.

Third-Party Cloud & SaaS Vendors
If Client's Order includes Third-Party Cloud or software-as-a-service, Provider will:

- 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.
- Provider will provide and install anti-malware software of Provider's choosing for each Device covered by this Attachment. 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.
- Provider will install remote access and remote monitoring and management software on Client's Devices possibly other equipment at Client's office. Client grants permission to Provider to install any remote access or remote monitoring and management software deemed necessary by Provider.