verified
technologies

Effective August 15, 2023. These Service Descriptions supersede and replace all prior versions.

Schedule of Services

MANAGED SERVICES

The Schedule of Services describes the Managed IT Services offered by Verified Technologies, a Florida corporation, (“Provider”). The Services to be performed for Client by Provider are set forth in the Order or Statement of Work. Only the Services itemized in the Order will be delivered. This Schedule of Services may be modified at Providers’ sole discretion.

Additional Services may be added only by entering into a new Order including those Services.

Managed Server Service Description

Managed Server is a foundation component of the Verified Technologies service offering. Verified Technologies provides total managed services aimed at alleviating the IT nightmares that bog you down. This service provides full maintenance of your Windows Server. This service consists of the following:

- Verified Technologies will install a management agent and anti-virus/anti-malware agent on each Server to be managed.
- Verified Technologies will provide 24x7 monitoring and alerting on critical events as defined in System Monitoring.
- In the event of an alert indicating Server offline or critical event failure, Verified Technologies will attempt to connect remotely and restart the service or resolve the incident.
- This service includes unlimited Remote Support for the Windows server operating system and Windows services, including SQL and Exchange.
- In the event a physical Server goes offline after-hours, a Verified Technologies engineer will be scheduled to perform onsite remediation the following morning.
- If onsite remediation is required, normal Reactive Support Service rates would apply and be billed accordingly.
- Third-party application support is not covered under this service. Verified Technologies will provide support for third-party applications at the normal Reactive Support Service rates.
- In the event of hardware failure covered under manufacturer warranty, Verified Technologies will contact the vendor on Client’s behalf and coordinate the replacement.
- Verified Technologies will perform patching as defined in Patch Management.
- Verified Technologies will include security tools as defined in Cyber Security Tool Stack.
- Verified Technologies will provide management reports as defined in Reporting.

Managed Desktop Service Description

Managed Server is a foundation component of the Verified Technologies service offering. Verified Technologies provides total managed services aimed at alleviating the IT nightmares that bog you down. This service provides full maintenance of your Windows Server. This service consists of the following:

- Verified Technologies will install a management agent and anti-virus/anti-malware agent on each Server to be managed.
- Verified Technologies will provide 24x7 monitoring and alerting on critical events as defined in System Monitoring.
- In the event of an alert indicating Server offline or critical event failure, Verified Technologies will attempt to connect remotely and restart the service or resolve the incident.
- This service includes unlimited Remote Support for the Windows server operating system and Windows services, including SQL and Exchange.
- In the event a physical Server goes offline after-hours, a Verified Technologies engineer will be scheduled to perform onsite remediation the following morning.
- If onsite remediation is required, normal Reactive Support Service rates would apply and be billed accordingly.
- Third-party application support is not covered under this service. Verified Technologies will provide support for third-party applications at the normal Reactive Support Service rates.
- In the event of hardware failure covered under manufacturer warranty, Verified Technologies will contact the vendor on Client’s behalf and coordinate the replacement.
- Verified Technologies will perform patching as defined in Patch Management.
- Verified Technologies will include security tools as defined in Cyber Security Tool Stack.
- Verified Technologies will provide management reports as defined in Reporting.

Managed Desktop - No-Helpdesk Service Description

Managed Desktop is a foundation component of the Verified Technologies service offering. This service provides full maintenance of your Windows Desktop without the cost of Help-Desk services. This is convenient for Client’s that have their own internal IT staff to handle day-to-day on-site IT requests but want improved overall security by having fully managed endpoints.

This service consists of the following:

- Verified Technologies will install a management agent and anti-virus/anti-malware agent on each Windows Desktop to be managed.
- Verified Technologies will provide 8x5 monitoring and alerting on critical events as defined in System Monitoring.
- Verified Technologies can provide access for Client’s IT staff to our service ticketing system in order to manage user-submitted service tickets.
- End users can call in to the Verified Technologies Service Desk at the normal Reactive Support Service rates, where a Verified Technologies support representative will provide remote support to the end user to resolve the incident.
- If onsite remediation is required, normal Reactive Support Service rates would apply and be billed accordingly.

- Third-party application support is not covered under this service. Verified Technologies will provide support for third-party applications at the normal Reactive Support Service rates.
- In the event of hardware failure covered under manufacturer warranty, Verified Technologies will contact the vendor on Client's behalf and coordinate the replacement.
- Verified Technologies will perform patching as defined in Patch Management.
- Verified Technologies will include security tools as defined in Cyber Security Tool Stack.
- Verified Technologies will provide management reports as defined in Reporting.

Managed Firewall Service Description

This service provides basic management of Client owned firewall appliances. This service consists of the following:

- Verified Technologies will provide 24x7 ICMP/ping monitoring to detect the up/down status of the firewall appliance and the ISP modem gateway.
- Verified Technologies will notify Client of upcoming service renewals for firewall service subscriptions.
- Verified Technologies will apply service renewals licenses to firewall upon Client purchase of subscription renewal.
- Verified Technologies will validate that latest firmware updates included in subscriptions are installed on firewall.
- Verified Technologies will make any required firewall configuration changes as needed.
- Verified Technologies will ensure that firewall rules are configured to meet best practices and maximize security.
- Verified Technologies will create and store configuration backups if device is capable.
- All firewall configuration changes will be performed remotely and will follow the Verified Technologies Change Control process.
- If onsite remediation is required, normal Reactive Support Service rates would apply and be billed accordingly.
- In the event of hardware failure covered under manufacturer warranty, Verified Technologies will contact the vendor on Client's behalf and coordinate the replacement.

Managed Firewall Hardware-as-a-Service Description

Managed Firewall Hardware-as-a-Service is a security component of the Verified Technologies service offering. This service provides firewall management and the physical hardware appliance. This service consists of the following:

- Verified Technologies will provide a firewall appliance to be installed at Client location.
- Verified Technologies will provide 24x7 ICMP/ping monitoring to detect the up/down status of the firewall appliance and the ISP modem gateway.
- Verified Technologies will make any required firewall configuration changes as needed.
- Verified Technologies will ensure that firewall rules are configured to meet best practices and maximize security.
- Verified Technologies will create backups and store firewall appliance configurations.
- All firewall configuration changes will be performed remotely.
- All firewall configuration changes will follow the Verified Technologies Change Control processes.
- In the event of hardware failure, Verified Technologies will provide and configure a replacement unit at no charge to the Client.

- In the event of hardware failure after-hours, a Verified Technologies engineer will be scheduled to perform onsite remediation the following morning.

Managed Wi-Fi - Hardware as a Service Description

This service includes device hardware and basic management of Verified Technologies owned wireless access point(s). This service consists of the following:

- Verified Technologies will provide wireless access point appliance installed at Client location.
- Verified Technologies will provide 24x7 monitoring to detect the status of the wireless appliance.
- Verified Technologies will validate that latest firmware updates are installed on appliance.
- Verified Technologies will make any required wireless configuration changes as needed.
- Verified Technologies will ensure that wireless configuration meets best practices and maximizes security.
- All wireless configuration changes will be performed remotely and will follow the Verified Technologies Change Control process.
- If onsite remediation is required, normal Reactive Support Service rates would apply and be billed accordingly.
- In the event of hardware failure covered under manufacturer warranty, Verified Technologies will contact the vendor and coordinate the replacement.

Managed VMware ESX Host Service Description

Managed VMware ESX Host ensures your virtual infrastructure is providing the solid foundation required to support your
virtual environment. This service consists of the following:

- Verified Technologies will configure a management agent on a physical server or guest server on the Client’s network to monitor VMware ESX Servers.
- Verified Technologies will provide 24x7 monitoring and alerting on CPU, memory utilization, disk space and other vital statistics.
- In the event of an alert indicating Server offline or critical event failure, Verified Technologies will attempt to connect remotely and restart the service or resolve the incident.
- In the event a physical Server goes offline after-hours, a Verified Technologies engineer will be scheduled to perform onsite remediation the following morning.
- If onsite remediation is required, normal Reactive Support Service rates would apply and be billed accordingly.
- In the event of hardware failure covered under manufacturer warranty, Verified Technologies will contact the vendor on Client’s behalf and coordinate the replacement.
- Verified Technologies will perform quarterly review of vSphere configuration to ensure current configuration is optimal.
- Verified Technologies will perform annual review and installation of VMware ESX updates. Installation of updates will be scheduled with Client to minimize downtime.
- Verified Technologies will perform annual review and updating of VMware tools on guest servers.

Requirements

- Client must have current VMware support subscription to gain access to current version and patches.
- Client must have HP Integrity Integrated Lights-Out (iLO), Cisco Integrated Management Controller (CIMC), IBM Remote Supervisor Adapter (RSA), or Dell Remote Access Controller (DRAC) to perform an orderly shutdown of server hardware for maintenance tasks and management.

Managed Security Information & Event Management (SIEM) Service Description

The Managed Security Information & Event Management (SIEM) service is a 24x7 world-class security monitoring service providing constant analysis of security logs generated within a Client's network to detect any malicious and unusual activity. To provide this service Verified Technologies has partnered with VijiLan, a 100% US-based Information Security Monitoring company. Suspicious log activities trigger analysis and review by highly skilled security engineers and Incident Response Team (IRT) to analyze and respond to threats 24x7x365. VijiLan's Incident Response Team works through Verified Technologies on recommended response resolution to incidents. This service consists of the following:

- Verified Technologies will configure a Vijilan virtual appliance log collector on the Client's network to collect logs from devices.
- Collected logs are parsed by the collector appliance then delivered to the management portal for analysis.
- Verified Technologies will work with VijiLan SOC to onboard Client.
- Verified Technologies will establish communication tree between VijiLan Incident Response Team (IRT), Verified and Client based on Client needs.
- Verified Technologies will coordinate incident resolution with Client.
- Incident Response Team will create a ticket in Verified Technologies PSA tool for each incident.
- In the event an incident is receive after-hours, a Verified Technologies engineer will be scheduled to respond the following morning.
- If After-Hours incident remediation is required, normal Reactive Support Service rates would apply and be billed accordingly.

Reporting:

- Verified Technologies will produce monthly executive security summary reports.
- Client will have access to management portal to create compliance reports as needed.

Requirements:

- Current supported and licensed operating systems.
- Business grade firewall appliance with current security support subscriptions.

Infrastructure Management Service Descriptions

Managed IP Device - Basic is a component of the Verified Technologies service offering which provides basic management of a Client owned IP based appliance, where full SNMP management is not needed. These devices may include, routers, switches, wireless access points and controllers, storage devices, or other network connected devices. This service consists of the following:

- Verified Technologies will provide 24x7 ICMP/ping monitoring to detect the up/down status of the device.
- Verified Technologies will make any required basic configuration changes as needed.
- Verified Technologies will ensure that requested configuration changes meet best practices.
- Verified Technologies will create and store configuration backups if device is capable.
- All device configuration work will be performed remotely.
- If onsite remediation is required, normal Reactive Support Service rates would apply and be billed accordingly.
- In the event of hardware failure covered under manufacturer warranty, Verified Technologies will contact the vendor on Client's behalf and coordinate the replacement.

Installations, Moves and Changes (IMACs)

- Installations, Moves and Changes of desktops, servers, and infrastructure hardware are not within the scope of the Agreement.
- For IMAC's, normal Reactive Support Service rates would apply and be billed accordingly.

Un-Managed Devices

- In the event the Client has devices which do not have a management interface or the ability to assign an IP address (Example: lower-end switches), Verified Technologies will not have the ability to monitor the status of those devices.
- If a device does have a management IP address but the Client has chosen not to place the device under Verified Technologies management, Verified Technologies' network management tools will detect the presence of the device but monitoring alert notifications will not be enabled for the device.
- The Client's list of covered devices is listed within Exhibit "B".

System Monitoring

Verified Technologies System Monitoring provides 24x7 proactive monitoring with notification of problems or changes with Client's Servers. This service consists of:

- Verified Technologies will review System Logs on all Servers for proper operation.
- Verified Technologies will review and verify Server Backup Logs for proper operation.
- Verified Technologies will configure Specified Monitoring and Alerts including:
    - Alert/Log on major hardware and software changes
    - Alert/Log on disk space when running low
    - Alert/Log on system online/offline status
    - Alert/Log on Server CPU Utilization
    - Alert/Log on critical Windows service failure
    - Alert/Log on critical SQL Server service failure
    - Alert/Log on critical Exchange Server service failure
    - Alert/Log scheduled discovery of all new devices on the network

- Review of the console and logs will occur during regular Verified Technologies business hours.
- If onsite remediation is required, normal Reactive Support Service rates would apply and be billed accordingly.
- The Client's list of covered devices is listed within Exhibit "B".
- Verified Technologies will provide management reports as defined in Reporting.

Cyber Security Tool Stack

Standard Cyber Security Stack

Cyber-crime and ransomware are the biggest threats to your business and data. Verified Technologies Cyber security tool stack is a set of tools and solutions, installed on all computers under our management, used to protect your data and systems from malicious attacks. The Standard Cyber Security Tool Stack tools are included in the base price of your Managed Server, Managed Desktop, Hosted Virtual Server or Azure AVD services. These tools include:

- Antivirus and Anti-malware Scanning. (Detects malware and viruses in real-time.)
- Application Whitelisting and RingFencing. (Permits only permitted applications to run, blocking all others.)
- Ransomware Attack Prevention and Client Isolation. (Detects crypto attacks and disconnects computer from the network if detected.)
- End User Security Awareness Training. (Included with Managed Desktop service.)

Advanced Cyber Security Tool Stack

When compliance regulations like PCI, FINRA or HIPAA demand an even higher standard of cyber security protection Verified Technologies offers many advanced security tools for both endpoints and entire networks. Client will incur additional charges for any Advanced Security Stack Tools. Any add-on Advanced Security Stack Tools subscribed to will be listed on your Statement of Work and monthly invoices. Advanced Security Stack Tools include:

- Managed Detection & Response. (MDR/EDR)
- Managed Disk Encryption.
- Internal Vulnerability Scanning.

Virus and Malware Protection

Virus Protection - Virus Protection for Client Windows Servers and Workstations provides protection with a centralized management console that affords automatic updating and reporting.

- Licensing for anti-virus / anti-malware is included in the Managed Server and Managed Desktop Services.
- The Client's list of covered devices is listed within Exhibit "B".
- If onsite or remote remediation is required due to a Virus or similar event, normal Reactive Support Service rates would apply and be billed accordingly.
- Virus Reports are included within the report as part of the scheduled Virtual CIO Services.

Malware Protection - Malware Protection utilizes technologies that are designed to quickly detect, destroy, and prevent malware.

- The Client's list of covered devices is listed within Exhibit "B".
- If onsite or remote remediation is required due to a Malware or similar event, normal Reactive Support Service rates would apply and be billed accordingly.
- Verified Technologies will provide management reports as defined in Reporting.

Patch Management

Verified Technologies Patch Management is not just scanning and applying patches to Servers and Workstations. Verified Technologies provides the software tools and infrastructure to easily address the complexities of software and security patch deployment. This service consists of:

- Verified Technologies will scan the Managed Servers and Managed Workstations monthly for installed and missing Critical Updates, Security Updates and vulnerabilities. (Only on Windows 10, 2012 R2 or newer Operating Systems).
- Verified Technologies will monitor and maintain patch compliance.
- Verified Technologies will schedule patch deployment and maintenance on Servers between Saturday 11:00 PM and Sunday 05:00 AM. Servers may be temporarily unavailable during this time-frame as Servers may be rebooted.
- Verified Technologies will schedule patch deployment and maintenance on Workstations after-hours during the week while users are logged out. Please notify Verified Technologies if these maintenance windows pose any risk or user disruption.
- The Client's list of covered devices is listed within Exhibit "B".
- Verified Technologies will provide management reports as defined in Reporting.

Security Awareness Training

Verified Technologies has partnered with Breach Secure Now, an industry recognized Cyber Security Awareness Training and Dark Web Monitoring platform. This training program is bundled with our Managed Desktop services and allows your organization to take a proactive stance on end-user cyber security education and provides statistics to assess current and ongoing security training effectiveness. Breach Secure Now includes a large library of security awareness video-based training content. The service consists of the following:

SECURITY AWARENESS TRAINING & TESTING

- Each week, users will be sent an email to watch a 1-2-minute micro-training video on the latest cyber security threats. After watching the video users will see a 4-question quiz. Each quiz completed increases a user's Employee Secure Score!

DARK WEB MONITORING

- The Dark Web is continually scanned for your organizations domains to detect any compromised email accounts. Users can check if their own personal email has been compromised and found on the Dark Web. Licensing includes 3 monitored domains.

SIMULATED PHISHING ATTACKS

- Periodically, users will receive fake phishing emails to test their ability to look for and avoid phishing emails. Phishing tests will be performed on a bi-weekly basis.

Manager Level Access can be granted to Client managers to allow visibility into the training performance of the entire organization.

Reporting:

- Verified Technologies will review cyber security training metrics as part of the Technology Business Review process. Training reports can be provided on request.

Managed Backup with Cloud Storage Service Description

Backup Management is the most critical element in protecting your company's data. For this service Verified Technologies will provide backup software licensing and management. This service consists of:

- Verified Technologies will provide license for image-based backups of Client’s Windows Server, including MS SQL Server and MS Exchange Server
- Verified Technologies will configure backups as follows:
  - Store backup images on local NAS storage (NAS provided by Client)
  - Replicate backup images to offsite cloud storage and retained for 30 days up to the allocated storage limit
  - Backup jobs to run on a daily basis
  - Backup application to deliver backup job status notifications to Verified Technologies’ backup monitoring queue.
- Verified Technologies will check the backup log on a daily basis.
- In the event of backup job failure, Verified Technologies will connect remotely to the backup server or application and, where possible, resolve the issue causing the job failure.
- If the backup job failure cannot be permanently resolved due to device failure or a cause beyond Verified Technologies’ control, Verified Technologies will immediately contact the Client and provide options or estimates for a permanent resolution.
- If file restoration or server recovery is required, normal Reactive Support Service rates would apply and be billed accordingly.
- Backup reports can be produced upon request.

Datto Backup Service Description

Datto Backup Monitoring provides crucial oversight of protecting your company's data. For this service Verified will monitor and manage a Client owned and licensed backup solution.

This service consists of:

- Verified Technologies will configure Client's Datto device to meet required RTO and RPO objectives. (Default is 30- or 15-minute backup intervals depending on available device storage)
- Verified Technologies will configure backup jobs to replicate data to the Datto Cloud. (Requires Datto Cloud subscription)

- Verified Technologies will configure Client's Datto backup application to deliver backup job status notifications to Verified Technologies' PSA tools.
- Verified Technologies will check the backup log on a daily basis.
- In the event of backup job failure, Verified Technologies will connect remotely to the backup server or application and, where possible, resolve the issue causing the job failure.
- If the backup job failure cannot be permanently resolved due to device failure or a cause beyond Verified Technologies' control, Verified Technologies will immediately contact the Client and provide options or estimates for a permanent resolution.
- If file restoration or server recovery is required, normal Reactive Support Service rates would apply and be billed accordingly.
- Verified Technologies will provide backup reports as defined in Reporting.

Requirements for this service:

- 2U server rack space (Depending on model)
- Dual 15 Amp power outlets.
- Local network connectivity and Internet access for cloud storage and remote management.
- Removal of existing backup software from source servers.
- Client must notify Verified Technologies if additional servers are to be included in backup schedule.

Backup Monitoring

Backup Monitoring is the most critical element in protecting your company's data. For this service Verified Technologies will monitor and manage a Client owned and licensed backup solution. This service consists of:

- Verified Technologies will configure Client's backup application to deliver backup job status notifications to Verified Technologies' backup monitoring queue.
- Verified Technologies will check the backup log on a daily basis.
- In the event of backup job failure, Verified Technologies will connect remotely to the backup server or application and, where possible, resolve the issue causing the job failure.
- If the backup job failure cannot be permanently resolved due to device failure or a cause beyond Verified Technologies' control, Verified Technologies will immediately contact the Client and provide options or estimates for a permanent resolution.
- If file restoration or server recovery is required, normal Reactive Support Service rates would apply and be billed
- accordingly.
- Backup reports are a function of the Client's' backup application and can be produced upon request.

Best Practice: A backup policy helps manage Client's expectations and provides specific guidance on the "who, what, when, and how" of the data backup and restore process. There are several benefits to documenting your data backup
policy. Your policy should dictate:

- where backups are located
- who can access backups and how they can be contacted
- how often data should be backed up
- what kind of backups are performed
- what hardware and software are recommended for performing backups that ensure business continuity

Verified Technologies can provide assistance in developing and creating a backup policy for your company or provide a Managed Backup Service to meet your policy requirements.

Reporting

Management reports are a critical component of the Verified Technologies service offerings. Reporting allows us to identify potential gaps in delivery of security updates, anti-virus updates or backups of managed servers and workstations. Verified Technologies is constantly improving our reports and adding new report sections as integrations allow. Current reporting includes the following content:

- Managed Server Patch Status.
- Managed Workstation Patch Status.
- Managed Server Anti-virus Status.
- Managed Workstation Anti-virus Status.
- Obsolete Server Operating Systems.
- Obsolete Workstation Operating Systems.
- Service tickets closed in the last 30 days.
- Open service tickets.
- Upcoming warranty and license subscription renewals in the next 60 days.
- Inventory of managed endpoints with management agents installed.
- Delivered via email to the Client primary contact or designated contact on the first day of every month.

Virtual CIO Services

Virtual CIO Services include a comprehensive yearly report of the services provided in the past. In addition, a yearly round table conversation with a Senior Technical Consultant or a key member of the Verified Technologies Technical Services Management Team to discuss:

- Managed services reports.
- Past issues/trends and recommended remediation.
- Future objectives and emerging technologies or products that are applicable to the environment.
- Overall technology direction on both a strategic and tactical level.
- Upcoming renewals for budgetary purposes.
- Any other related technology topics that the Client wishes to discuss.

Microsoft Azure Cloud Service Description

Verified Technologies brings the security and reliability of the Microsoft Azure Cloud to provide a secure, fully managed, cloud-based virtual desktop experience to your end-users on the device of their choice. The Microsoft Azure Virtual Desktop (AVD) delivers a multi-session Windows 11 or Windows 10 deployment that delivers a full Windows experience with scalability to host your line-of-business applications. This service consists of the following:

- Verified Technologies will provide dedicated session-host server(s).
- Resources including disk storage, memory and processor capacity will be provisioned as to provide optimal performance and in accordance with the services purchased. Additional resources may incur additional charges.
- Verified Technologies will perform a backup of Client data and applications on a daily basis.
- Verified Technologies will provide 24x7 monitoring and alerting on critical events as defined in System Monitoring.
- In the event of an alert indicating Server offline or critical event failure, Verified Technologies will attempt to connect and restart the service or resolve the incident.
- This service includes unlimited Remote Support for the server operating system and services including, but not limited to:
  - Microsoft Office suite
  - network connectivity
  - printing issues
  - access to servers
- End users can call in to the Verified Technologies Service Desk, where a Verified Technologies support representative will provide remote support to the end user to resolve the incident.
- If onsite remediation is required, normal Reactive Support Service rates would apply and be billed accordingly.
- Third-party application support is not covered under this service. Verified Technologies will provide support for third-party applications at the normal Reactive Support Service rates.
- Verified Technologies will perform patching as defined in Patch Management.
- Verified Technologies will include security tools as defined in Cyber Security Tool Stack.
- This service does not include any Microsoft Office 365 license subscriptions.

THESE DESCRIPTIONS ARE SUBJECT TO CHANGE ANY TIME WITHOUT NOTICE.