Managed Services

(Please refer to the Quote to determine which Managed Services you will be receiving.)

SERVICES	GENERAL DESCRIPTION
Backup and File Recovery	Implementation and facilitation of a backup and file recovery solution from our designated Third Party Provider. • 24/7 monitoring of backup system, including offsite backup, offsite replication, and an onsite backup appliance ("Backup Appliance"). • Troubleshooting and remediation of failed backup disks. • Preventive maintenance and management of imaging software. • Firmware and software updates of backup appliance. • Problem analysis by the network operations team. • Monitoring of backup successes and failures. • Daily recovery verification. Backup Data Security: All backed up data is encrypted in transit and at rest in 256-bit AES encryption. All facilities housing backed up data implement physical security controls and logs, including security cameras, and have multiple internet connections with failover capabilities. Backup Retention: Backed up data will be retained for the periods indicated below, unless a different time period is expressly stated in the Quote. This includes both on-premise and cloud backups. • On-Premise Backups All on-premise backups will be stored on a Network Attached Storage (NAS) device, which will be kept in a secure location with restricted access. On-premise backups will be performed daily and retained on a rolling thirty (30) day basis. • Cloud Backups All cloud backups will be stored in a secure, off-site location that meets the organization's security standards. Cloud backups will be performed daily and retained on a rolling thirty (30) day basis. Backup Alerts: Managed servers will be configured to inform of any backup failures. Recovery of Data: If you need to recover any of your backed up data, then the following procedures will apply: • Service Hours: Backed up data can be requested during our normal business hours. • Request Method. Requests to restore backed up data should be made through one of the following methods: o Email: mailto:mdieter.wolf@wolferdawg.com o Phone: (580) 956-8424 • Restoration Time: We will endeavor to restore backed up data as quickly as possible following our receipt of a request to do so; however, in all cases data restoration services are subject to (i) technician availability and (ii) confirmation that the restoration point(s) is/are available to receive the backed up data.

Backup Monitoring	Implementation and facilitation of a backup monitoring solution from our designated Third Party Provider. Features include: • Monitoring backup status for certain backup applications then-installed in the managed environment, such as successful completion of backup, failure errors, and destination free space restrictions/limitations. • Helping ensure adequate access to Client's data in the event of loss of data or disruption of certain existing backup applications. Note: Backup monitoring is limited to monitoring activities only and is not a backup and file recovery solution.
Dark Web Monitoring	Implementation and facilitation of a Dark Web Monitoring solution from our designated Third Party Provider. Credentials supplied by Client will be added into a system that continuously uses human and machine-powered monitoring to determine if the supplied credentials are located on the dark web. If compromised credentials are found, they are reported to Help Desk Services staff who will review the incident and notify affected end-users. Dark web monitoring can be a highly effective tool to reduce the risk of certain types of cybercrime; however, we do not guarantee that the dark web monitoring service will detect all actual or potential uses of your designated credentials or information.
Email Threat Protection	Implementation and facilitation of a trusted email threat protection solution from our designated Third Party Provider. • Managed email protection from phishing, business email compromise (BEC), SPAM, and email-based malware. • Friendly Name filters to protect against social engineering impersonation attacks on managed devices. • Protection against social engineering attacks like whaling, CEO fraud, business email compromise or W-2 fraud. • Protects against newly registered and newly observed domains to catch the first email from a newly registered domain. • Protects against display name spoofing. • Protects against "looks like" and "sounds like" versions of domain names. **Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.** **All hosted email is subject to the terms of our Hosted Email Policy and our Acceptable Use Policy.**
Endpoint Antivirus & Malware Protection	Implementation and facilitation of an endpoint malware protection solution from our designated Third Party Provider. • Artificial intelligence and machine learning to provide a comprehensive and adaptive protection paradigm to managed endpoints. • Detection of unauthorized behaviors of users, applications, or network servers. • Blocking of suspicious actions before execution. • Analyzing suspicious app activity in isolated sandboxes. • Antivirus and malware protection for managed devices such as laptops, desktops, and servers. • Protection against file-based and fileless scripts, as well as malicious JavaScript, VBScript, PowerShell, macros and more. • Whitelisting for legitimate scripts. • Blocking of unwanted web content.

	• Detection of advanced phishing attacks. • Detection / prevention of content from IP addresses with low reputation. *** Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Extended Detection & Response (XDR)	Implementation and facilitation of an endpoint malware protection solution with extended functionalities from our designated Third Party Provider. • Automated correlation of data across multiple security layers*—email, endpoint, server, cloud workload, and the managed network, enabling faster threat detection. • Provides extended malware sweeping, hunting, and investigation. • Allows whitelisting for legitimate scripts. • Next-generation deep learning malware detection, file scanning, and live protection for workstation operating system. • Web access security and control, application security and control, intrusion prevention system. • Data loss prevention, exploit prevention, malicious traffic detection, disk and boot record protection. • Managed detection, root cause analysis, deep learning malware analysis, and live response. • On-demand endpoint isolation, advanced threat intelligence, and forensic data export. * Requires at least two layers (*e.g.*, endpoint, email, network, servers, and/or cloud workload.) **Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
End User Security Awareness Training	Implementation and facilitation of a security awareness training solution from an industry-leading third party solution provider. • Online, on-demand training videos (multi-lingual). • Online, on-demand quizzes to verify employee retention of training content. • Baseline testing to assess the phish-prone percentage of users; simulated phishing email campaigns designed to educate employees about security threats. **Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Firewall Solution (firewall appliance provided / purchased by Client)	• Monitors, updates (software/firmware), and supports Client-supplied firewall appliance. • Helps to prevent hackers from accessing internal network(s) from outside the network(s), while providing secure and encrypted remote network access; provides antivirus scanning for all traffic entering and leaving the managed network; provides website content filtering functionality.
Managed Detection & Response (MDR)	Implementation and facilitation of a top-tier MDR solution from our designated Third Party Provider. • 24x7 Managed network detection and response. • Real time and continuous (24x7) monitoring and threat hunting. • Real time threat response. • Alerts handled in accordance with our Service response times, below. • Security reports, such as privileged activities, security events, and network reports, are available upon request. • 24x7x365 access to a security team for incident response*

	* **Remediation services provided on a time and materials basis. Please see Anti-Virus; Anti-Malware and Breach / Cyber Security Incident Recovery sections below for important details.**
Password Manager	Implementation and facilitation of a password management protection solution from our designated Third Party Provider. • Password Vault: Securely store and organize passwords in a secure digital location accessed through your browser or an app. • Password Generation: Generate secure passwords with editable options to meet specific criteria. • Financial Information Vault: Securely store and organize financial information such as bank accounts and credit card information in a secure digital location accessed through your browser or an app. • Contact Information Vault: Store private addresses and personal contact information within your vault accessed through your browser or an app. • Browser App: Browser extension permits easy access to your information including the vaults, financial information, contact information, and single sign-on through the app. • Smart-Phone App: Mobile phone app enables access to your vault and stored information on your mobile device.
Remote Helpdesk	• Remote support provided during normal business hours for managed devices and covered software • Tiered-level support provides a smooth escalation process and helps to ensure effective solutions.
Remote Infrastructure Maintenance & Support	• Configuration, monitoring, and preventative maintenance services provided for the managed IT infrastructure • If remote efforts are unsuccessful, then Wolferdawg IT will dispatch a technician to the Client's premises to resolve covered incidents (timing of onsite support is subject to technician availability and scheduling).
Remote Monitoring and Management	Software agents installed in Covered Equipment (defined below) report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below. • Includes capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD partitions, not external devices such as USB or mapped drives) • Includes routine operating system inspection and cleansing to help ensure that disk space is increased before space-related issues occur. • Review and installation of updates and patches for supported software. In addition to the above, our remote monitoring and management service will be provided as follows:

Event	Server	Workstation
Hardware Failures	Yes	No
Device Offline	Yes	No
Failed/Missing Backup	Yes	No

Failed/Missing Updates	Yes	Yes
Low Disk Space	Yes	No
Agent missing/misconfigured	Yes	Yes
Excessive Uptime	Yes	No
Automatic Reboots (weekly)	No	Yes

Security Incident & Event Monitoring (SIEM)

Implementation and facilitation of an industry leading SIEM solution from our designated Third Party Provider.

The SIEM service utilizes threat intelligence to detect threats that can exploit potential vulnerabilities against your managed network.

- Initial Assessment. Prior to implementing the SIEM service, we will perform an initial assessment of the managed network at your premises to define the scope of the devices/network to be monitored (the "Initial Assessment").

- Monitoring. The SIEM service detects threats from external facing attacks as well as potential insider threats and attacks occurring inside the monitored network. Threats are correlated against known baselines to determine the severity of the attack.

- Alerts & Analysis. Threats are reviewed and analyzed by third-party human analysts to determine true/false positive dispositions and actionability. If it is determined that the threat was generated from an actual security-related or operationally deviating event (an "Event"), then you will be notified of that Event.

  Events are triggered when conditions on the monitored system meet or exceed predefined criteria (the "Criteria"). Since the Criteria are established and optimized over time, the first thirty (30) days after deployment of the SIEM services will be used to identify a baseline of the Client's environment and user behavior. During this initial thirty (30) day period, Client may experience some "false positives" or, alternatively, during this period not all anomalous activities may be detected.

Note: The SIEM service is a monitoring and alert-based system only; remediation of detected or actual threats are not within the scope of this service and may require Client to retain Wolferdawg IT's services on a time and materials basis.

Server Monitoring & Maintenance

As part of our RMM service, we will monitor and maintain managed servers as follows:

- Software agents installed in covered servers report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below.
- Online status monitoring, alerting us to potential failures or outages
- Capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD and SSD partitions, not external devices such as USB or mapped network drives)
- Performance monitoring, alerting us to unusual processor or memory usage
- Server essential service monitoring, alerting us to server role-based service failures
- Endpoint protection agent monitoring, alerting us to potential security vulnerabilities
- Routine operating system inspection and cleansing

	• Secure remote connectivity to the server and collaborative screen sharing • Review and installation of updates and patches for Windows and supported software • Asset inventory and server information collection
Two Factor Authentication	Implementation and facilitation of a two factor authentication solution from our designated Third Party Provider. • Advanced two factor authentication with advanced administrative features • Secures on-premises and cloud-based applications • Permits custom access policies based on role, device, location • Identifies and verifies device health to detect “risky” devices
Server Next-Generation Antivirus	Implementation and facilitation of a top-tier, next generation antivirus protection solution from our designated Third Party Provider. Software agents installed in covered server devices protect against malware and prevents intruder access. Used in coordination with other endpoint security layers and security solutions to form a comprehensive defense strategy. • Next-generation deep learning malware detection, file scanning, and live protection for Server OS • Web access security and control, application security and control, intrusion prevention system • Data loss prevention, exploit prevention, malicious traffic detection, disk and boot record protection
Updates & Patching	• Remotely deploy updates (e.g., x.1 to x.2), as well as bug fixes, minor enhancements, and security updates as deemed necessary on all managed hardware. • Perform minor hardware and software installations and upgrades of managed hardware. • Perform minor installations (i.e., tasks that can be performed remotely and typically take less than thirty (30) minutes to complete). • Deploy, manage, and monitor the installation of approved service packs, security updates and firmware updates as deemed necessary on all applicable managed hardware. Please note: We will keep all managed hardware and managed software current with critical patches and updates (“Patches”) as those Patches are released generally by the applicable manufacturers. Patches are developed by third party vendors and, on rare occasions, may make the Environment, or portions of the Environment, unstable or cause the managed equipment or software to fail to function properly even when the Patches are installed correctly. We will not be responsible for any downtime or losses arising from or related to the installation or use of any Patch. We reserve the right, but not the obligation, to refrain from installing a Patch if we are aware of technical problems caused by a Patch, or we believe that a Patch may render the Environment, or any portion of the Environment, unstable.
Wi-Fi Services	Wolferdawg IT will install at the Client’s premises Wireless Access Points to provide bandwidth in all areas requiring wireless network coverage, as agreed upon by Wolferdawg IT and Client. • Wolferdawg IT will maintain, supervise, and manage the wireless system at no additional cost.

	• Installed equipment, if provided by Wolferdawg IT, will be compatible with the then-current industry standards. • Wolferdawg IT will provide remote support services during normal business hours to assist with device connectivity issues. (Support services will be provided on a "best efforts" basis only, and Client understands that some end-user devices may not connect to the wireless network, or they may connect but not perform well). Please note: Any Wi-Fi devices, such as access points or routers, that are supplied by Client cannot be older than five (5) years from the applicable device's original date of manufacture, and in all cases must be supported by the manufacturer of the device(s).
Workstation Next-Generation Malware Solution	Implementation and facilitation of an industry-recognized, next generation workstation malware protection solution from our designated Third Party Provider. Software agents installed in covered devices protect against malware and prevent intruder access. Used in coordination with other endpoint security layers and security solutions to create a comprehensive defensive strategy. • Next-generation deep learning malware detection, file scanning, and live protection for Workstation OS. • Web access security and control, application security and control, intrusion prevention system. • Data loss prevention, exploit prevention, malicious traffic detection, disk, and boot record protection.
Workstation Monitoring & Maintenance	Software agents installed in covered workstations report status and IT-related events on a 24x7 basis; alerts are generated and responded to in accordance with the Service Levels described below. • Online status monitoring, alerting us to potential failures or outages. • Capacity monitoring, alerting us to severely decreased or low disk capacity (covers standard fixed HDD and SSD partitions, not external devices such as USB or mapped network drives). • Performance monitoring, alerting us to unusual processor or memory usage. • Endpoint protection agent monitoring, alerting us to potential security vulnerabilities. • Routine operating system inspection and cleansing. • Secure remote connectivity to the workstation and collaborative screen sharing. • Review and installation of updates and patches for Windows and supported software. • Asset inventory and workstation information collection.