Computer and Network Systems
Service Level Agreement (SLA)

This Agreement entered into on this ___ day of _____ by and between Clover Services, Inc., a North Carolina Corporation, herein after referred to as Clover Services, Inc. with offices located in Charlotte, North Carolina, and _____at_____(Corporation, LLC, Partnership) herein after referred to as Client, under the following terms and conditions.

AGREEMENT

Clover Services, Inc. shall provide to Client, support which includes, but is not limited to the following:
This Agreement is for onsite and remote Corporate Support services provided for the offices, or building of Client, Headquartered at: _____for a period of 24 months.

1. This Agreement may be used toward residential computer and network support for Client staff and family, providing the work is approved by Client and requested as part of the Client extended user network.
   1.1 Troubleshooting of reported computer or network problems
   1.2 Installing and configuring computer operating systems, application software
   1.3 Remote support
   1.4 User access addition(s)/removal(s)
   1.5 Office automation and technology integration, long-term planning, technology consultation
   1.6 Computer network asset documentation and acquisition services
   1.7 Practice Management Software customizations and interface/file structure design
   1.8 Computer, Server and Network security services, network optimization services

2. Additional Support services including, but is not limited to the following may be contracted by client and will be quoted and billed separately:
   2.1 Structured Wiring and network physical infrastructure
   2.2 Phone Service
   2.3 Network Design and Planning
   2.4 Installation and troubleshooting services

This Agreement includes descriptions of types of Support and the applicable rate structures. New services, and some specific services not explicitly described here may be priced separately than rates described herein. Services requiring their own rate structure will be defined and approved of by Client prior to commencing.

SUPPORT TYPES

Client shall have the right to purchase from Clover Services the Support type it desires, found on Appendices, which include the following:

1. Corporate Silver (Hosted Phone Clients Appendix A)
2. Corporate Gold (Appendix B)
3. Corporate Platinum (Appendix C)
4. Platinum Premium 24x7 (Appendix D)
5. Pricing (Appendix E)

PAYMENTS

1. Payments by Client to Clover Services, Inc., shall be made within 15 days of invoice and Client shall pay by either check or credit card.
2. Rates are outlined in Appendix E.
3. A $35.00 late fee is added to all late payments.
4. Clover Services, Inc., support professionals do not accept payments.
5. If mailed payments are required, payments shall be mailed to the address on the invoice: Clover Services, Inc., 2923 S. Tryon Street, Suite 240, Charlotte, NC 28203.

BILLING

1. Billable time begins upon arrival at location or upon the beginning of telephone, Email, Remote administration support session.
2. Invoices are sent via Email with one or more of the following options applied by Clover Services, Inc.
3. After 15 days of receiving an invoice, amounts due are automatically charged against your Credit Card on file. All billing disputes must be made within 15 days prior to invoice due date via Email using customerservice@cloverservies.com.

EARLY TERMINATION

Early Termination Charge. If Customer terminates this agreement, in whole or in part, prior to the end of the then current term, in addition to any other damages or liability of Customer resulting from such termination, Customer must pay a lump sum Early Termination charge as follows:

1. 100% of all remaining months of Agreement; and
2. 100% of any invoices or charges that have been paid by Carrier on Customer's behalf.

SUPPORT REQUESTS & TIME

1. Requesting Support and Scheduled Appointment

1.1. All Clients will have a Client web portal which is accessed via a username and password.
   a. Only personnel that the Client specifies can request support. As many authorized users may
   b. be added as the Client needs. Here you may enter new support requests, track your open
   c. tickets, add information to tickets, see who your ticket is assigned to, the method of support
   d. provided – be it on-site or remote, and the estimated completion date. Here you may search
   e. the interactive knowledgebase of the most common IT issues at your site, so end-users can
   f. try to remedy easily solved previous events.
2. After Business Hours Support, Weekend Support, and Time Commitments
   a. Unscheduled support provided after Standard Support hours and/or weekends is billable as outline in Appendix A and must be pre-approved by the customer
3. Time
   a. It is assumed that all time spent in dialogue with a customer experiencing an issue or seeking Technical questions of any kind via phone, Email or onsite, may be invoiced.

CONFIDENTIALITY, SECURITY, AND DATA INTEGRITY

1. Clover Services, Inc., may identify security risks, breaches, or other liabilities and make specific
2. recommendations in writing for the resolution of these risks. Clover Services, Inc., cannot be held
3. responsible for exploited security threats.

4. Clover Services, Inc., accepts no responsibility or liability for lost, missing, or corrupted data caused
5. by viruses, worms, unauthorized user activity (hacking), and the like. From time to time, Clover
6. Services, Inc., may identify specific threats and may recommend and undertake immediate action
7. to protect Client networks without prior authorization. While this is rare, notice of this action will be
8. given in the earliest reasonable time after the work occurred, including details of what the specific
9. issue was and why immediate action was necessary. Corporate Standard Support services given
10. to intervene or remediate these issues are billable activities for which Client assumes responsibility.

11. In order to provide Support Services as described herein, Clover Services, Inc., technicians will
12. necessarily be privy to and have access to sensitive Client firm data files and other sensitive
13. information. Clover Services, Inc., agrees to take all reasonable measures to keep all files, client
14. information, passwords, and any other proprietary client data secure and confidential.
15. Clover Services, Inc. will not delete, remove, or alter client data files.

CLOVER SERVICES, INC. STAFFING

NON-COMPETE. During the period of time that the Customer employs services from Clover Services,
Inc., and for a period of (1) year after the termination or cessation of such employment for any reason,
(both periods of time, taken together, being referred to hereinafter as the "RESTRICTED PERIOD", the customer shall not, anywhere in the United States, directly, or indirectly, whether individually or as an officer, director, employee, consultant, partner, stockholder (other than as the holder of not more
than one percent (1%) of a publicly held corporation), individual proprietor, joint venture, investor, lender, consultant or in any other capacity whatsoever, solicit, entice, approach, advance or offer a position for reimbursement of trade of products or services competitive with those developed, designed, produced, marketed, sold, or rendered by Clover Services, Inc., at any time during the Restricted Period.

NON-SOLICITATION. During the Service Period and the Restricted Period, the Customer shall not, directly or indirectly, whether individually or as an officer, director, employee, consultant, partner, stockholder, individual proprietor, joint venture, investor, lender, consultant, or any other capacity whatsoever: (a) solicit, divert, or take away, or attempt to solicit, divert, or take away, or attempt to solicit, divert, or take away Clover Services, Inc. Staff or (b) hire, retain (including as a consultant) or encourage Clover Services, Inc., Staff to leave the employment of Clover Services, Inc., or hire or retain (including as a consultant) any former employee of the Company who has left the employment of the Company within one (1) year prior to such hiring or retention.

ACKOWLEDGEMENT. The Customer agrees and acknowledges that their non-competition and non-solicitation obligations hereunder are essential to the protection of the Clover Services, Inc., business.

EQUITABLE REMEDIES. The parties hereto hereby agree that breaches of covenants and obligations undertaken in this Agreement are likely to cause Clover Services, Inc., substantial and irrevocable damage, which would be difficult, if not impossible, to prove precisely; therefore, it is agreed that this Agreement shall be enforceable by specific performance. If breach is found on behalf of the Customer, the Customer agrees to pay a 6 month average of previous IT labor invoices. This date is determined by the Clover Services, Inc., staff worker performing IT related

services as defined in the Service Level Agreement for the Customer directly and thus circumventing
Clover Services, Inc. services. If the Customer is less than 6 months old, 50% of the averaged IT labor generated to date shall be owed.

Litigated cases where the Customer is in Breach of the Agreement shall only be tried in Mecklenburg County, North Carolina regardless of where the Customer resides.

Rulings against the Customer require the Customer to pay all court and lawyer fees on behalf of Clover Services, Inc.

WARRANTY INFORMATION

5. Software and hardware warranties are as supplied from the respective manufacturers.

6. Clover Services, Inc. makes no implied or explicit warranties other than software and hardware will be installed correctly based upon manufacturer and/or industry standards.

7. Return visits or remote sessions initiated in response to warranty service requests may reveal an underlying cause was not due to any failure or error on the part of Clover Services, Inc. At that time, the return visit may become billable. If this is the case, Clover Services, Inc., will provide documentation explaining the root cause and why it is not a warranty issue.

8. Warranty support requests should be made in writing to managers@cloverservices.com and shall include the following:
    a) Statement of known issue.
    b) State how this issue is related to or appears caused by the prior work.
    c) Statement of intended outcome(s).

9. It is the desire of Clover Services, Inc., to provide superior service, however, computers and networks are complex systems with sometimes unpredictable interactions between various applications software and hardware configurations. Clover Services, Inc. will strive to explain clearly when these unanticipated interactions cause problems which are not specifically tied to warranted work.

WARRANTY EXCLUSIONS

1. Generic PC's assembled from off-the-shelf components (AKA "White Boxes") are not recommended by Clover Services, Inc.

2. Refurbished machines and machines that were previously owned.

3. Any PC's knowingly and intentionally operated by client without a pay licensed virus protection, or unlicensed and un-patched software.

4. As offsite IT administration; Clover Services, Inc., accepts no responsibility or liability for: lost, missing or corrupted data, viruses, worms, hacked systems, and similar items resulting in a mission critical situation or financial loss.

5. User error, user inability to run applications, hardware failure and help installing removing or using software.

Clover Services, Inc. reserves the right to decline any warranty including, but not limited to, other IT support provider's actions, such as: when the user/Client (or another administrator/3rd party) elects self-installation of software in a corporate setting without prior approval from Clover Services, Inc., this includes, but is not limited to: applications, Windows updates, other software updates and any hardware installation. Request for modification must be requested with approval granted via e-mail to support@cloverservices.com prior to any installations.

6. Clover Services, Inc. cannot warrant the outcome of work completed on 3rd party IP based (multifunction) printers.

7. Clover Services, Inc., does not service printer hardware of any kind.

8. Clover Services, Inc., does not service laptop hardware except for memory modules and hard drives.

GENERAL ITEMS

1. Clover Services, Inc. policy prohibits installation or support of any pirated or illegal copies of software. Client must be able to produce, on request, proof of ownership for all software with sufficient licenses for the number of users in the office. Original software disks indicating Client as the legal owner including proof of license shall be kept available, preferably in one central place to facilitate verification, software updates, and system reloads.

2. Sometimes Clover Services, Inc., may be required to contact a 3rd party for support (such as a hardware or software manufacturer). Clover Services, Inc., will bill the client up to 100% of any costs incurred for this 3rd party support.

3. The client is responsible for all drop shipments signed for and left at locations from all carriers. Please provide us with a main contact within your office if you would like to appoint a specific person for this activity.

4. Clover Services, Inc., recommends corporate grade systems, from manufacturers like Dell, Lenovo, HP and similar companies. Clover Services, Inc., does not generally sell hardware, but as a service, can assist with obtaining competitive quotes for Clover Services, Inc., Clients to purchase

the hardware directly. All quotes and time spent via email or phone are billed accordingly as Network Consultation at the rates listed herein.

5. Clover Services, Inc., hardware support and repair services are limited in scope.
   5.1. On Desktop PC's, Clover Services, Inc., generally only performs memory module upgrades. Other hardware upgrades may be obtained from a 3rd party vendor.
   5.2. Clover Services, Inc., does not service failed laptop hardware other than replacing hard drives or memory module upgrades.

6. Rates and terms are subject to change, as business conditions merit.

CLOVER SERVICES, INC., SUPPORT MINIMUM SYSTEM REQUIREMENTS

Minimum System Requirements are in place to protect clients from being billed for support equal to or more than the value of the actual equipment.

1. Clover Services, Inc., Minimum System Requirements – machines shall have ≥ 2.2 GHz processors, machines shall be running one of the following Operating Systems Windows 7 and higher, and Windows Server 2008 and higher.

2. Clover Services, Inc., supports most other Microsoft applications and all 3rd party Windows-based applications.

NOTICES

All notices and major consulting requests in connection with this Agreement shall be made in writing to the address listed below, unless notified by fax or email.

To Clover Services, Inc.:
Clover Services, Inc.
2923 S. Tryon St.
Ste. 240
Charlotte, NC 28203

Telephone: 704-706-2100
Email: support@cloverservices.com

GOVERNING LAW

This agreement and performance hereunder shall be governed by and construed in accordance with the
laws of the State of North Carolina.

ENTIRE AGREEMENT

Each party acknowledges that it has read this Agreement, understands, and agrees to be bound by its terms ad further agrees that it is the complete and exclusive statement of the agreement between the parties. This Agreement may not be modified or altered except by mutual written agreement, signed by both parties.

Clover Services, Inc.:

By: _____

_____

Jon Hobday

President

_____

Client:

By:

PRINTED NAME: _____

TITLE:

Support Level: _____

Additional Services See Appendix E?

Yes **No**

Appendix A
Corporate Silver (Hosted Phone Clients)

1. Server RMM
2. Workstation RMM
3. Managed Antivirus
4. Reports
5. Time to be Included

Corporate Silver Support Plan Explanations

1. Server & Remote Monitoring and Management

- Automatic notifications about device availability, performance, security, and backup status.
- Health check hardware and software.
- Virtual machine monitoring.
- Proactive Maintenance windows to run during off hours so you don't disrupt employees' productivity or raise false downtime alarms.

2. Managed Antivirus

- Extensive signature-based scanning: Use traditional signature-based threat detection to block known threats.
- Heuristic checks: Protect against previously unknown threats using heuristic checks, which detect new, unrecognized viruses in a sandbox environment away from a business's core systems.

- Active protection and behavioral scanning: Shut down even the most sophisticated malware via continuous real-time monitoring, which detects programs that perform actions commonly associated with malware exploits.
- Lightweight scans to reduce system resource drain.
- Reduces the number of false positives with more accurate scanning.
- Schedule deep scans ahead of time so you don't disrupt employees during important productive hours.
- Control timing: Pause or cancel scans when needed.

4. Reports

- One Executive summary report per month that display key metrics and support activities in an easy-to-digest, report that showcases all the critical functions performed.

5. Time to be included

- **Remote:** All time is billable with a one hour minimum.
- **On-site:** One hour minimum charge.
- **Travel Charge:** There will be a discounted travel charge for on-site visits.
- **After Hours & Public Holidays:** No work will be performed.

Appendix B

Corporate Gold

1. Server & Workstation RMM
2. Managed Antivirus
3. Encrypted Local Server Backup & Recovery
4. Central Managed Firewall/Router
5. Reports
6. Scheduled Task
7. Automation
8. Windows Patch Management
9. Spam Filter
10. Time to be Included

Corporate Gold Support Plan Explanations

1. Server & Remote Monitoring and Management

- Automatic notifications about device availability, performance, security, and backup status.
- Health check hardware and software.
- Virtual machine monitoring.
- Proactive Maintenance windows to run during off hours so you don't disrupt employees' productivity or raise false downtime alarms.

2. Managed Antivirus

- Extensive signature-based scanning: Use traditional signature-based threat detection to block known threats.
- Heuristic checks: Protect against previously unknown threats using heuristic checks, which detect new, unrecognized viruses in a sandbox environment away from a business's core systems.
- Active protection and behavioral scanning: Shut down even the most sophisticated malware via continuous real-time monitoring, which detects programs that perform actions commonly associated with malware exploits.
- Lightweight scans to reduce system resource drain.
- Reduces the number of false positives with more accurate scanning.
- Schedule deep scans ahead of time so you don't disrupt employees during important productive hours.
- Control timing: Pause or cancel scans when needed.

3. Encrypted Local Server Backup & Recovery

- Block level, allowing for lightweight and rapid backups. This makes it easier to back up more frequently and improve recovery point objectives, thereby minimizing data loss during a disaster.
- Bare metal protection automatically backs up the entire OS boot up environment, system state, applications, and data so you're prepared for a disaster.
- Continuous recovery: When you can't continuously update a running server, our backup and recovery feature automatically updates the standby server via a restore after each backup session of the live server completes.

4. Central Managed Firewall/Router

- Automatically updated with newest firmware.
- Manage all WAP's from one location.
- Dual WAN.

- Load balancing.
- Custom Firewall rules.
- High availability
- QoS
- SSL VPN
- VLAN
- PCI-DDS Credit card security.
- Wireless built in.
- AC

5. Reports
    - Executive summary report display key metrics and support activities in an easy-to-digest, report that showcases all the critical functions performed.
    - Additional reports: A wide variety of additional reports. These reports cover such key areas as device inventory, pricing, antivirus protection, backup integrity, user audits, hardware and software checkups, and more.
    - Custom reports.
6. Scheduled Task
    - Scripts can be deployed at any given time.
7. Automation
    - Background maintenance: Fix issues without disrupting end users or causing downtime.
    - Proactive tasks: Set tasks to trigger automatically when a monitoring check signals a problem.
    - Task automation.
    - Custom scripts built for your needs.
8. Windows Patch Management
    - Critical Microsoft packages—including Office 365, Exchange, SQL Server, Internet Explorer, and Windows OS.
    - Safeguard the network with deep vulnerability scans.
9. Spam Filter

- Protects from phishing, malware, and other email-borne threats, runs a unique combination of antivirus and anti-spam engines to check every incoming, outgoing, and internal email and to quarantine any threats. Additionally, with real-time pattern-based threat recognition, we can detect emerging threats and help you stay protected.
- Maintain Email continuity during an outage. Users can log into their dashboards to send and receive email, even if a business's on-premises or cloud-based mail infrastructure fails.
- Enhanced support for Office 365 because Office 365 is so prevalent, malicious actors frequently try to exploit it.

12. Time to be Included

- **Remote:** First 15 minutes of remote work during normal business hours is free. After the 15 minutes an hour minimum will be charged at the discounted rate.
- **On-site:** One hour minimum charge.
- **Travel Charge:** There will be a discounted travel charge for on-site visits.
- **After Hours & Public Holidays:** All time is billable at their specific rates. Work will only be performed for planned maintenance or upgrades.

13. Special Terms

- **Spam Filter:** One email address per workstation.
- **Automation:** Six or more automatic task executed per Automation Policy will be billed as an hour.

Appendix C
Corporate Platinum

1. Server & Workstation RMM
2. MDM
3. Network Performance Monitoring
4. Managed Antivirus
5. Encrypted Local & Online Server Backup & Recovery
6. Encrypted Online Workstation Backup & Recovery
7. Central Managed Firewall/Router
8. Firewall Security Services
9. Reports
10. Scheduled Task
11. Automation
12. Windows Patch Management
13. 3rd Party Patch Management
14. Driver Updates
15. Email Encryption
16. Spam Filter
17. Remote Access
18. Time to be Included
19. Special Terms

Corporate Platinum Plan Explanations

1. Server & Remote Monitoring and Management

- Automatic notifications about device availability, performance, security, and backup status.
- Health check hardware and software.
- Virtual machine monitoring.
- Proactive Maintenance windows to run during off hours so you don't disrupt employees' productivity or raise false downtime alarms.

2. Mobile Device Management.

- Keep track of smartphones and tablets with mobile device checks and monitoring.
- Detailed security settings on business-owned devices.
- Location tracking protect against device theft and keep track of device locations with reports that leverage the devices' GPS features.
- Ownership details keep track of devices registered to individuals and associated handset details.
- Data usage monitoring help make sure you don't pay extra data usage fines by monitoring data usage on your users' registered devices.
- Remote features: Lock phones, set passwords, or wipe devices
- Configure email and Wi-Fi access on your devices.
- Empower BYOD employees - staff work quicker, more efficiently, more effectively and flexibly using the devices of their choice and providing secure access to company systems and data.

3. Network Performance Monitoring

- SNMP functionality to monitor network devices—including servers, printers, routers, and switches.

- Complete Active Directory monitoring in any Windows network handling issues before they cause greater problems.
- Connection logs: See when devices come online and when they disconnect from the network.
- Additional security: Prevent exposure to unmanaged devices, such as personal devices, that might compromise your network. This keeps your users more secure and allows you to better enforce your customers' bring-your-own-device policies.

4. Managed Antivirus

- Extensive signature-based scanning: Use traditional signature-based threat detection to block known threats.
- Heuristic checks: Protect against previously unknown threats using heuristic checks, which detect new, unrecognized viruses in a sandbox environment away from a business's core systems.
- Active protection and behavioral scanning: Shut down even the most sophisticated malware via continuous real-time monitoring, which detects programs that perform actions commonly associated with malware exploits.
- Lightweight scans to reduce system resource drain.
- Reduces the number of false positives with more accurate scanning.
- Schedule deep scans ahead of time so you don't disrupt employees during important productive hours.
- Control timing: Pause or cancel scans when needed.

5. Encrypted Local & Online Server Backup & Recovery

- Hybrid-cloud backup and recovery.
- Block level, allowing for lightweight and rapid backups. This makes it easier to back up more frequently and improve recovery point objectives, thereby minimizing data loss during a disaster.

- Bare metal protection automatically backs up the entire OS boot up environment, system state, applications, and data so you're prepared for a disaster.
- Continuous recovery: When you can't continuously update a running server, our backup and recovery feature automatically updates the standby server via a restore after each backup session of the live server completes.

6. Encrypted Online Workstation Backup & Recovery
   - Private encryption key: MSP RMM helps ensure that only the private key owner can recover and access data. This prevents any unauthorized access and keeps business data secure.
   - End-to-end encryption: All backups are encrypted on site, then transferred over secure connections until they reach the cloud. Data only gets decrypted during a recovery at the business's site.
7. Central Managed Firewall/Router
   - Automatically updated with newest firmware.
   - Manage all WAP's from one location.
   - Dual WAN.
   - Load balancing.
   - Custom Firewall rules.
   - High availability
   - QoS
   - SSL VPN
   - VLAN
   - PCI-DDS Credit card security.
   - Wireless built in.
   - AC
8. Firewall Security Services
   - Internet Control
   - DNS filter.

- Web content filter.
- IP filter.
- Digital content filter.
- Network level safe searching.

9. Reports
   - Executive summary report display key metrics and support activities in an easy-to-digest, report that showcases all the critical functions performed.
   - Additional reports: A wide variety of additional reports. These reports cover such key areas as device inventory, pricing, antivirus protection, backup integrity, user audits, hardware and software checkups, and more.
   - Custom reports.
10. Scheduled Task
    - Scripts can be deployed at any given time.
11. Automation
    - Background maintenance: Fix issues without disrupting end users or causing downtime.
    - Proactive tasks: Set tasks to trigger automatically when a monitoring check signals a problem.
    - Task automation.
    - Custom scripts built for your needs.
12. Windows Patch Management
    - Critical Microsoft packages—including Office 365, Exchange, SQL Server, Internet Explorer, and Windows OS.
    - Safeguard the network with deep vulnerability scans.
13. 3rd Party Patch Management
    - Wide software support for most standard business software--covers over 80 third-party application families, including Apple, Google, Java, Adobe, zip tools, Skype, Yahoo Messenger, and more.
14. Driver Updates
    - Keep your devices running smooth with up to date drivers.

15. Email Encryption

- In the office or on the road, users easily exchange secure e-mail with anyone, even those outside the organization network. Have the option of direct-to-inbox encrypted delivery, or access via secure portal. No software to download.
- Policies can be configured to scan email content, subject and attachments. Manually encrypt or let the system automatically encrypt for you.
- Protecting financial information isn't option, it is the law. Our email encryption ensures you are in compliance with all email and data security regulations such as HIPAA, PCI, GLBH, CFPB, ALTA BP3, and more. Compliance reports are available upon request as well as email audit trails and delivery reports.

16. Spam Filter

- Protects from phishing, malware, and other email-borne threats, runs a unique combination of antivirus and anti-spam engines to check every incoming, outgoing, and internal email and to quarantine any threats. Additionally, with real-time pattern-based threat recognition, we can detect emerging threats and help you stay protected.
- Maintain Email continuity during an outage. Users can log into their dashboards to send and receive email, even if a business's on-premises or cloud-based mail infrastructure fails.
- Enhanced support for Office 365 because Office 365 is so prevalent, malicious actors frequently try to exploit it.

17. Remote Access

- Remote access to all your devices.
- Customize access for individual users.
- Secure connections: All remote viewing sessions occur over a secure connection and have low impact on bandwidth.
- Easily move, copy, and delete files remotely.

18. Time to be Included

- **Remote:** First 25 minutes of remote work during normal business hours is free. After the 25 minutes an hour minimum will be charged at the discounted rate.
- **On-site:** One hour minimum charge.
- **Travel Charge:** There will be a discounted travel charge for on-site visits.

- **After Hours & Public Holidays:** All time is billable at their specific rates. Work will only be performed for planned maintenance or upgrades.

19. Special Terms

- **Email Encryption:** One email address per workstation.
- **Spam Filter:** One email address per workstation.
- **MDM:** One device per workstation.

Appendix D
Corporate Platinum Premium 24x7

1. Server & Workstation RMM
2. MDM
3. Network Performance Monitoring
4. Managed Antivirus
5. Encrypted Local & Online Server Backup & Recovery
6. Encrypted Online Workstation Backup & Recovery
7. Central Managed Firewall/Router
8. Firewall Security Services
9. Reports
10. Scheduled Task
11. Automation
12. Windows Patch Management
13. 3rd Party Patch Management
14. Driver Updates
15. Email Encryption
16. Spam Filter
17. Remote Access
18. Time to be Included
19. Special Terms

Corporate Platinum Premium 24x7 Plan Explanations

1. Server & Remote Monitoring and Management
    - Automatic notifications about device availability, performance, security, and backup status.
    - Health check hardware and software.
    - Virtual machine monitoring.
    - Proactive Maintenance windows to run during off hours so you don't disrupt employees' productivity or raise false downtime alarms.
2. Mobile Device Management.
    - Keep track of smartphones and tablets with mobile device checks and monitoring.
    - Detailed security settings on business-owned devices.
    - Location tracking protect against device theft and keep track of device locations with reports that leverage the devices' GPS features.
    - Ownership details keep track of devices registered to individuals and associated handset details.
    - Data usage monitoring help make sure you don't pay extra data usage fines by monitoring data usage on your users' registered devices.
    - Remote features: Lock phones, set passwords, or wipe devices
    - Configure email and Wi-Fi access on your devices.
    - Empower BYOD employees - staff work quicker, more efficiently, more effectively and flexibly using the devices of their choice and providing secure access to company systems and data.

3. Network Performance Monitoring
    - SNMP functionality to monitor network devices—including servers, printers, routers, and switches.

- Complete Active Directory monitoring in any Windows network handling issues before they cause greater problems.
- Connection logs: See when devices come online and when they disconnect from the network.
- Additional security: Prevent exposure to unmanaged devices, such as personal devices, that might compromise your network. This keeps your users more secure and allows you to better enforce your customers' bring-your-own-device policies.

4. Managed Antivirus

- Extensive signature-based scanning: Use traditional signature-based threat detection to block known threats.
- Heuristic checks: Protect against previously unknown threats using heuristic checks, which detect new, unrecognized viruses in a sandbox environment away from a business's core systems.
- Active protection and behavioral scanning: Shut down even the most sophisticated malware via continuous real-time monitoring, which detects programs that perform actions commonly associated with malware exploits.
- Lightweight scans to reduce system resource drain.
- Reduces the number of false positives with more accurate scanning.
- Schedule deep scans ahead of time so you don't disrupt employees during important productive hours.
- Control timing: Pause or cancel scans when needed.

5. Encrypted Local & Online Server Backup & Recovery

- Hybrid-cloud backup and recovery.
- Block level, allowing for lightweight and rapid backups. This makes it easier to back up more frequently and improve recovery point objectives, thereby minimizing data loss during a disaster.

- Bare metal protection automatically backs up the entire OS boot up environment, system state, applications, and data so you're prepared for a disaster.
- Continuous recovery: When you can't continuously update a running server, our backup and recovery feature automatically updates the standby server via a restore after each backup session of the live server completes.

6. Encrypted Online Workstation Backup & Recovery
   - Private encryption key: MSP RMM helps ensure that only the private key owner can recover and access data. This prevents any unauthorized access and keeps business data secure.
   - End-to-end encryption: All backups are encrypted on site, then transferred over secure connections until they reach the cloud. Data only gets decrypted during a recovery at the business's site.
7. Central Managed Firewall/Router
   - Automatically updated with newest firmware.
   - Manage all WAP's from one location.
   - Dual WAN.
   - Load balancing.
   - Custom Firewall rules.
   - High availability
   - QoS
   - SSL VPN
   - VLAN
   - PCI-DDS Credit card security.
   - Wireless built in.
   - AC
8. Firewall Security Services
   - Internet Control
   - DNS filter.

- Web content filter.
- IP filter.
- Digital content filter.
- Network level safe searching.

9. Reports
   - Executive summary report display key metrics and support activities in an easy-to-digest, report that showcases all the critical functions performed.
   - Additional reports: A wide variety of additional reports. These reports cover such key areas as device inventory, pricing, antivirus protection, backup integrity, user audits, hardware and software checkups, and more.
   - Custom reports.
10. Scheduled Task
    - Scripts can be deployed at any given time.
11. Automation
    - Background maintenance: Fix issues without disrupting end users or causing downtime.
    - Proactive tasks: Set tasks to trigger automatically when a monitoring check signals a problem.
    - Task automation.
    - Custom scripts built for your needs.
12. Windows Patch Management
    - Critical Microsoft packages—including Office 365, Exchange, SQL Server, Internet Explorer, and Windows OS.
    - Safeguard the network with deep vulnerability scans.
13. 3rd Party Patch Management
    - Wide software support for most standard business software--covers over 80 third-party application families, including Apple, Google, Java, Adobe, zip tools, Skype, Yahoo Messenger, and more.
14. Driver Updates
    - Keep your devices running smooth with up to date drivers.

15. Email Encryption

- In the office or on the road, users easily exchange secure e-mail with anyone, even those outside the organization network. Have the option of direct-to-inbox encrypted delivery, or access via secure portal. No software to download.
- Policies can be configured to scan email content, subject and attachments. Manually encrypt or let the system automatically encrypt for you.
- Protecting financial information isn't option, it is the law. Our email encryption ensures you are in compliance with all email and data security regulations such as HIPAA, PCI, GLBH, CFPB, ALTA BP3, and more. Compliance reports are available upon request as well as email audit trails and delivery reports.

16. Spam Filter

- Protects from phishing, malware, and other email-borne threats, runs a unique combination of antivirus and anti-spam engines to check every incoming, outgoing, and internal email and to quarantine any threats. Additionally, with real-time pattern-based threat recognition, we can detect emerging threats and help you stay protected.
- Maintain Email continuity during an outage. Users can log into their dashboards to send and receive email, even if a business's on-premises or cloud-based mail infrastructure fails.
- Enhanced support for Office 365 because Office 365 is so prevalent, malicious actors frequently try to exploit it.

17. Remote Access

- Remote access to all your devices.
- Customize access for individual users.
- Secure connections: All remote viewing sessions occur over a secure connection and have low impact on bandwidth.
- Easily move, copy, and delete files remotely.

18. Time to be Included

- **Remote:** Time included
- **On-site:** Time included
- **Travel Charge:** There will be a discounted travel charge for on-site visits.

19. Special Terms

- **Email Encryption:** One email address per workstation.

- **Spam Filter:** One email address per workstation.
- **MDM:** One device per workstation.

20. Special Terms

- **Email Encryption:** One email address per workstation.
- **Spam Filter:** One email address per workstation.
- **MDM:** One device per workstation.

Appendix E
Pricing

Call for pricing