Customer Protection Agreement

Revised: June 17, 2019

Thank you for choosing Palmer Technology Solutions as your IT provider.

PTS customer network environments with the most success have an in-house Network Administrator or someone who fills that role. PTS provides them high-level support and acts as their backup. The in-house Network Administrator and your company's points of contacts with PTS should follow this CPA in order to get the best service from PTS. Please visit the links below updates to the CPA and TAC.

For the most current version of Terms and Conditions (TAC), please visit http://www.palmerts.com/tac.pdf. For the most current version of the Customer Protection Agreement (CPA), please visit http://www.palmerts.com/cpa.pdf

This Customer Protection Agreement establishes the default level of service provided and the PTS standard operational recommendations between our companies. Changes or additions to this level of service will require a Service Level Agreement (SLA) with the detail of specific service requirements necessary.

PTS Offers

- **Service Level Agreements (SLA)**
  - Rollover SLA
  - Discounted SLA
  - Unlimited Business Hours SLA
  - Recommended Maintenance SLA
- **Proactive Monitoring and Maintenance (PMM)**
- **Managed Backup**
  - Onsite and Offsite
- **Managed Network Security**
  - Firewall
  - Redundant internet
- **Licenses**
  - Microsoft Office 365, Server and Users
  - Antivirus
  - Antimalware

206 West Rhapsody San Antonio, Texas 78216
(210) 341-4806 (210) 341-4930 Fax

- **Managed Email Filtering (PEQ)**
    - Inbound Email Filtering and Virus protection
    - Outbound Email Filtering (PEQ)
    - Outbound Email Encryption
- **Cloud & On-Site Server Hosting**
- **Phone System Hosting**
    - Phone system and maintenance
- **Break Fix**

Customer Web Portal

The customer portal will allow you to access your tickets, create tickets, review invoices, agreements, recommendations, and create and maintain your company's users to the portal.

Web link: https://connect.palmerts.com/support

Please contact Customer Service for your username and password by emailing customerservice@palmerts.com or calling 210-341-4806 and pressing 2.

Proactive Monitoring and Maintenance (PMM) Web Portal

Your in-house Network Administrator can access all your network devices using our PMM Web Portal. This will allow them to perform service on your network and save you money.

Please contact PTS for this link.

Service and Scheduling

- PTS normal business hours are Monday thru Friday from 8 am to 5 pm.
- All requests for service are emailed to support@palmerts.com or by calling 210-341-4806 and pressing 1.
- Non-emergency requests for service received after 3:00 pm will be scheduled for the following business day.
    - It is an Emergency (appropriate rates will apply)
    - You have a SLA Agreement

Emergencies after Hours

- If you have an After Hours Emergency, call our office at 210-341-4806 and press 9 to be connected to our on-call technicians. Please be patient and do not hang up; a technician will answer the phone.

Additional Services or Sales

- For additional Managed Services, Service Level Agreements or product contact Customer Service during Business Hours at 210-341-4806 and press 2 or email customerservice@palmerts.com.

Palmer Technology Solutions
206 West Rhapsody San Antonio, Texas 78216
(210) 341-4806 (210) 341-4930 Fax

Accounting

- Contact accounting during Business Hours at 210-341-4806 and press 3 or email accounting@palmerts.com.

Second Time Rule

- If you are experiencing an issue more than once, please notify us. To escalate your ticket add "Second Time" to the subject of your email to support@palmerts.com.

Survey

- Every service ticket sent to you with "Complete Follow-up" in the subject has a link to a customer survey. Please complete the survey from time to time so we can improve.

Canceling service requests

- Customers are required to contact PTS via email to support@palmerts.com or call the office at 210-341-4806 at least (2) hours prior to the scheduled time for onsite service calls.

Quotes

- Normal turnaround time for a quote is within three business days; however, large quotes may take up to 10 business days, and your PTS Customer Service rep will inform you if more time is required.
- You can electronically sign or fax to 210-341-4930 quotes.
  If you choose to fax in a signed quote, please send all the original pages.
- PTS prefers to deliver complicated quotes to customers in person.

Purchasing

- For New/COD customers and for customers where the order will exceed the credit limit PTS requires a 50% deposit.
- For products that are nonrefundable, full payment of the product may be required.
- A restocking fee may apply for some returns.
- Normal delivery is 7-10 business days

Information Technology Policies

PTS recommends that every company using technology have the following:

- Employee Electronic Policy (Deliverable)
- IT Electronic Policy (Deliverable)
- Internet Usage Policy
- Password Policy
- Disaster Recovery Plan
- Network Diagram
- Backup and Recovery Plan
- User IT On-Boarding and Off-boarding Policies and Procedures (Deliverable)

If you would like PTS to help you create these policies or give you a templates/deliverables to create your own policies please email your request to customerservice@palmerts.com .

Customer Responsibilities

- Our most successful customers manage costs by filtering all service requests through a single point of contact at their office. PTS recommends the in-house Network Administrator or your company primary point of contact to PTS.

Palmer Technology Solutions
206 West Rhapsody San Antonio, Texas 78216
(210) 341-4806 (210) 341-4930 Fax

- The customer's in-house Network Administrator will be required to know the master passwords in order to perform maintenance.
- Do not allow users to have administrator rights assigned to their user logins.

Daily network management not provided by PTS without SLA

  - Local user and device management
  - User and group folder and file security
  - Anti-virus management
  - Patching management
  - Password management
  - Reviewing and remediating reports and alerting from PTS
  - Notify PTS If your reports and alerts are not being received.

- Keep all computers on all the time to allow PTS to perform maintenance and monitoring (PMM)
- **Keep PTS informed of all IT changes and IT planning with other vendors**
- If you do not receive reports for PTS weekly, notify PTS
- Approve PTS Service Tickets for work to be performed
- Primary contact or user must be available to work with the PTS Technicians to verify that correct and accurate information of the issue can be gathered to resolve the issue and to verify that the issue has been resolved.
- To ensure satisfaction, check the work performed by the PTS Technician while the technician is still onsite or on the phone.
- If the primary point of contact or the end user is unable to check the work performed, another billable service call may be required.
- Work with PTS Technicians and Customer Service to determine the best solution based on your company's needs.
- **Assist PTS Technicians and Customer Service in working with your third party vendors.**
- Maintain support, updates and upgrades for all your third party applications.
- Insure your hardware warranties do not expire.
- Insure your operating systems do not End of Life.
- If access to the network is required by, a third party have PTS Technicians give them and disable their access.
- The PTS Technicians will be responsible to you for your satisfaction of the work performed. If you have any problems with our service, please notify techmanager@palmerts.com.
- Sign and return Service Work Approval Form via E-mail, Verbally or Digital Signature to customerservice@palmerts.com
- Sign and return Customer Approval and Contact Information Form to customerservice@palmerts.com
- Sign and return Credit Application to accounting@palmerts.com

***PTS is not responsible for any service disruptions or any outages caused by 3rd party vendors or personnel outside of PTS that have not been pre-approved by PTS ***

PTS Responsibilities

Palmer Technology Solutions
206 West Rhapsody San Antonio, Texas 78216
(210) 341-4806 (210) 341-4930 Fax

- Technicians at PTS are part of a team. PTS technicians consult with each other to solve your IT problems in a timely fashion. Because of this, PTS Technicians will be on their cell phones while at your site. If a technician is unable to perform work for you while they are assisting another technician, they are required stop billing you until they can get back to your problem.
- As part of the service call, the PTS technician will complete the Service Ticket and update your records while onsite and get your approval on the work completed.
- All PTS Technicians are required to acquire and maintain technical certifications.
- PTS technicians will inform you, verbally and by email, of proactive ways to improve your network.
- PTS Technicians follow a second time rule. If the technician is working on the same problem twice, they are required to communicate with PTS Technician Manager and the Primary Point of contact prior to the second appointment. The communication will be verbal and by email. The communication will explain the path and timeframe for resolution to the problem. Management or another PTS technician may assist with a resolution.
- The Primary Point of Contact will be emailed the service ticket at the end of the service call.

PTS Recommendations

Recommended Maintenance

- PTS technicians will create tickets of recommended maintenance to proactively improve your network
- PTS has reoccurring recommended maintenance Service Level Agreement.
- Approvals for recommended maintenance will be sent with the classification of **Critical** or **Non Critical**
    - **Critical Maintenance** means if the ticket is not approved there will be possible outages, unexpected downtime or data loss
    - **Non Critical Maintenance** means if the ticket is not approved there will most likely not be outages, unexpected downtime or data loss

Minimum Backup Standards

- Perform daily backups of all Operating Systems, data and programs
- Store backups on-site and off-site
- Monitor backups daily
- Monitor backups weekly through reporting

Anti-Virus and threat Protection Standards

- Purchase and install Anti-virus and Anti-Spyware protection on all computers, servers, mobile devices and routers
- Purchase and install a firewall with Anti-virus, Anti-Malware and Intrusion protection.
- Purchase and install an email filter to remove viruses and threats from email.
- PTS recommends that all end users are trained on how to respond to viruses, Phishing etc.

Palmer Technology Solutions
206 West Rhapsody San Antonio, Texas 78216
(210) 341-4806 (210) 341-4930 Fax

- PTS recommends that all end users are trained on company Electronic Policies.

Password Policy

- The name of the administrator user on a server or workstation should never be admin or administrator. PTS recommends that a modified administrator username be used. For example, the admin user name for XYZ Company could be xyzadmin.
- The password for the XYZadmin user should be a minimum of 15 characters in length and be complex in nature. The password should also change regularly. Password complexity rules should be enforced to include upper case letters, lower case letters, numbers and characters (such as ! or @) in the password.
- If an administrator user account has been compromised, notify PTS immediately.

User Passwords

- Do not keep a written list or file stored of user passwords.
- Users should not login to the server or workstations with administrator rights.

All users except administrators

- Passwords will be forced to change every 90 days
- Passwords will be a minimum of 10 characters with complexity rules of uppercase letters, lowercase letters, numbers and characters such as ! or @.
- Do not use sequential letters or numbers such as AaBb or 123
- Do not use the same passwords by not allowing a password less than the 5 previous passwords to be reused.
- Force a password change after a user's password has been reset by the administrator,
- Force a User account to be locked out after 5 failed attempts to login.

Software and Application account Logins and Passwords

- Create unique users accounts and passwords for software and application with only the required permissions.

Palmer Technology Solutions
206 West Rhapsody San Antonio, Texas 78216
(210) 341-4806 (210) 341-4930 Fax