Title of Bid: Family Arena Point of Sale System with Touchscreens and Handhelds

Bid #: IFB 19-130

Dept.: Family Arena

Contact Person: Bob Schnur

Ext.: 3924

Description (product/service, justification and use):

The Family Arena requires a new Micros or comparable hardware and software solution for a POS System, event management, inventory control and suites management for food service operations. The new system will require an upgrade from our current Tangent POS Back Office application to a Micros or comparable solution. The new system needs to include design, coordination, supply, installation, testing, training and yearly maintenance.

Additional benefits of upgrading our current system will be increased speed of service in concessions and merchandise stands. Faster turnaround on transactions will enable us to serve more guests per minute, reducing their time away from the event. This upgrade will also allow us to replace the current manual order-taking system. Our current system requires orders to be hand-delivered to the kitchen requiring servers to make multiple trips for a single order. The new system is tablet-based that is linked via wifi to the kitchen, allowing servers to enter orders remotely and consolidating order deliveries to suites. Less time will be needed per order placed which will enhance the likelihood of re-orders during the event. The current system also requires Suite Captains to take the guest's form of payment back to the kitchen. The new system will allow payment to be made in the suite.

Cost for the new system is $107,321.80 which includes all hardware, software, 12 month warranty, Installation, training, go-live support and one month of Software as a Service (SaaS). The remaining 11 months of SaaS for the first year is $29,403.00 for a total bid award of $136,724.80. Each additional year of SaaS is $32,076 annually ($2,673.00 per month).

Award to: DCRS

Location: 2605 Metro Blvd., St. Louis, MO 63043

Price: $136,724.80

Contract term (if applicable): No term listed-monthly SaaS will remain same throughout use

Bid opening held on: October 16, 2019 at 10AM

Opened by: Finance Department

Account number to be charged for purchase: 5213600-47500

If bid was not awarded to lowest bidder, please explain:

If paying for with grant funds, please indicate (1) grant name, (2) total grant amount, (3) what portion of purchase is being paid for by a grant, and (4) when grant period ends as applicable:
FORMAL BID – REQUEST FOR APPROVAL

Bid #: IFB 19-130

Additional Bids Received

The following additional bids were received:

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Location</th>
<th>Price</th>
<th>Meets all specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Squirrel</td>
<td>8585 Baxter Place, Burnaby, British Columbia</td>
<td>$225,187.00</td>
<td>Yes</td>
</tr>
<tr>
<td>Lightspeed</td>
<td>Olympia, WA</td>
<td>No Response</td>
<td>No</td>
</tr>
<tr>
<td>Cash Control Business Systems</td>
<td>Overland, MO</td>
<td>No Response</td>
<td>No</td>
</tr>
<tr>
<td>Tablecrunch</td>
<td>St. Louis, MO</td>
<td>No Response</td>
<td>No</td>
</tr>
<tr>
<td>Salesforce</td>
<td>San Francisco, CA</td>
<td>No Response</td>
<td>No</td>
</tr>
<tr>
<td>Fiserv</td>
<td>Brookfield, WI</td>
<td>No Response</td>
<td>No</td>
</tr>
</tbody>
</table>

For each vendor that doesn’t meet specifications, please explain why:

Vendor: 

Vendor: 

☐ Sole source justification memos from (1) dept. and (2) vendor attached.

Department Director/Elected Official must sign the request prior to routing to the Purchasing Manager.

[Signature]
Department Director/Elected Official Signature  2-18-20
Date

Approval or Concurrence of Director of Finance  Date

BELOW ONLY TO BE COMPLETED FOR BIDS AT LEAST $15,000 AND LESS THAN $50,000. See instructions at the top of pg. 1.

Director of Administration Signature  Date
# SALES ORDER AGREEMENT

**Family Arena**

2002 Arena Parkway

St. Charles, MO 63303-0009

536-898-4200

**Quote #:** DMQ8111

**Sales Order #:**

**Date:** 10/10/2019

**Expires:** 11/12/2019

**PO #:**

**Sales Rep:** Danny McCarthy

<table>
<thead>
<tr>
<th>Item</th>
<th>QTY</th>
<th>Item Number</th>
<th>Description</th>
<th>Unit Price</th>
<th>Extended Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>TOAST</td>
<td>TOAST</td>
<td>$0.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>Toast:SaaS-1st</td>
<td>1st Device-Monthly Toast Software as a Service (SaaS) Subscription</td>
<td>$120.00</td>
<td>$120.00</td>
</tr>
<tr>
<td>3</td>
<td>65</td>
<td>Toast:SaaS-2+</td>
<td>Additional Device-Monthly Toast Software as a Service (SaaS) Subscription</td>
<td>$30.00</td>
<td>$3,900.00</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>Toast:SaaS KDS</td>
<td>KDS-Monthly Toast Software as a Service (SaaS) Subscription, per device</td>
<td>$25.00</td>
<td>$25.00</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>Toast:SaaS Inventory</td>
<td>Inventory-Monthly Toast Software as a Service (SaaS) Subscription, per site</td>
<td>$75.00</td>
<td>$75.00</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>CSnotax</td>
<td>CUSTOMER SATISFACTION DISCOUNT (Non-Taxable)</td>
<td>($1,447.00)</td>
<td>($1,447.00)</td>
</tr>
<tr>
<td>7</td>
<td>60</td>
<td>BS: E277419</td>
<td>Toast ELO 10&quot; Tablet Terminal 2GB ROM, 16GB RAM</td>
<td>$710.00</td>
<td>$42,600.00</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>BS: E911675</td>
<td>Toast ELO 22&quot; KDS Touchscreen 2G RAM 16GB RAM</td>
<td>$1,290.00</td>
<td>$1,290.00</td>
</tr>
<tr>
<td>9</td>
<td>60</td>
<td>Toast: EMV Reader EDynano</td>
<td>EDynano EMV Reader (with Mounting Kit)</td>
<td>$300.00</td>
<td>$18,000.00</td>
</tr>
<tr>
<td>10</td>
<td>60</td>
<td>BS: 185-00194</td>
<td>Toast Flip stand for 10&quot; or 15&quot; ELO</td>
<td>$110.00</td>
<td>$6,600.00</td>
</tr>
<tr>
<td>11</td>
<td>6</td>
<td>Toast: GoPay-6</td>
<td>Toast GoPay at the Table 6&quot; HH Tablet: Encrypted MSR, Case (Manufacturer warranty repair only)</td>
<td>$300.00</td>
<td>$3,000.00</td>
</tr>
<tr>
<td>12</td>
<td>24</td>
<td>EPS-C31CD52A9912</td>
<td>Thermal Receipt: Epson T20II IP Ethernet, 6&quot; IP Cable</td>
<td>$349.00</td>
<td>$8,376.00</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>EPS-C31CG51A8041</td>
<td>Impact Autocut Remote: Epson U220 IP Ethernet, ADD CABLE</td>
<td>$399.00</td>
<td>$399.00</td>
</tr>
<tr>
<td>14</td>
<td>60</td>
<td>APG-VB320-1616</td>
<td>APG Cash Drawer: 5-bill, 10-coin, 18&quot;Wx16.7&quot;Dx14&quot;H REOs Printer &amp; CD-101A CABLE KIT</td>
<td>$199.00</td>
<td>$11,940.00</td>
</tr>
<tr>
<td>15</td>
<td>60</td>
<td>CD-101A</td>
<td>Cable for APG Cash Drawer</td>
<td>$0.00</td>
<td>$540.00</td>
</tr>
<tr>
<td>16</td>
<td>1</td>
<td>ML10B</td>
<td>LCD Monitor Wall Mount, up to 33ibs, 90 degree tilt, 14&quot; max extension (ALL POS-VEAS)</td>
<td>$55.00</td>
<td>$55.00</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>Toast:mc_20</td>
<td>Magnetic Stripe Cards, Encoded, Toast Employee: SET of 20</td>
<td>$28.00</td>
<td>$28.00</td>
</tr>
<tr>
<td>18</td>
<td>1</td>
<td>FreightIN</td>
<td>Freight INBOUND (FOB Origin): Freight to St. Louis</td>
<td>$5,356.00</td>
<td>$5,356.00</td>
</tr>
<tr>
<td>19</td>
<td>1</td>
<td>DISCOUNT</td>
<td>Special Discount</td>
<td>($14,020.20)</td>
<td>($14,020.20)</td>
</tr>
<tr>
<td>20</td>
<td>1</td>
<td>SERVICE-PPM</td>
<td>SERVICES: PREPARATION &amp; PROJECT MANAGEMENT</td>
<td>$19,845.00</td>
<td>$19,845.00</td>
</tr>
<tr>
<td>21</td>
<td>1</td>
<td>WARR-DIRECT</td>
<td>*WARRANTY: 12-Mo MANUFACTURER DIRECT DEPOT REPAIR ONLY</td>
<td>$0.00</td>
<td>$0.00</td>
</tr>
<tr>
<td>22</td>
<td>1</td>
<td>WD1</td>
<td><em>WARRANTY: 12-Mo DEPOT HARDWARE REPAIR, DCRS St. Louis (Ship/Carry-in)</em></td>
<td>$0.00</td>
<td>$0.00</td>
</tr>
</tbody>
</table>
Hardware Configuration
(20) 10" Terminals with EMV readers
(6) Toast Go Handhelds
(24) Thermal Receipt Printers
(69) APG Cash Drawers
(1) 22" ELO - KDS
(1) Impact printer

12 month manufacturer warranty on Toast Go handhelds
12 month depot warranty on all other hardware.
Includes 15% hardware discount - $14020.20

DCRS to use Family Arena networking equipment - patch cables, wireless access points, firewall and switch

Labor includes:
- On-Site Planning Meeting
- Programming
- Database Review
- Full Training
- Full Installation
- Go-Live Support

<table>
<thead>
<tr>
<th>Requested Delivery Date</th>
<th>Installer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Subtotal

<table>
<thead>
<tr>
<th>Taxable Items</th>
<th>$107,321.60</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subtotal</td>
<td>$107,321.60</td>
</tr>
<tr>
<td>Total Cash Price</td>
<td>$107,321.60</td>
</tr>
</tbody>
</table>

Received $ __________ on __________ as cash with order

Signature of
Account Manager

Balance of contract to be paid in the following manner:

Down Payment

Balance Due on Delivery

The Additional Terms and Conditions printed on the last 2 pages of the DCRS Sales Order Agreement are part of this Agreement. Customer acknowledges he or she has read this Agreement, including the Additional Terms and Conditions, and understands and agrees to all terms and conditions stated herein.

ACCEPTED BY: DCRS SOLUTIONS INC. (DCRS)  
(DISTRIBUTOR)

ACCEPTED BY: ____________________________
(CUSTOMER'S NAME)

AUTHORIZED SIGNATURE:

TITLE:

DATE:  

AUTHORIZED SIGNATURE:

TITLE:

DATE:
1. PRICE. Hardware, Software and/or Cloud Software as a Service, and Services, are sometimes collectively referred to as "System" herein. Customer agrees to pay the purchase price for System on the Date of Physical Delivery, unless otherwise stated herein. Customer's copier(s) shall apply against the purchase price of System. The prices shown are F.O.B. Maryland Heights, Missouri. All transportation, insurance, license fees, and other such charges shall be paid by Customer. There shall be added to the prices shown and Customer agrees to pay the amount of any taxes resulting from this Agreement or any Sales Orders hereunder, exclusive, however, of taxes based upon net income of Distributor. If no taxes are shown on this Agreement, Customer remains responsible for any payment of pertinent sales and use taxes. Any personal property taxes assessed on System after delivery to the carrier shall be borne by the Customer. Sales Orders canceled or not accepted for delivery within 12 months are subject to a minimum restocking fee of 25% of the purchase price of Hardware and a minimum cancellation fee of 100% of the non-returnable purchase price of Software and/or Cloud Software as a Service.

2. TITLES AND SECURITY INTEREST. CUSTOMER ACKNOWLEDGES AND ACCEPTS THE ADDITIONAL TERMS AND CONDITIONS, AS SET FORTH IN ANY SEPARATE SOFTWARE LICENSE AND/OR CLOUD SERVICE AGREEMENT(S) REQUIRED BY THE SOFTWARE MANUFACTURER, PRIOR TO TIME OF ORDER BY DISTRIBUTOR. DISTRIBUTOR shall transfer title to System, and license rights to any unauthorized software to Customer upon delivery and at such time Distributor shall have a purchase money security interest in System, including all additions and replacements thereto, and proceeds thereof, to secure performance of all of such obligations of Customer. Customer agrees promptly upon demand to execute any financing statement, applications for registration and like documents to take any other action deemed necessary or desirable by Distributor in order to perfect Distributor's security interest hereunder. Customer hereby appoints Distributor as Customer's limited attorney-in-fact to prepare, sign and file or record for Customer, in Customer's name, any such documents. Customer shall insure and keep System in good order and repair until the purchase price has been paid in full and shall promptly pay all tax and assessments upon System or use of System.

3. RISK OF LOSS. Risk of loss or damage to System shall pass to Customer upon delivery of System to the carrier (regardless of whether the purchase price has been paid in full). Unless otherwise advised by Customer, Distributor may insure to full value System shipped or declare full value thereof to the carrier at the time of delivery to the carrier and all such insurance costs shall be for Customer's account. Conflagration or destruction of, or damage to, System shall not in any way affect the liability of Customer to pay the purchase price in full. Customer shall inspect System immediately upon delivery, and shall notify Distributor immediately in writing of all defects in System, including but not limited to defective materials, defective workmanship or that System is not in good working order. Customer shall immediately file claims with the carrier thereon when there is evidence of shipping damage. Customer's failure to so notify Distributor or file claims with the carrier shall be conclusive evidence that no such defects or damages existed upon delivery.

4. CUSTOMER RESPONSIBILITIES AND ACCEPTANCE. Customer shall be responsible for site preparation including, but not limited to, adequate electrical power, and working space for Distributor's personnel to perform installation services, if specified, and provide a suitable environment for System. Customer shall be responsible for network cabling except as specifically set forth herein to be provided by Distributor. System shall be deemed accepted by Customer when System has been physically delivered if Distributor's installation services have not been specified. If Distributor's installation services have been specified, System shall be deemed accepted by Customer when System has been installed and made ready for use at the Customer's site in accordance with the manufacturer's installation and operational specifications; and the Distributor has tested to insure that all included hardware and software substantially meet the manufacturer's specifications or those contained in this Agreement. Provided that the Customer has entered into and is then covered by a support plan, Customer will allow Remote Access to Distributor support personnel at will, to perform tasks necessary to execute the support plan, unless otherwise specified by the Customer.

WARRANTIES AND LIMITATION OF LIABILITY. DISTRIBUTOR WARRANTS THAT SYSTEM WILL BE IN GOOD WORKING ORDER AND WILL INFORM TO MANUFACTURER'S PUBLISHED SPECIFICATIONS, IF ANY, ON THE DATE OF PHYSICAL DELIVERY (OR DATE OF INSTALLATION, IF SERVICES ARE PROVIDED BY DISTRIBUTOR, AS DEFINED IN SECTION 4) AND FOR NINETY (90) DAYS THEREAFTER. HARDWARE COVERED BY THE MANUFACTURER'S WARRANTIES IS HEREBY ASSIGNED DIRECTLY TO CUSTOMER. EACH MANUFACTURER'S WARRANTY CLAIM PROCEDURE MUST BE FOLLOWED WHEN A DEFECT APPEARS IN ANY OF THOSE ITEMS. ADDITIONAL PROTECTION IS AVAILABLE ONLY PURSUANT TO THE TERMS AND CONDITIONS OF DISTRIBUTOR'S THEN CURRENT DOCUMENT ENTITLED CUSTOMER SUPPORT USER'S GUIDE LOCATED AT HTTP://WWW.DCRS.COM/SERVICES FOR HARDWARE REPAIR AND/OR SOFTWARE SUPPORT OF THE SYSTEM PURCHASED FROM DISTRIBUTOR. DISTRIBUTOR'S OBLIGATIONS HEREUNDER SHALL BE LIMITED SOLELY TO DISTRIBUTOR MAKING, AT DISTRIBUTOR'S COST AND EXPENSE, SUCH REPAIRS AND REPLACEMENTS AS ARE NECESSARY TO PUT SYSTEM IN GOOD WORKING ORDER AND TO CONFORM SYSTEM TO MANUFACTURER'S PUBLISHED SPECIFICATIONS, IF ANY, EXCLUDING REPAIR OR REPLACEMENT OF PHYSICAL DAMAGE CAUSED TO DISTRIBUTOR'S EQUIPMENT OR HARDWARE RESULTING FROM CUSTOMER'S FAILURE TO ATTAIN COMPLIANCE WITH THE PAYMENT CARD INDUSTRY (PCI) PAYMENT APPLICATION DATA SECURITY STANDARD (PA-DSS), LOSS OF USE OF SYSTEM, LOST OR CORRUPTED DATA, THEFT OF DATA, DATA LOSSES, THE AT WILL DISTRIBUTOR'S USE OF REMOTE ACCESS TO PERFORM TASKS NECESSARY TO PROVIDE SUPPORT, OR FOR ANY CLAIM OR CLAIM AGAINST THE CUSTOMER BY ANY OTHER PARTY, DISTRIBUTOR'S LIABILITY UNDER THIS AGREEMENT, INCLUDING DISTRIBUTOR'S LIABILITY FOR LOSS AFTER REPEATED EFFORTS TO INSTALL SYSTEM IN GOOD WORKING ORDER OR TO REPAIR OR REPLACE IN ACCORDANCE WITH THE WARRANTY IN SECTION 5, SHALL IN NO EVENT EXCEED THE PURCHASE PRICE OF SYSTEM.

LIMITATION OF LIABILITY. CUSTOMER AGREES THAT SYSTEM HAS BEEN SELECTED BY CUSTOMER AND IS OF A DESIGN, SIZE, FITNESS AND CAPACITY SELECTED BY CUSTOMER AND THAT CUSTOMER IS SATISFIED THAT THE SAME IS SUITABLE AND FIT FOR CUSTOMER'S PURPOSE. CUSTOMER HEREBY WAIVES ANY CLAIM CUSTOMER MAY HAVE AGAINST DISTRIBUTOR FOR ANY LOSS, DAMAGE, OR EXPENSE OF ANY KIND WHATSOEVER CAUSED BY SYSTEM OR BY ANY DEFECT THEREIN, THE USE OR MAINTENANCE THEREOF, OR ANY SERVICING OR ADJUSTMENT THERETO, NOT EXPRESSLY COVERED BY THE WARRANTY CONTAINED IN THIS AGREEMENT. CUSTOMER FURTHER AGREES THAT DISTRIBUTOR WILL NOT BE LIABLE, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT OR IN TORT INCLUDING NEGLIGENCE, FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL OR SPECIAL DAMAGES ARISING UNDER ANY DOCUMENT, DAMAGES ARISING FROM CUSTOMER'S FAILURE TO ATTAIN COMPLIANCE WITH THE PAYMENT CARD INDUSTRY (PCI) PAYMENT APPLICATION DATA SECURITY STANDARD (PA-DSS), LOSS OF USE OF SYSTEM, LOST OR CORRUPTED DATA, THEFT OF DATA, DATA LOSSES, THE AT WILL DISTRIBUTOR'S USE OF REMOTE ACCESS TO PERFORM TASKS NECESSARY TO PROVIDE SUPPORT, OR FOR ANY CLAIM OR CLAIM AGAINST THE CUSTOMER BY ANY OTHER PARTY, DISTRIBUTOR'S LIABILITY UNDER THIS AGREEMENT, INCLUDING DISTRIBUTOR'S LIABILITY FOR LOSS AFTER REPEATED EFFORTS TO INSTALL SYSTEM IN GOOD WORKING ORDER OR TO REPAIR OR REPLACE IN ACCORDANCE WITH THE WARRANTY IN SECTION 5, SHALL IN NO EVENT EXCEED THE PURCHASE PRICE OF SYSTEM.

7. SECURITY, MALWARE AND PCI COMPLIANCE. Customer acknowledges that the security and protection of System and data, including protections against unauthorized access, and attaining and maintaining compliance with the PAYMENT CARD INDUSTRY (PCI) PAYMENT APPLICATION DATA SECURITY STANDARD (PA-DSS), is solely the responsibility of the Customer. If the Customer's System has persistent connections to the Internet, or allows access to or from the Internet, or uses persistent connections to any network where there is potential unauthorized access, Customer is solely responsible for security. Customer must secure and maintain secure and malware and spyware protection software, which may include, but is not limited to firewalls, passwords, physical security, access control policies, and the like. Customer acknowledges that, to be effective, malware protection and other security software require periodic updates, which Customer must obtain from Customer's supplier or the manufacturer. Distributor disclaims any warranty, express or implied, that, after the initial installation by Distributor of System, the System's data or system will remain malware-free and secure. Support or services necessitated by computer malware, or by any failure or breach of Customer's security to Customer's System or data, including, without limitation, any failure or breach of Customer's security to Customer's System or data, including, without

Page 3 of 4
8. REMEDIES UPON DEFAULT. Failure of Customer to perform its obligations hereunder including, without limitation, payment in full of the purchase price for System, or the insolvency, filing of any voluntary or involuntary petition of bankruptcy, assignment for the benefit of creditors or dissolution, liquidation, or winding up of the business of Customer shall constitute a default under this Agreement, and shall afford Distributor all other remedies of a secured party under the Uniform Commercial Code of the State of Missouri. Distributor may, in addition to any other remedies, which Distributor may have, refuse to provide service or support to System under any support plan agreed to relating to the System in effect between Distributor and Customer at the time of Customer's default. Failure of Distributor to exercise any rights under this Agreement shall not constitute a waiver of such right. Default by Customer in the performance of any of its obligations hereunder shall, at Distributor's option, render the total purchase price and all other obligations at once due and payable.

9. INABILITY TO PERFORM. Distributor shall not be required to perform Distributor's obligations under this Agreement, or be liable for Distributor's failure to perform or for delay in performance of Distributor's obligations hereunder if such performance is prevented, hindered or delayed by reason of any cause beyond the reasonable control of Distributor, including without limitation, any labor dispute, act of God, or regulation or order of any government authority.

10. NON-SOLICITATION/NON-HIRER. Customer agrees not to solicit, hire or otherwise engage in any manner whatsoever, directly or indirectly, any of the Distributor's employees from the date of this Agreement and for a period of two years thereafter. If the Customer violates this provision, the Customer shall pay the Distributor the sum of one year's direct salary of each employee hired or engaged as liquidated damages and not as a penalty.

11. ASSIGNMENT. This Agreement is not assignable by Customer without written permission from Distributor and any attempt by Customer to assign any rights, duties or obligations, which arise under this Agreement without such permission, shall be void. The System shall not be sold, leased, pledged or otherwise transferred or encumbered by Customer until all Customers' obligations hereunder have been satisfied.

12. ENFORCEMENT COSTS. Customer agrees to pay to Distributor any reasonable attorneys' fees and other costs and expenses incurred by Distributor in connection with the enforcement of this Agreement. All past due obligations of Customer shall bear interest at the rate of 1.5% per month or, if such rate be unlawful, at the highest lawful rate.

13. GOVERNING LAW. This Agreement shall be governed by the laws of the State of Missouri applicable to contracts entered into and to be performed within the State of Missouri.

14. VALIDITY OF AGREEMENT. If any provision or provisions of this Agreement shall be held to be invalid, illegal or unenforceable, the remainder of the Agreement shall not be affected or impaired thereby.

15. MISCELLANEOUS. This Agreement constitutes the complete and exclusive statement of the agreement between the parties and supersedes all proposals, oral or written, and all other communications between the parties relating to the subject matter of the Agreement.

Customer represents that Customer is not relying on any oral or written representations or warranties not contained in this written Agreement. In the event that Customer uses Customer's purchase order form in connection with the ordering of the System, such order will be governed by the terms of this Agreement and any provision of such order form, which in any manner differs from or is in addition to the provision of this Agreement shall be of no force or effect. Distributor's acceptance of such order is expressly made conditional on Customer's assent to the terms of this Agreement. Any acknowledgment by Customer of this Agreement shall be limited to the terms of this Agreement, and any provision in such acknowledgment, which in any manner differs from or is in addition to the provisions of this Agreement, shall be of no force or effect.

This Agreement may only be amended in writing, executed by an officer of Distributor and an officer of Customer.

The paragraph captions of these additional terms and conditions are for reference only, do not constitute a part of this Agreement and shall not be used to construe it.

All notices required pursuant to this Agreement and the Uniform Commercial Code of Missouri shall be in writing and shall be deemed to be duly given only if personally delivered or mailed by certified mail, to the parties hereto at their addresses as shown herein or at such other address as shall be designated in writing. Notices shall be effective upon delivery or mailing.

CUSTOMER ACKNOWLEDGES THAT IT HAS READ THIS AGREEMENT, AND UNDERSTANDS AND AGREES TO ALL TERMS AND CONDITIONS STATED HEREIN.

CUSTOMER'S SIGNATURE

VERSON 102715
LEGAL NOTICE

INVITATION FOR FORMAL BID
IFB 19-130

For

Point-of-Sale System with Touchscreens and Handhelds

For

ST. CHARLES COUNTY GOVERNMENT
ST. CHARLES, MISSOURI

The St Charles County Family Arena requires a Micros or comparable hardware and software solution for a POS system, event management, inventory control, and suites management for food service operations. The vendor must guarantee the quoted prices for a period of one year. The county reserves the right to terminate the contract for any violation, by the successful bidder, of any term or condition of the contract by giving thirty (30) days written notice stating the reasons therefore and giving the party time to remedy any deficiencies. All bid prices submitted must be guaranteed for ninety (90) days.
BID INSTRUCTIONS

One (1) signed original and one (1) signed copy of the bid must be received in a sealed envelope plainly marked with the title, date and time of the bid opening in the lower left corner of the envelope.

An authorized representative of the company/person submitting the bid must sign the bid, in blue ink.

Bids must be submitted to the St. Charles County Finance Department, 201 North Second Street, Room 541, St. Charles, MO 63301 prior to the bid opening.

Bid opening will be on 10/16/2019 at 10:00 AM, in Room 534 of the St. Charles County Administration Building, 201 North Second Street, St. Charles, MO 63301.

St. Charles County reserves the right to accept and/or reject any and all bids.

Bid results may be obtained by going to our St Charles County Government website @ http://www.sccmo.org/Bids.aspx click on “show Closed/Awarded/Cancelled bids”, select bid and click on “related documents”. No phone calls please. The time it takes for final bid results to be made public depends on the complexity of the project and the cost of the project.

BID INQUIRIES

All questions or clarifications concerning this Request for Bid must be submitted in writing via E-mail (preferred), mail or fax to:

Pam Luesse
St. Charles County Government
201 North Second Street, Room 541
St. Charles, MO 63301
pluesse@sccmo.org

For questions or Inquiries concerning the specifications please contact:
Elizabeth Silbert, Suites and Club Sales Manager
St. Charles County Family Arena
2002 Arena Parkway
St. Charles, Missouri 63303
Fax: (636)896-4205
esilbert@familyarena.com

- The bid number and title shall be referenced on all correspondence.
- All questions must be received no later than 3:00 PM on 10/09/2019. Any question received after this deadline may not be answered.
- Responses to questions/clarifications will be placed on the County's website. Check this http://www.sccmo.org/Bids.aspx website frequently for updates and any addendum that are issued.
Prohibited Communication

Contact with any representative, other than through the procedure outlined in the section titled "Bid Inquiries", concerning this request is prohibited PRIOR TO BID OPENING. Representative shall include, but not be limited to, all elected and appointed officials, and employees of St. Charles County and their Agents within St. Charles County. Any Offeror engaging in such prohibited communications prior to Bid Opening may be disqualified at the sole discretion of St. Charles County.
TERMS AND CONDITIONS

- St. Charles County reserves the right to reject any and all bids or parts of a bid and waive technicalities, and to adjust quantities.
- All bids will be considered final. No additions, deletions, corrections, or adjustments will be accepted after the time of bid opening.
- All delivery costs or charges must be included in the F.O.B. destination bid price.
- City, County and State of Missouri Sales Tax and Federal Taxes are not applicable to sales made to St. Charles County and must be excluded.
- The contract shall be effective for the approximate twelve (12) month period from the date of the notice of award.
- The County, with the consent of the vendor, shall have the option to renew said contract for two (2) additional twelve (12) month periods at the same specifications and terms and conditions of any contract that may be derived from this request for proposal.
- The electronic version of this bid/RFP is available upon request. The document was entered into WORD for Microsoft Windows. The Purchasing Office does not guarantee the completeness and accuracy of any information provided on the electronic version. Therefore, respondents are cautioned that the hard copy of this bid/RFP on file in the Purchasing Office governs in the event of a discrepancy between the information contained in or on the electronic version and that which is on the hard copy.
- Vendors are required to clearly identify any deviations from the specifications in this document.
- An authorized officer of the company submitting the bid must sign all bids, in blue ink.
- Vendors must submit two [2] signed copies of their bid; one is to be an original and the other marked.
- All prices and notations must be in blue ink or typewritten on the attached form. Mistakes must be crossed out, corrections typed adjacent and must be initialed in blue ink by the person signing the bid.
- St. Charles County will not award any bid to an individual or business having any outstanding amounts due from a prior Contract or business relationship with the County or who owes any amount(s) for delinquent Federal, State or Local taxes, fees and licenses.
- Sealed proposals received after the designated time of the receipt of the sealed proposals will be considered as "No Bid" and "Void" and will not be opened.
- The successful bidder is specifically denied the right of using in any form or medium the names of St. Charles County or any other public agency within St. Charles County Government for public advertising unless express written permission is granted.
- All bidders must possess the necessary and appropriate business and/or professional licenses in their field.
- Award will be made to the low responsive, responsible bidder, or to the offeror whose proposal is most advantageous to the County, price and other factors considered including geographic location. When payments are to be made to the County, award will be made to the most advantageous offer.
County reserves the right to accept any item or group of items offered, unless the bidder qualifies his bid by specific limitations. The bid can be on an "all or none" basis if wording in the bid so states and if all items solicited are included in the bid.

When applicable, provide unit prices and extension prices. Where there is disagreement in the unit and extension prices, the unit price shall govern.

INSURANCE:
The successful bidder must agree to provide and maintain during the life of the Contract the insurance(s) listed below, in the minimum amounts specified, with an insurance company licensed to do business in the State of Missouri. All policies must name the County as an additional insured and provide for thirty (30) days written notice prior to any material changes or cancellation.

Workers Compensation: Statutory limits, as required by the statutes of the State of Missouri and Employer's Liability with limits, is no less than $500,000.

Comprehensive General Liability (including automobile): Limits of no less than $1,000,000/3,000,000/1,000,000 per occurrence or $3,000,000/

**Employment of Unauthorized Aliens Prohibited** *(Missouri Revised Statutes Section 285.530)*

As a condition for the award of any contract or grant in excess of five thousand dollars by St. Charles County to a business entity, the business entity shall, by sworn affidavit and provision of documentation**, affirm its enrollment and participation in a federal work authorization program (E-Verify) with respect to the employees working in connection with the contracted services. Every such business entity shall sign an affidavit affirming that it does not knowingly employ any person who is an unauthorized alien in connection with the contracted services. [RSMO 285.530 (2)]

An employer may enroll and participate in a federal work authorization program (E-Verify) and shall verify the employment eligibility of every employee in the employer’s hire whose employment commences after the employer enrolls in a federal work authorization program. The employer shall retain a copy of the dated verification report received from the federal government. Any business entity that participates in such program shall have an affirmative defense that such business entity has not violated subsection 1 of this section. [RSMO 285.530 (4)]

Any entity contracting with St. Charles County shall only be required to provide the referenced affidavit on an annual basis. A copy of the affidavit is included in this bid request. Vendors may choose to send the required documentation using one of the following options:

- Send the notarized affidavit and E-Verify MOU signature page to: St. Charles County, Attn: Purchasing Manager, 201 N Second Street, Room 541, St. Charles, MO 63301 prior to responding to any solicitations; OR

- Send the notarized affidavit and E-Verify MOU signature page along with a bid solicitation response.

These documents will be kept on file. The notarized affidavit will remain current for **one year** from the date of the notarized affidavit.
** PLEASE NOTE:

Acceptable enrollment and participation documentation consists of a valid copy of the signature page of the E-Verify Memorandum of Understanding, completed and signed by the Contractor, and the Department of Homeland Security - Verification Division.

The online address to enroll in the E-verify program is:


---

OPEN RECORDS

Any and all information contained in or submitted with the bid becomes a public record subject to the Missouri Sunshine Law when the bids are opened. If the bidder believes that any information contained in or submitted with the bid is protected from disclosure by the Missouri Sunshine Law, the bidder must clearly identify what information the bidder believes is so protected and must also clearly identify the legal basis therefor.

---

Veteran Friendly Employment Policy

"Indicate whether you have developed a veteran friendly employment policy and, if so, attach a copy of such policy to your response as a point of information."

_____ "YES" our company has a veteran friendly employment policy.

____ √ "NO" our company does not have a veteran friendly employment policy.

Please include a copy of your veteran friendly employment policy with your submission.
BID SPECIFICATIONS

The Family Arena requires a Micros or comparable hardware and software solution for a POS system, event management, inventory control, and suites management for food service operations. The system should also function as a time clock system. Vendor supplied hardware must be new and unused. The bid requires an upgrade from the existing POS Tangent Back Office application and database to a Micros solution. Data from the old system needs to be converted into the new system. All measurements provided in this specification are considered estimates. The County reserves the right to accept any, all or none of the vendor offerings to this bid.

The bid needs to include the design, coordination, supply, installation, testing, training, and yearly maintenance of the proposed system. All bids must include warranty and helpdesk support for all equipment and software necessary to provide a complete system. All warranty and helpdesk support pricing must be itemized in the bid.

The Family Arena operates approximately 60 tangent POS terminals. The vendor should specify and include the potential reuse of any hardware including cash drawers and pedestals in their bid. All cost savings from this reuse should also be included.

St. Charles County will provide network connectivity, server hardware, and SQL server.

Experience/References

The bidder and the recommended system shall have documented experiences implementing in other similar sites. The list of client references must be available for site inspection, if deemed necessary, at the County's cost.

Family Arena Background

The Family Arena is a 192,855 square-foot multi-purpose facility located in St. Charles, MO, built in 1999 and owned by St. Charles County. With 17,900 square feet of arena floor space and seating capacity of approximately 10,000, the arena offers a variety of events including concerts, sporting events, ice shows, motor sports, family shows, rodeos, trade shows, and conventions. There are 44 private suites seating 16 guests and 2 party rooms, seating up to 24 guests. The Family Arena has a stylish 2500 square foot restaurant with a capacity of 200. There is full-service catering on site, including an Executive Chef, professional staff, and an extensive menu offering for any occasion. Extremely fan friendly, the arena maintains excellent sight lines and close proximity to the event floor with parking capabilities for 3600 vehicles.
**Functional Requirements**

Please answer to the availability of functionality in the proposed system. If you answer no, please explain differences in detail. Attach additional sheets of paper, if necessary. Identify in detail any third-party solutions or willingness to make modifications to the software application. Any requirements not responded to by the vendor will be considered unavailable functionality.

- Yes=Y
- No=N
- Third party=3
- Modification=M

Reference the question number in your description.

### General (Applies to POS, Suite Management Software, and Inventory Management)

#### Data Network/Communication Requirements

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) The software must be event driven, with the ability to have multiple events at the same time.</td>
<td>Y</td>
</tr>
<tr>
<td>2) Software needs to support multiple security access levels based on user profiles and groups.</td>
<td>Y</td>
</tr>
<tr>
<td>3) The system must operate over an Ethernet configuration</td>
<td>Y</td>
</tr>
<tr>
<td>4) Application must function properly over Category 5e/6 network cabling.</td>
<td>Y</td>
</tr>
<tr>
<td>5) The system must have capability to export reporting to formats such as Excel and PDF.</td>
<td>Y</td>
</tr>
<tr>
<td>6) Software/Credit card processing must meet PCI Security Standards.</td>
<td>Y</td>
</tr>
<tr>
<td>7) Must be able to customize menu selections for each stand location. (i.e. Stand 1 has different selections than Stand 2 which has different selections than the Suites hand-helds etc.)</td>
<td>Y</td>
</tr>
</tbody>
</table>

#### Inventory Control & Account Software

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>6) Inventory system (POS and Suite Management) must support inventory tracking and audit from a central location in real-time.</td>
<td>Y</td>
</tr>
<tr>
<td>9) All reports for the system (Point-of-Sale, Handhelds, Inventory Control and the Suites POS) must be run at workstations that have the management software installed.</td>
<td>Y</td>
</tr>
<tr>
<td>10) Each sales transaction must assign a unique transaction number to assist in an audit trail.</td>
<td>Y</td>
</tr>
<tr>
<td>11) System must support multiple inventory locations, multiple location types, and allow for management of the inventory.</td>
<td>Y</td>
</tr>
<tr>
<td>12) Transactions reports must be capable to be broken down into cash, credit, and debit in real-time and after an event.</td>
<td>Y</td>
</tr>
<tr>
<td>13) End of event function to produce inventory and sales information for multiple locations by concession stand, POS terminal, and inventory supplies.</td>
<td>Y</td>
</tr>
<tr>
<td>14) The ability to produce inventory and inventory cost reports on demand.</td>
<td>Y</td>
</tr>
<tr>
<td>15) The ability to track inventory/product in each location as well as spoilage and discounts.</td>
<td>Y</td>
</tr>
<tr>
<td></td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>-------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>16</td>
<td>The ability to flag items low in stock.</td>
</tr>
<tr>
<td>17</td>
<td>The system must maintain item lists by multiple suppliers.</td>
</tr>
<tr>
<td>18</td>
<td>The system must have the ability to balance physical inventory sales to actual cash deposited during and after an event to produce an over/short balance.</td>
</tr>
<tr>
<td>19</td>
<td>The system must allow for custom reports, not limited to the following: sales by stand/item, sales of stand, over/short, consolidated sales for the facility, and cash room balancing report.</td>
</tr>
<tr>
<td>20</td>
<td>The ability to produce sales by company and sales by product category.</td>
</tr>
<tr>
<td>21</td>
<td>The system must have the ability to check for duplicate credit card transactions manually.</td>
</tr>
<tr>
<td>22</td>
<td>System must automatically batch and settle credit cards at the end of the night with no human interaction.</td>
</tr>
<tr>
<td>23</td>
<td>The ability to setup theoretical food costs/recipes to track estimated food costs. For example, a recipe could include the following: hotdog, bun, ketchup, napkins, etc.</td>
</tr>
</tbody>
</table>
### POS System/Cashier Stations:

<table>
<thead>
<tr>
<th>Software Requirements</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>24) POS terminal are used for customer transactions and the following data should be generated in a report for each user and a total for each selling location: amount collected, amount voided, returned to inventory, spoilage, gratis, etc.</td>
<td>Y**</td>
</tr>
<tr>
<td>25) Cash drawer must not include a separate source of power.</td>
<td>Y</td>
</tr>
<tr>
<td>26) POS units must have a minimum of 75 user programmable keys. Specify the number of programmable keys.</td>
<td>Y</td>
</tr>
<tr>
<td>27) POS terminals must have magnetic card readers integrated into the unit to process credit cards, magnetic employee cards, debit cards, etc.</td>
<td>Y</td>
</tr>
<tr>
<td>28) POS terminals must display specific menu item, price, total transaction amount, and if the POS is closed.</td>
<td>Y</td>
</tr>
<tr>
<td>29) POS units must have the same menu and prices within a concession stand. Different stands may have different menu items and prices.</td>
<td>Y</td>
</tr>
<tr>
<td>30) Menus and pricing must exist in a central database.</td>
<td>Y</td>
</tr>
<tr>
<td>31) Menus and pricing must be manageable from a central location.</td>
<td>Y</td>
</tr>
<tr>
<td>32) Menu and pricing may be different per event. The system must propagate menu items and prices from a central location to all POS units on the network. The process should take no longer than 10 minutes.</td>
<td>Y</td>
</tr>
<tr>
<td>33) POS terminal should be user swappable within concession stands and between concession stands. User should be able to easily download new prices and menu items.</td>
<td>Y</td>
</tr>
<tr>
<td>34) POS terminal must have the ability to connect with a single printer or networked printer.</td>
<td>Y</td>
</tr>
<tr>
<td>35) POS unit must be able to record a receipt for credit cards, cash, and debit card and print a receipt itemizing menu items, quantity sales tax, etc.</td>
<td>Y</td>
</tr>
<tr>
<td>36) POS unit must have the ability to print sales report, summarizing quantities sold, total sale amounts, and other reports.</td>
<td>Y</td>
</tr>
<tr>
<td>37) Central database system must have the ability to gather all sales information on demand.</td>
<td>Y</td>
</tr>
<tr>
<td>38) POS terminal must have the ability to manually enter dollar amounts and programmable amount tendered keys ($5.00, $10.00, $20.00, etc.) to speed up transactions, and it must have a full 10-digit keyboard (plus a decimal point/period) so that the operator can enter specifically tendered amounts.</td>
<td>Y</td>
</tr>
<tr>
<td>39) POS terminal must have the ability to discount selected sales by a fixed dollar amount or percentage authorized by the central system based on the use of discount cards.</td>
<td>Y</td>
</tr>
<tr>
<td>40) Each POS unit must have a unique identifier in the master database.</td>
<td>Y</td>
</tr>
<tr>
<td>41) All POS terminals should be capable limiting/expanding selected access to keys/functions based on job titles or passwords.</td>
<td>Y</td>
</tr>
<tr>
<td>42) POS units must be able to reroute to a different printer in the event of a printer failure.</td>
<td>Y</td>
</tr>
<tr>
<td>43) Customizable touchscreen for programmable keys</td>
<td>Y</td>
</tr>
<tr>
<td>Requirement</td>
<td>Status</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Each POS unit must be capable of paging back through at least the 100</td>
<td>Y</td>
</tr>
<tr>
<td>previous sales. This procedure must be maintained even after the sale</td>
<td></td>
</tr>
<tr>
<td>may have been transmitted to the back office.</td>
<td></td>
</tr>
<tr>
<td>POS terminals must be able to search for individual transactions by</td>
<td>Y</td>
</tr>
<tr>
<td>terminal, sale ID, credit card, quantity, or price.</td>
<td></td>
</tr>
<tr>
<td>Security allows the ability to restrict credit card credits/refunds to</td>
<td>Y</td>
</tr>
<tr>
<td>specific users and specific POS terminals.</td>
<td></td>
</tr>
<tr>
<td>Credit card receipting can be turned off for dollar amounts below a</td>
<td>Y</td>
</tr>
<tr>
<td>certain value for the entire system.</td>
<td></td>
</tr>
<tr>
<td>Credit card receipts can be manually printed after a sale is complete.</td>
<td>Y</td>
</tr>
<tr>
<td>The POS system must support a club/restaurant environment.</td>
<td>Y</td>
</tr>
</tbody>
</table>

**Physical Requirements For POS/Inventory Management**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed cable must be hidden from view to maintain a professional</td>
<td>Y</td>
</tr>
<tr>
<td>environment.</td>
<td></td>
</tr>
<tr>
<td>Cash drawer should be mountable above or below the counter.</td>
<td>Y</td>
</tr>
<tr>
<td>POS units must be able to sit atop the cash drawer or next to the unit.</td>
<td>Y</td>
</tr>
<tr>
<td>POS terminal must have two displays: one for the staff and one for the</td>
<td>Y</td>
</tr>
<tr>
<td>customer; which shows order, pricing, subtotal, tax, and totals.</td>
<td></td>
</tr>
<tr>
<td>POS terminals, magnetic readers, cash drawers, printers, should be spill</td>
<td>Y</td>
</tr>
<tr>
<td>resistant.</td>
<td></td>
</tr>
<tr>
<td>Units must withstand regularly cleaning. Please recommend cleaning</td>
<td>Y</td>
</tr>
<tr>
<td>process/chemicals.</td>
<td></td>
</tr>
<tr>
<td>The POS terminals should allow for the following options:</td>
<td>Y</td>
</tr>
<tr>
<td>programmable touchscreen buttons, barcode scanners, customer display,</td>
<td></td>
</tr>
<tr>
<td>and multiple cash drawers.</td>
<td></td>
</tr>
<tr>
<td>POS units must operate independently and operate as a freestanding unit</td>
<td>Y</td>
</tr>
<tr>
<td>capable of operation in the event of a server failure and maintain menu,</td>
<td></td>
</tr>
<tr>
<td>pricing, stored transactions, etc. and update the stored information once</td>
<td></td>
</tr>
<tr>
<td>service is restored without the loss of data.</td>
<td></td>
</tr>
</tbody>
</table>
### Suites Management Application

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>58) Suite personnel must be able to enter advance orders for upcoming events by Suite Account with no time limit as to when the event will take place.</td>
<td>Y</td>
</tr>
<tr>
<td>59) The system must print food distribution reports that show where the advance orders should be distributed prior to the event.</td>
<td>Y</td>
</tr>
<tr>
<td>60) The system must allow for individual event set up for data collection and sales reporting.</td>
<td>N**</td>
</tr>
<tr>
<td>61) The system must print production reports for kitchen production that tells the kitchen staff what to prepare for the upcoming events. These production reports should show roll-up quantities of all advance items ordered. The system must also have the ability to generate tickets in the warehouse from the kitchen or concession stands.</td>
<td>Y</td>
</tr>
<tr>
<td>62) The system must print Prep-Delivery Labels for all Advance Orders.</td>
<td>Y</td>
</tr>
<tr>
<td>63) System must support handheld devices for sales and payment for multiple users, multiple devices per event, and different users signed on to each.</td>
<td>Y</td>
</tr>
<tr>
<td>64) Handhelds must communicate with a kitchen order screen when sales are made in real time.</td>
<td>Y</td>
</tr>
<tr>
<td>65) Handhelds must be programable to show multiple menu items, and have these items organized by category.</td>
<td>Y</td>
</tr>
<tr>
<td>66) Handhelds must process credit cards and be PCI compliant. Must also accept cash payment option for closing a check.</td>
<td>Y</td>
</tr>
<tr>
<td>67) Must be able to keep multiple transactions open on the handheld.</td>
<td>Y</td>
</tr>
<tr>
<td>68) Kitchen must have a display for real time orders and have the capability to notify the origin of the order when it is complete.</td>
<td>Y</td>
</tr>
<tr>
<td>69) Kitchen must have a printer to produce tickets when orders are submitted.</td>
<td>Y</td>
</tr>
<tr>
<td>70) Menu items and pricing must have the capability of editing.</td>
<td>Y</td>
</tr>
<tr>
<td>71) System must automatically batch and settle credit cards at a pre-determined time. There should be no manual intervention required.</td>
<td>Y</td>
</tr>
<tr>
<td>72) All Suites Sales Information should be captured in the primary Concessions POS Database so sales from Concessions, Premium, and Suites.</td>
<td>Y</td>
</tr>
<tr>
<td>73) Suites must be able to close checks for pre-orders to a &quot;suite charge&quot; or &quot;pre-order&quot; category for revenue tracking and reporting.</td>
<td>Y</td>
</tr>
<tr>
<td>74) Integrated credit card processing and settlement.</td>
<td>Y</td>
</tr>
</tbody>
</table>

### Pricing

Itemized pricing must be included but not limited to the following:

- Requirements for a complete system
- Installation costs
- Training costs
- Help Desk Support/Open event support
- Warranty and maintenance on hardware and software
- Estimated quantities may change
- Price per unit will be used to add and subtract additional units, if estimated quantities change.

### POS Workstation and Peripherals Hardware (Itemize any additional hardware needed)

<table>
<thead>
<tr>
<th>Estimated Quantity</th>
<th>Item Description</th>
<th>Price Per Unit</th>
<th>Extended Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>60</td>
<td>Toast 10&quot; Table Terminal</td>
<td>$710.00</td>
<td>$42600.00</td>
</tr>
<tr>
<td>1</td>
<td>22&quot; Touchscreen</td>
<td>$1290.00</td>
<td>$1290.00</td>
</tr>
<tr>
<td>60</td>
<td>Dynamo EMV Reader (with mounting kit)</td>
<td>$300.00</td>
<td>$18000.00</td>
</tr>
<tr>
<td>60</td>
<td>Toast Flip Stand for 10&quot;</td>
<td>$110.00</td>
<td>$6600.00</td>
</tr>
<tr>
<td>6</td>
<td>Toast Go Pay 6&quot; HH Tablet</td>
<td>$600.00</td>
<td>$3600.00</td>
</tr>
<tr>
<td>24</td>
<td>Thermal Receipt Printers</td>
<td>$349.00</td>
<td>$8376.00</td>
</tr>
<tr>
<td>1</td>
<td>Impact Autocut Remote</td>
<td>$399.00</td>
<td>$399.00</td>
</tr>
<tr>
<td>60</td>
<td>APG Cash Drawer</td>
<td>$199.00</td>
<td>$11940.00</td>
</tr>
<tr>
<td>60</td>
<td>Cable for APG Cash Drawer</td>
<td>$9.00</td>
<td>$540.00</td>
</tr>
<tr>
<td>1</td>
<td>LCD Monitor Wall Mount</td>
<td>$95.00</td>
<td>$95.00</td>
</tr>
<tr>
<td>1</td>
<td>Magnetic Stripe Cards (for user login)</td>
<td>$28.00</td>
<td>$28.00</td>
</tr>
<tr>
<td>1</td>
<td>Special Discount – 15% Off hardware</td>
<td>($14020.20)</td>
<td>($14020.20)</td>
</tr>
<tr>
<td></td>
<td>($3000 of proposed discount requires 24 month agreement,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>discount reduced by $3000 for 12 month contract)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Freight</td>
<td>$5356.00</td>
<td>$5356.00</td>
</tr>
</tbody>
</table>

### Software (Itemize any additional software)

<table>
<thead>
<tr>
<th>Estimated Quantity</th>
<th>Item Description</th>
<th>Price Per Unit</th>
<th>Extended Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Toast Software Service, Cloud Based Webhosting Subscription</td>
<td>See Below</td>
<td>$2673 Total Monthly Cost. Unit Prices Below.</td>
</tr>
<tr>
<td>1</td>
<td>First Device Monthly SaaS</td>
<td>$120</td>
<td>$120</td>
</tr>
<tr>
<td>65</td>
<td>Additional Device Monthly SaaS</td>
<td>$60</td>
<td>$3900</td>
</tr>
<tr>
<td>1</td>
<td>KDS Monthly SaaS</td>
<td>$25</td>
<td>$25</td>
</tr>
<tr>
<td>1</td>
<td>Inventory Monthly SaaS</td>
<td>$75</td>
<td>$75</td>
</tr>
<tr>
<td>1</td>
<td>Monthly SaaS Discount - $975, Monthly Terminal Discount 15% off - $472</td>
<td>($1447)</td>
<td></td>
</tr>
</tbody>
</table>

---

10-130 Point-of-Sale System with Touchscreens and Handhelds

Proposal Response from (please complete)

[Signature]

Name of Company or Individual
<table>
<thead>
<tr>
<th>Item Description</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training – The vendor must provide a detailed plan for project team training and technology personnel. This information MUST include:</td>
<td>$10845.00 for Preparation and Project Management. Includes Programming, Training, Database Review, Installation, Go Live Support</td>
</tr>
<tr>
<td>* Overview of proposed Training, including project team and technology personnel.</td>
<td></td>
</tr>
<tr>
<td>* Training would be preferred to be done based on a train the trainer model.</td>
<td></td>
</tr>
<tr>
<td>* Use of third-party training resources. Vendor should identify third party partners that provide training on the use of their application.</td>
<td></td>
</tr>
<tr>
<td>Data Conversion –</td>
<td>No Data Conversion Included**</td>
</tr>
<tr>
<td>Equipment Installation and Implementation</td>
<td>Inclusive with Training Cost</td>
</tr>
<tr>
<td>The vendor shall be responsible for installation, integration and testing of all hardware and software. All hardware and software installation must be coordinated with the County I.S. department. All installations must be scheduled to create a minimum of interruption in the daily operations of the St. Charles County and Family Arena.</td>
<td>Depot Support included at no additional cost for first year. Phone Support is included in software contract - 24/7 through DCRS. Depot Support available after first year for $12236. Onsite 5 Day Support available for $17334. Onsite 6 Day Support Available for $20393.</td>
</tr>
<tr>
<td>Maintenance and Support Program</td>
<td></td>
</tr>
<tr>
<td>Specify the nature of any post-implementation and on-going support provided by the vendor including:</td>
<td></td>
</tr>
<tr>
<td>* Depot support for first year and phone support ongoing. Additional support available for additional cost.</td>
<td></td>
</tr>
<tr>
<td>* Telephone support (include toll-free support hotline, hours of operation, availability of 24 X 7 hotline, etc.)</td>
<td></td>
</tr>
<tr>
<td>* Special plans defining “levels” of customer support (e.g., gold, silver, etc.).</td>
<td></td>
</tr>
<tr>
<td>* Availability of user groups.</td>
<td></td>
</tr>
<tr>
<td>* Problems reporting and resolution procedures</td>
<td></td>
</tr>
<tr>
<td>* Bug Fixes and Patches included in automatic updates. System includes automatic updates with new functionality and patch fixes</td>
<td></td>
</tr>
<tr>
<td>* Warranties</td>
<td></td>
</tr>
<tr>
<td>* Other support (e.g., on-site, remote access, Website access to patches, fixes and knowledge base).</td>
<td></td>
</tr>
</tbody>
</table>
Exception Sheet

If the item(s) and/or services proposed in the response to this bid is in any way different from that contained in this proposal or bid, the bidder is responsible to clearly identify all such differences in the space provided below. Otherwise, it will be assumed that the bidder's offer is in total compliance with all aspects of the proposal or bid.

Below are the exceptions or differences to the stated specifications (attach additional sheets as needed):

19. The system must allow for custom reports, not limited to the following: sales by stand/item, sales of stand, over/short, consolidated sales for the facility, and cash room balancing report.
   Y** - The Toast system does not allow for custom reports, but it does allow for filterable reports.

21. The system must have the ability to check for duplicate credit card transactions manually.
   N** - Toast does not have the same issue as the Tangent software of creating duplicate credit card transactions which this question addresses.

24. POS terminal are used for customer transactions and the following data should be generated in a report for each user and a total for each selling location: amount collected, amount voided, returned to inventory, spoilage, gratis, etc.
   Y** - Spoilage will be recorded as a discount.

60. The system must allow for individual event set up for data collection and sales reporting.
   N** - The Toast system cannot filter by event, but it can filter by time down to the minute.

DATA CONVERSION - Data Conversion is not included with implementation.

Special Discount – DCRS is including a 15% hardware discount. $3000 of the discount requires a 2 year contract. DCRS will reduce the discount by $3000 for a 1 year contract.
BID FORM

IFB 19-130

**Point-of-Sale System with Touchscreens and Handhelds**

DCRS Solutions

(Bidder name)

Submits the following bid for this project:

<table>
<thead>
<tr>
<th>Total bid price for cost and installation:</th>
<th>$107321.80</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Maintenance Cost:</th>
<th>1st Yr. Help Desk &amp; Depot Support Included</th>
<th>2nd Yr. Help Desk included, Optional Depot -- $12236.00</th>
<th>3rd Yr. Help Desk included, Optional Depot -- $12236.00</th>
</tr>
</thead>
</table>

Authorized signature

Date 10/15/19
AFFIDAVIT OF WORK AUTHORIZATION

Comes now Matt Keamer as President first being duly sworn, on my oath, affirm DCRS Solutions is enrolled and will continue to participate in a federal work authorization program in respect to employees that will work in connection with the contracted services related to Point of Sale System with Touchscreens and Handhelds, BID IFB 19-130

(Describe project or insert bid number)

for the duration of the contract, in accordance with RSMo Chapter 285.530 (2). I also affirm that DCRS Solutions does not and will not knowingly employ a person who is an unauthorized alien in connection with the contracted services related to the Point-of-Sale System with Touchscreens and Handhelds, BID IFB 19-130.

(Describe project or insert bid number)

In affirmation thereof, the facts stated above are true and correct (the undersigned understands that false statements made in this filing are subject to the penalties provided under section 575.040, RSMo).

Matt Keamer

Signature (person with authority)
President

Printed name
10-11-19

Date

Subscribed and sworn to before me this 11TH of OCTOBER, I am commissioned as a notary

Public within the County of ST. LOUIS, State of MISSOURI, and my commission expires on MAY 11, 2021

Signature of Notary

10-11-2019

19-130 Point-of-Sale System with Touchscreens and Handhelds

Proposal Response from (please complete)

DCRS SOLUTIONS

Name of Company or Individual
American Made:

In accordance with the Domestic Product Procurement Act (hereinafter referred to as the Buy American Act) RSMo 34.350-34.359, the bidder is advised that any goods purchased or leased by any public agency where the purchase, lease or contract involves the expenditure of twenty-five ($25,000) or more, shall be manufactured or produced in the United States. Section 34.350.2(1) of that Act specifies that the term “public agency” includes all political subdivisions of the State of Missouri, which definition includes counties.

The requirements of the Buy American Act shall not apply if other exceptions to the Buy American mandate in RSMo 34.353 are met.

If the bidder claims there is only one line of the good manufactured or produced in the United States, RSMo 34.353 (2), or that one of the exceptions of RSMo 34.353 (3) applies, the Department Head or Elected Official bears the burden of certification as required prior to the award of a contract.

In accordance with the Buy American Act, the bidder must provide proof of compliance with RSMo 34.353. Therefore the bidder should complete and return Exhibit A, certification regarding proof of compliance, with the bid. This document must be satisfactorily completed prior to an award of a contract.
ST. CHARLES COUNTY
DOMESTIC PRODUCTS PROCUREMENT ACT (BUY AMERICAN)

The Missouri Domestic Products Procurement Act (34.350-34.359 RSMo) requires that for all bids with a value of $25,000 or more, the goods or commodities purchased by any public agency (which definition includes all political subdivisions of the State, including counties) or used or supplied in the construction, alteration, repair, or maintenance of any public works must be manufactured or produced in the United States. As defined in 34.350 RSMo, United States means the United States of America, the District of Columbia, and all territories and possessions subject to the jurisdiction of the United States. The law also requires that the bidder must provide proof of compliance. Note: In general, if an import tariff is applied to an item, it does not qualify for the Buy American preference. In addition, Most Favored Nation status does not allow application of the preference.

Section A – All Products Are Manufactured or Produced In U.S.
If all products bid qualify as domestic products under Missouri law, complete only Section A.

<table>
<thead>
<tr>
<th>Signature</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td></td>
</tr>
</tbody>
</table>

If Section A is completed, do not complete Section B.

Section B – Only One Product Line or No Products Are Manufactured or Produced In U.S.
If only one product line or no products are manufactured or produced in the U.S. complete only section B.

<table>
<thead>
<tr>
<th>Signature</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td></td>
</tr>
</tbody>
</table>

Section C – Products May Qualify Because of Qualifying Treaty
If some or all products bid qualify for domestic status because of a trade treaty, etc., then the bidder must identify each product, country and qualifying treaty, etc. below. The bidder must list ALL products which are or may qualify as domestic below. If more space is needed, please copy this form and submit as an attachment.

<table>
<thead>
<tr>
<th>Bid Item Number(s)</th>
<th>Country Where Manufactured or Produced</th>
<th>Qualifying Treaty, Law, Agreement, or Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SECTION C

I hereby certify that the specific items listed above are domestic, that the information provided is true and correct, and complies with all provisions of Sections 34.350-34.359 RSMo. I understand that any misrepresentation herein constitutes the commission of a class A misdemeanor pursuant to Section 34.355 of the Revised Statutes of Missouri.

<table>
<thead>
<tr>
<th>Signature</th>
<th>N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company Name</td>
<td></td>
</tr>
</tbody>
</table>
Table of Contents

Section 1 - DCRS Company Overview
  • DCRS Vendor Information
  • What Differentiates DCRS from Other POS Companies

Section 2 - Toast Overview
  • Product Overview
  • Offline Mode Overview

Section 3 - DCRS Support and PCI Compliance
  • Attachment 1 - PCI Data Security Standards REQUIREMENTS and RESPONSIBILITIES
  • Attachment 2 - Customer Support User's Guide
  • Attachment 3 - Toast Certificate of Validation
  • Attachment 4 - Toast PCI Deployment Guide
  • Attachment 5 - Customer Information Planning Information
  • Attachment 6 - Planning Meeting Agenda
  • Attachment 7 - DCRS Final Installation Review
  • Attachment 8 - Highest Level of Certifications

Section 4 - RFP Responses

Section 5 - Toast POS Pricing
VENDOR INFORMATION

**DCRS Solutions** (incorporated as Data Cash Register Systems Inc., February 1976) is one of the Midwest’s largest suppliers of retail business solutions, but what **DCRS** really stands for is:

*Delivering Certified Results & Satisfaction*

**Our Difference...**Delivering Certified Results and Satisfaction: Delivering with the technical training that makes our staff Industry-Certified to provide you positive **Results** and a Customer Program that includes daily management follow-up & staff incentives to insure your **Satisfaction**.

**Our Purpose** Since 1976, DCRS Solutions has been helping restaurant, hospitality and retail operators run their businesses more efficiently. From electronic cash registers, to windows based point of sale systems, to Android and IOS cloud systems, DCRS has always evolved to bring the most current and purpose built solutions to market. We strive to retain our customers by exceeding their expectations with superior service and meaningful retail tools, permitting us to grow and be successful for the well-being of our customers and employees. Whether you are a single unit operator, multi-unit chain or manage an enterprise environment, we have a solution for you. Beyond POS, DCRS offers a wide range of services including a 24x7 IT support center, on site professional services, merchant services (credit card processing), managed services, network management and much more.

**Our Solutions** include Point of Sale Hardware and Software (Both Cloud and On Premise), Labor Management, Inventory, Online Ordering, Loyalty/Gift, Consultation, Customization, Implementation, Installation, Training and Support. Our Managed Services offerings include, Above Store Management and Reporting, Disaster Recovery, Cellular Failover, Firewall Management, Antivirus Management, Network Management, Payment Processing, PCI Assistance, Remote Monitoring, Wi-Fi Management and Wireless Device Management

**Our Milestones**

**2010’s**
- Celebrated 40 years in business
- Become the exclusive distributor for Toast (Android) and MobileBytes (IOS)
- Added Merchant Services to our offerings
- Installed 100+ POS with Anheuser Bush in their Breweries and Craft Pubs
- Installed 380+ POS at Busch Stadium
- Rolled out Sugarfire with new cloud POS for existing and franchisee locations
- Rolled out 20+ American Cleaners with new cloud POS
- Certified as PCI-SSC Qualified Integrators & Resellers (PCI-QIR) company

**2000’s**
- Awarded 1st ever MICROS Customer Service Award of Excellence
- Awarded Microsoft Certified Solution Provider status from Microsoft
- Completed 50 store rollout of UNIFY Retail software to CVC
- Completed 200+ MICROS rollout for Build-A-Bear Workshop
- Completed MICROS rollout for Mercy Healthcare, 37 sites in 4 states
- Slaged 600+ MICROS for Panera/Saint Louis Bread Company
1980's
- Awarded A+ Certified Authorized Service Center status from CompTIA
- Received Award as Top IBM Remarketer
- Shipped 300+ IBM's to Fox Photo, 40+ IBM's to Copy USA
- Received MICROS "President's Award" – top 5 MICROS dealers
- Shipped 300+ MICROS to Panera/Saint Louis Bread Company

1980's
- Authorized by MICROS Systems
- Developed "Retail & POS Manager" inventory and POS software
- Shipped 400+ IBM's to CPI Photo Finish
- Sold 350+ terminals to Edison Brothers Shoe Stores
- Sold 100+ terminals to retail division of Kellwood
- Installed 100+ lanes of Scanning Systems to grocery store market

1970's
- Represented DTS: 1st Electronic Cash Register system made in USA

When evaluating POS Systems, differences are sometimes determined AFTER THE SALE...

Our Systems Include:
- 1st month of SaaS included in your contract
- Industry Standard Peripherals in Epson Printers and APG Cash Drawers
- Business Class Firewall – SonicWALL, to protect your POS Network and adhere to PCI Guidelines.
  First year subscription included with purchase. DCRS will manage ongoing subscriptions on your behalf.
- 1000Mbps Ethernet Switch
- Magnetic Cards for your Staff included with every system
- 12 month Hardware Depot warranty with DCRS. No shipping hardware all over the world, simply bring to us and we'll replace or fix, right here in our office.
- Not to exceed Professional Services and Installation (see below)
- Fully Certified with POS Vendor. Everything from Sales, to Installation to Support comes through DCRS, we use no 3rd parties or contractors.

Our Implementation Includes:
- Planning Meeting...DCRS Project Manager and Dedicated Installation Specialist to review expectations of the system purchased
- Site Survey...review existing setup to determine what can be reused or what needs to be installed from a networking standpoint.
- Database Programming...Installation Specialist to program all menu items, modifiers, employees, taxes, etc.
- Database Review...review menu design (face to face) to discuss any changes that might be needed prior to training.
- Management & Employee Training...Installation Specialist to train all management staff and assist in all employee training at DCRS Solutions or Customers site.
- Installation...Installation Specialist to install everything once you are ready to go live, no subcontractors needed!
- Live Support...we will be there with you for your opening shift to ensure everything is setup to your liking, as well as review your first days reporting and credit card deposits.
- Post Live Follow up...our Project Manager will follow up to ensure you are 100% satisfied and your Installation Specialists will be available should you have any questions during your first week.
Our Certifications include:

- **26 employees dedicated to POS**
- **9 A+ Certifications** from CompTIA, certifies competency and commitment to computer repair and software
- **8 Network+ Certifications** from CompTIA, validates essential knowledge and skills needed to design, configure, manage and troubleshoot any wired and wireless networks.
- **PCI-SSC Qualified Integrators** and Resellers, Visa mandate that all Payment Application Installs are performed only by a QIR Certified Company as of March 31, 2016.
- **3 SonicWALL Certified Security Administrators**, certifies competency and commitment to managed subscription services.
- **2 Security+ Certifications** from CompTIA, validates security knowledge and skills. Covers the essential principles for network security and risk management.
- **5 MCP’s** (Microsoft Certified Professionals), certifies competency and commitment to a MS operating system.
- **13 PCI Wise Certifications**, by RSPA, certifies individuals knowledge on PCI-Data Security Standards
- **24 x 7 Support**, all employed by DCRS, no 3rd parties or subcontractors.
- **Customer Support Users Guide**, in writing. Our Guide puts all the details in writing for exactly what is covered.

**What is a PCI – SSC Qualified Integrators and Resellers (PCI-QIR) Company?**
Organizations qualified by PCI SSC to implement, configure and/or support PA-DSS validated Payment Applications on behalf of merchants and service providers are referred to as “Qualified Integrator and Reseller Companies” or “QIR Companies.” The quality, reliability and consistency of a QIR Company’s work provide confidence that the application has been implemented in a manner that supports the customer’s PCI DSS compliance. **VISA has issued a mandate that all existing Level 4 merchants use PCI-certified QIR professionals from the QIR Companies list as of January 31, 2017.**

**What are A+ and Network+ Certifications?** A+ Certification is a program sponsored by the Computing Technology Industry Association (CompTIA) to certify a technician’s competency. The program is backed by major hardware & software vendors, including IBM, HP, Microsoft, and the Association of Field Service Management, Inc. To become certified, you must pass tests that cover configuring, installing, diagnosing, repairing, upgrading, and maintaining computers. CompTIA has awarded DCRS the designation of “A+ Authorized Service Center” every year since 1999, for having our staff A+ Certified, a Customer Satisfaction Program in place, and having multiple individuals with CompTIA’s Network+ Certification (for computer network skills).

**What is a Microsoft Certified Partner?** Microsoft's Certification program recognizes companies with a certified staff and competencies, as well as satisfied customers. DCRS has maintained MCP status since 2000. Certification requires testing of multiple employees to insure competency. Microsoft contacting customers to insure satisfaction, and requires a number of employees be **Microsoft Certified Professionals** (in current Operating Systems).

**Why are Certifications Important?** PCI-QIR, A+, Network+, Microsoft, SonicWall, Oracle and RSPA Solutions Provider industry Certifications means that DCRS possesses the knowledge and customer relation skills essential for successful technical support, as defined by experts from companies across the industry. **Certified Technicians are more likely to meet your expectation and increase your satisfaction.**

Our Markets
Restaurant/Hospitality... You have the comfort of knowing **we are the largest POS supplier in the St. Louis Region** for Quick Service, Table Service and Large Enterprise solutions, representing Oracle Hospitality (formerly MICROS), Toast and MobileBytes. We support large sites like Anheuser Busch, Oaklawn Racetrack, Mercy & BJ's, multi-sites such as Kaldi's Coffee, Pasta House Company, Sugarfire & Livelyen's and hundreds of single sites with only one terminal.

Our Value ...as one of the largest and oldest POS providers in the region, DCRS has been located in the West Port area of St. Louis County, MO. We built a 13,000 square foot facility located on Metro Boulevard at Dorsett Road in May 1982. In 40 years we have sold or supported 15,000+ terminals. **These products will deliver a lot to you, but the real difference behind the products is the PEOPLE of DCRS.**
## Our Industry Experience

<table>
<thead>
<tr>
<th>Name</th>
<th>Retail</th>
<th>Hosp</th>
<th>POS Before DCRS</th>
<th>DCRS</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grayson, C</td>
<td>6</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>Hemp, J</td>
<td>0</td>
<td>15</td>
<td>0</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>Houston, V</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>2</td>
<td>12</td>
</tr>
<tr>
<td>Ingram, B</td>
<td>2</td>
<td>10</td>
<td>0</td>
<td>10</td>
<td>22</td>
</tr>
<tr>
<td>Jordan, J</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td>21</td>
<td>36</td>
</tr>
<tr>
<td>Kramer, M</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>17</td>
<td>22</td>
</tr>
<tr>
<td>Kramer, M</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td>Krise, D</td>
<td>0</td>
<td>0</td>
<td>10</td>
<td>19</td>
<td>29</td>
</tr>
<tr>
<td>Lartochnik, D</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Lonero, D</td>
<td>13</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>17</td>
</tr>
<tr>
<td>McCarty, M</td>
<td>0</td>
<td>24</td>
<td>0</td>
<td>21</td>
<td>45</td>
</tr>
<tr>
<td>McCarthy, D</td>
<td>5</td>
<td>8</td>
<td>0</td>
<td>1</td>
<td>14</td>
</tr>
<tr>
<td>McGuinness, P</td>
<td>0</td>
<td>17</td>
<td>25</td>
<td>1</td>
<td>43</td>
</tr>
<tr>
<td>Moore, B</td>
<td>0</td>
<td>18</td>
<td>0</td>
<td>2</td>
<td>18</td>
</tr>
<tr>
<td>Potter, Z</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>Repp, B</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>20</td>
<td>29</td>
</tr>
<tr>
<td>Schultz, M</td>
<td>10</td>
<td>6</td>
<td>0</td>
<td>19</td>
<td>35</td>
</tr>
<tr>
<td>Schweiss, P</td>
<td>1</td>
<td>10</td>
<td>0</td>
<td>2</td>
<td>13</td>
</tr>
<tr>
<td>Spurlock, J</td>
<td>10</td>
<td>15</td>
<td>0</td>
<td>2</td>
<td>27</td>
</tr>
<tr>
<td>Taylor, W</td>
<td>0</td>
<td>15</td>
<td>0</td>
<td>2</td>
<td>17</td>
</tr>
<tr>
<td>Tripp, R</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>8</td>
<td>14</td>
</tr>
<tr>
<td>Unverferth, G</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>17</td>
<td>27</td>
</tr>
<tr>
<td>Warren, M</td>
<td>0</td>
<td>8</td>
<td>0</td>
<td>14</td>
<td>22</td>
</tr>
<tr>
<td>Warren, T</td>
<td>3</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>13</td>
</tr>
<tr>
<td>Wells, J</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>8</td>
<td>18</td>
</tr>
<tr>
<td>Williams, T</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>57</td>
<td>202</td>
<td>50</td>
<td>213</td>
<td>524</td>
</tr>
</tbody>
</table>
Our Common Law of Business... A buyer becomes far more educated after purchasing and installing their first POS system. Unfortunately, many prospective customers do not find out the real differences between DCRS and others until after that first system purchase or installation. That is why many new DCRS customers were previously someone else's.

"It's unwise to pay too much, but it's worse to pay too little. When you pay too much, you lose a little money—that is all. When you pay too little, you sometimes lose everything, because the thing you bought was incapable of doing the thing it was bought to do. The common law of business balance prohibits paying a little and getting a lot—it can't be done. If you deal with the lowest bidder, it is well to add something for the risk you run, and if you do that you will have enough to pay for something better." --John Ruskin (1819-1900).

DCRS is in the business of creating and retaining customers.

A few of our references

John Harris
Pasta House
314-635-6944

Josh Ferguson
Kaldi's Coffee House
314-727-9991

Jim Schneithorst
Schneithorst Restaurant
314-993-4100

Pat Carr
One 19 North
314-821-4119

James Meskill
Anheuser-Busch
541-976-5228

Laura Ravenscraft
BJC Children's
314-454-2643

Veronica Schuster
Sugarfire
314-997-2301

Anthony Scarato
Anthonino's
314-773-4455

Tom Caruso
LuLu Belles
314-981-0020

John Wetzel
American Cleaners
636-227-8269
When evaluating Restaurant POS Systems, differences are sometimes determined AFTER THE SALE...

**Systems offered from DCRS...**

*1st month of SaaS* included in your contract

*Industry Standard Peripherals* in Epson Printers and APG Cash Drawers

*Business Class Firewall* – Meraki MX64, to protect your POS Network and adhere to PCI Guidelines. First year subscription included with purchase. DCRS will manage ongoing subscriptions on your behalf.

*1000Mbps Ethernet Switch*

*Magnetic Cards* for your Staff included with every system

*12 month Hardware Depot warranty with DCRS.* No shipping hardware all over the world, simply bring to us and we’ll replace or fix, right here in our office.

*Not to exceed Professional Services and Installation (see below)*

*Fully Certified with POS Vendor.* Everything from Sales, to Installation to Support comes through DCRS, we use no 3rd parties or contractors.

**POS Implementation from DCRS...**

*Planning Meeting...* DCRS Project Manager and Dedicated Installation Specialist to review expectations of the system purchased

*Site Survey...* review existing setup to determine what can be reused or what needs to be installed from a networking standpoint.

*Database Programming...* Installation Specialist to program all menu items, modifiers, employees, taxes, etc.

*Database Review...* review menu design (face to face) to discuss any changes that might be needed prior to training.

*Management & Employee Training...* Installation Specialist to train all management staff and assist in all employee training at DCRS Solutions or Customers site.
Installation... Installation Specialist to install everything once you are ready to go live, no subcontractors needed!

Live Support... we will be there with you for your opening shift to ensure everything is setup to your liking, as well as review your first days reporting and credit card deposits.

Post Live Follow up... our Project Manager will follow up to ensure you are 100% satisfied and your Installation Specialists will be available should you have any questions during your first week.

Support, after the sale, from DCRS... all support employed by DCRS Solutions, no 3rd parties

DCRS Employees and our Certifications...

42 Years in Business

26 employees dedicated to POS

9 A+ Certifications from Comp TIA, certifies competency and commitment to computer repair and software

8 Net+ Certifications from Comp TIA, validates essential knowledge and skills needed to design, configure, manage and troubleshoot any wired and wireless networks.

PCI-SSC Qualified Integrators (8) and Reseller, Visa mandate that all Payment Application installs are performed only by a QIR Certified Company as of March 31, 2016.

3 SonicWALL Certified Security Administrators, certifies competency and commitment to managed subscription services.

2 Security+ Certifications from Comp TIA, validates security knowledge and skills. Covers the essential principles for network security and risk management.

5 MCP's (Microsoft Certified Professionals), certifies competency and commitment to a MS operating system.

13 PCI Wise Certifications, by RSPA, certifies individuals knowledge on PCI-Data Security Standards

24 x 7 Support, all employed by DCRS, no 3rd parties or subcontractors.


Cloud Systems features (all systems are not alike)...

Real Time Reporting, anytime, anywhere
Tablets for handheld and tableside ordering
Kitchen Display System, better manager incoming orders and improve turnaround times
Labor Reporting, automatically track hours, pay and productivity and simplify close out
CRM and Analytics, provides spend insights and improves marketing
Loyalty, integrated at payment to get more customers to opt in
Gift Card (both electronic and physical)
Inventory, real-time updates that make for better informed decisions to improve your bottom line
Online Ordering, eliminate vendor fees and easily push updates from your POS
Kiosk, simplify the guest ordering experience, improve speed of service and order turnaround
iBeacon Technology to alert guest when they enter a specific restaurant
Scan to Pay, give guests the power to control their checkout experience
EMV and NFC, avoid the liability shift from the card brands
Host Waitlist, send text message to a mobile phone when a guest's table is ready
Android and iOS
Notifications when orders are ready
Split Checks and Menu Items
Digital Receipts (email or text), cut down on paper costs
Product Mix Reporting to identify your top menu groups, items and modifiers
Quick Edit Mode
86 Countdown, to allow servers to know what you are out of
Delivery Dispatch, assign delivery orders, provide directions and manage drivers
Signature Capture, capture a customer's signature without a receipt, saving time and money
Caller ID, know who is calling so that a customer profile is available when the call is answered

"It's unwise to pay too much, but it's worse to pay too little. When you pay too much, you lose a little money--that is all. When you pay too little, you sometimes lose everything, because the thing you bought was incapable of doing the thing it was bought to do. The common law of business balance prohibits paying a little and getting a lot--it can't be done. If you deal with the lowest bidder, it is well to add something for the risk you run, and if you do that you will have enough to pay for something better." --John Ruskin (1819-1900).
toast

Product Overview

- Built for commercial use and powered by Android
- Cloud-based updates and monitoring
- Platform enables extensibility & scalability
- Continuing to invest in and scale the platform
- Security is our top priority
- Leader in restaurant customer success
Toast Steam lines the Entire Restaurant Experience

Next Generation POS Experience  Synchronized Cooking, Service & Delivery  Real-Time Analysis of Sales, Labor, and Menu Performance  Full Lifecycle Marketing
Partner Ecosystem for Best-of-Breed Capabilities

Front of House (revenue-generation focus)

Back of House (operations focus)

B2B Ordering/Drywall Ordering/Drywall
Reservations & Events
Loyalty & Marketing
Labor & Payroll Management
Reporting & Inventory Mgmt
Accounting & Bookkeeping
Distributors

Enterprise
Mid Market
SMB
HARDWARE SOLUTIONS

TOAST POINT OF SALE

✓ Runs on Android
✓ Intuitive and Easy to Use
✓ Restaurant Grade Hardware
✓ Table Management
✓ Real-time Feedback Alerts
✓ Real-time Reporting
✓ Digital Receipts
✓ Hardwired Terminals with Offline Mode
✓ Split Checks
✓ Orders Fire Directly to your KDS
HARDWARE SOLUTIONS

TOAST GO!

- Boost Revenue, Increase Efficiency and delight your guest!
- Pocket-Friendly
- Order Notifications
- Tableside Payments
- Fire Directly to the Kitchen
- Drop & Spill Resistant
- 14 Hour Battery Life
- Automatic Menu Updates
- Real-time Feedback Alerts
HARDWARE SOLUTIONS

KITCHEN DISPLAY SYSTEM

- Double Tap Fulfill, Single Recall
- Fire by Prep Time
- Route to Stations by Dine In or Out
- Speed of Prep Reporting by Station
- Restaurant grade hardware
- Integrated with All Incoming Orders
- Color-coded Modifiers
- Texts Guests When the Order is Ready
- Foreign Language Support
- Integrates directly with Toast Go™
REAL-TIME REPORTING

✓ Real-time sales, menu, and labor data
✓ No more waiting days or weeks to review results.
✓ Automatic nightly email
✓ Key business metrics sent directly to your inbox each night.
✓ One place for all your data
✓ All the insights you're looking for in one report - no downloading or extra analyses required.
REPORTING & ANALYTICS

REAL-TIME REPORTING

✓ Cloud-enabled reporting
✓ Access your data anytime, anywhere.
✓ Mobile-optimized—Pull up your reports on your phone if you’re on the go.
✓ Best-in-class user interface
✓ Easily compare sales across multiple locations or time periods in a single report.
✓ View performance on specific days of the week to measure the impact of holidays or promotions.
✓ Track sales of a menu item across all your menus, whether in-store or online.
GUEST FEEDBACK

Improve Operations, Coach Staff & Avoid Negative reviews with GUEST FEEDBACK
✓ Immediate feedback -Thumbs up/down feature prompts easy rating.
✓ Seamless integration -Use on Toast Go, Toast Online Ordering or Toast Kiosk.
✓ Build customer relationships -Opt-in guest info capture for manager follow up.
✓ Detailed feedback report-Identify trends in feedback to improve hospitality.
✓ Prompt resolution-Immediately resolve negative experiences in person or via email.
✓ Guest promotions-Turn happy guest into regulars by including them in promotional campaigns.
✓ Analyze performance trends -Reward top servers providing stellar service.
✓ Give constructive feedback-Use comments as an opportunity to train underperforming staff.
✓ Feedback detail -Uncover what influenced guest reviews, from level of service to atmosphere.
LABOR MANAGEMENT

Easy Access to a Single, Centralized Hub for PAYROLL & HR

✓ Simplified payroll and taxes
  ✓ Built-in tools make complex processes simple, while keeping the functionality restaurants need most.

✓ Seamless time tracking
  ✓ Easy manager approval for employee punch data, shift swaps, and PTO requests that sync to payroll.

Single platform for labor

✓ Manage all stages of the employee lifecycle in one system, with robust reporting and dashboards to boot.

✓ Benefits administration
  ✓ Manage open enrollment and empower your team with plans tailored to the size of your restaurant.
Reduce time spent on Labor Management with Payroll that syncs with POS

✓ Easier new hire processes

✓ One employee profile across POS and payroll systems means no more double-entering new hire information.

✓ Faster timesheet approval

✓ Automated tip distribution eliminates time-consuming manual edits at the end of each shift.

✓ Hours sync to payroll

✓ No external files or manual entry of hours, so running payroll is smooth and simple.
REAL-TIME REPORTING

- Real-time sales, menu, and labor data
- No more waiting days or weeks to review results.
- Automatic nightly email
- Key business metrics sent directly to your inbox each night.
- One place for all your data
- All the insights you're looking for in one report - no downloading or extra analyses required.
REPORTING & ANALYTICS

REAL-TIME REPORTING

✓ Cloud-enabled reporting
✓ Access your data anytime, anywhere.
✓ Mobile-optimized—Pull up your reports on your phone if you're on the go.
✓ Best-in-class user interface
✓ Easily compare sales across multiple locations or time periods in a single report
✓ View performance on specific days of the week to measure the impact of holidays or promotions.
✓ Track sales of a menu item across all your menus, whether in-store or online.
GUEST FEEDBACK

Improve Operations, Coach Staff & Avoid Negative reviews with GUEST FEEDBACK

✅ Immediate feedback - Thumbs up/down feature prompts easy rating.

✅ Seamless integration - Use on Toast Go, Toast Online Ordering or Toast Kiosk.

✅ Build customer relationships - Opt-in guest info capture for manager follow up.

✅ Detailed feedback report - Identify trends in feedback to improve hospitality.

✅ Prompt resolution - Immediately resolve negative experiences in person or via email.

✅ Guest promotions - Turn happy guest into regulars by including them in promotional campaigns.

✅ Analyze performance trends - Reward top servers providing stellar service.

✅ Give constructive feedback - Use comments as an opportunity to train underperforming staff.

✅ Feedback detail - Uncover what influenced guest reviews, from level of service to atmosphere.
LABOR MANAGEMENT

Easy Access to a Single, Centralized Hub for PAYROLL & HR

✓ Simplified payroll and taxes
  ✓ Built-in tools make complex processes simple, while keeping the functionality restaurants need most.

✓ Seamless time tracking
  ✓ Easy manager approval for employee punch data, shift swaps, and PTO requests that sync to payroll.

Single platform for labor

✓ Manage all stages of the employee lifecycle in one system, with robust reporting and dashboards to boot.

✓ Benefits administration
  ✓ Manage open enrollment and empower your team with plans tailored to the size of your restaurant.
PAYROLL PROCESSING

Reduce time spent on Labor Management with Payroll that syncs with POS

✓ Easier new hire processes
  ✓ One employee profile across POS and payroll systems means no more double-entering new hire information.

✓ Faster timesheet approval
  ✓ Automated tip distribution eliminates time-consuming manual edits at the end of each shift.

✓ Hours sync to payroll
  ✓ No external files or manual entry of hours, so running payroll is smooth and simple.
ONLINE ORDERING
Eliminate Extra Tablets & Save money with integrated Online Ordering
✓ No 3rd-party commission on orders
  ✓ Engage your guests and avoid the fees that third-party platforms often charge.
✓ No extra staffing required
  ✓ Eliminate the need for extra staffing as orders go directly to the kitchen.
✓ Full menu visibility with prompted modifiers
  ✓ Easily display add-ons like extra chicken or a dessert to help increase average check size.

A Convenient Online Ordering Platform built into your POS
✓ Mobile-responsive site
  ✓ Guests can order from any device from the office, at home, or on the go.
✓ Customizable restaurant branding
  ✓ Ensure your digital brand matches the look and feel of your restaurant.
✓ Modifiers and special requests
  ✓ Personalized order changes go straight to the kitchen – no crossed wires here.
✓ Saved credit cards and user profiles
  ✓ Make it simple for your guests to checkout.
ONLINE ORDERING
Eliminate Extra Tablets & Save money with integrated Online Ordering

✓ No 3rd-party commission on orders
  ✓ Engage your guests and avoid the fees that third-party platforms often charge.

✓ No extra staffing required
  ✓ Eliminate the need for extra staffing as orders go directly to the kitchen.

✓ Full menu visibility with prompted modifiers
  ✓ Easily display add-ons like extra chicken or a dessert to help increase average check size.

A Convenient Online Ordering Platform built into your POS

✓ Mobile-responsive site
  ✓ Guests can order from any device from the office, at home, or on the go.

✓ Customizable restaurant branding
  ✓ Ensure your digital brand matches the look and feel of your restaurant.

✓ Modifiers and special requests
  ✓ Personalized order changes go straight to the kitchen – no crossed wires here.

✓ Saved credit cards and user profiles
  ✓ Make it simple for your guests to checkout.
Grow your business and keep your menu in sync with integrated digital ordering solutions

- Real-time menu sync
  - Updates to inventory and menu items are pushed seamlessly to all menus – both in the restaurant and online.

- POS, KDS, and Caller ID integrations
  - Save minutes on each order by sending all tickets directly to your kitchen.

- Customizable ordering hours
  - Set windows for accepting takeout and delivery orders – like weekends only – to ensure a great guest experience overall.

- Delivery zones
  - Dispatch your drivers to complete deliveries within a pre-set zone.
toast

GUEST REWARDS & LOYALTY

Simplify Loyalty Program Management

Intuitive Loyalty Opt-in
✓ Opt-in on checkout screen
  ✓ Enter an email when checking out to sign up.
✓ Rewards points lookup
  ✓ Diners can log in to check loyalty progress anytime.

Easy Access to Loyalty Points
✓ Points-based rewards
  ✓ Customize sign up bonuses, set accrual and redemption rates, and offer birthday rewards.
✓ One flat fee per month
  ✓ Don't be surprised by your loyalty program fees.

Customer Order History & Info
✓ Credit Card-linked program
  ✓ Guests seamlessly accrue points with each swipe of their credit card. No need to carry a loyalty card or sign-in on each visit
✓ Loyalty Reporting
  ✓ Get a clear picture of your regulars with Loyalty Reporting
GIFT CARDS
A Modern Gift Card Program that fits your Restaurant

Easy to Sell, Track & Manage
✓ E-Commerce Sale
  ✓ Sell Gift Cards in your restaurant & Online
✓ Simple to Redeem
  ✓ Scan or Key-In the gift card number to pay with a gift card

Let your guests choose the option that works for them.
✓ Email & Text Gift Cards
  ✓ Increase revenue with easy-to-give digital gift cards
✓ Physical Cards
  ✓ Offer your guests branded physical gift cards tailored to your restaurants brand
✓ Gift Card Balance lookup
  ✓ Guest can manage and access gift card balances online
INVENTORY

Drive down your food costs with a simple Inventory Tool

- Log what you're using and wasting to protect your bottom line
  - Inventory value report
    - Understand the exact value of the goods on your shelves.
  - Variance and COGS reports
    - Compare your actual performance against your theoretical performance and analyze your food cost percentage
  - Waste Tracking
    - Tools to help you reduce over-portioning, over-buying, and theft

All your inventory data in one place!

- Integrated Tool
  - Inventory that's always in sync-no data export needed
- Menu Engineering
  - Shed low-performing items & run experiments to improve profitability
- Shelf Layout
  - Map your inventory count to your actual kitchen setup
PARNTER INTEGRATIONS

Run your restaurant at full speed with technology partners certified to work with Toast
✓ LABOR
✓ RESERVATIONS
✓ INVENTORY
✓ ACCOUNTING
✓ SECURITY
✓ ANALYTICS
✓ MARKETING & CRM
✓ ONLINE ORDERING
✓ LOYALTY & REWARDS
✓ PAYROLL
✓ MOBILE PAY
✓ GIFT CARDS

Restaurant365  PAYTRONIX  GRUBHUB
YELLOW DOG  HotSchedules  LevelUp  SHIFTS
GUEST REWARDS & LOYALTY

Simplify Loyalty Program Management

Intuitive Loyalty Opt-in
✓ Opt-in on checkout screen
  ✓ Enter an email when checking out to sign up.
✓ Rewards points lookup
  ✓ Diners can log in to check loyalty progress anytime.

Easy Access to Loyalty Points
✓ Points-based rewards
  ✓ Customize sign up bonuses, set accrual and redemption rates, and offer birthday rewards.
✓ One flat fee per month
  ✓ Don't be surprised by your loyalty program fees.

Customer Order History & Info
✓ Credit Card-linked program
  ✓ Guests seamlessly accrue points with each swipe of their credit card. No need to carry a loyalty card or sing-in on each visit
✓ Loyalty Reporting
  ✓ Get a clear picture of your regulars with Loyalty Reporting
GIFT CARDS

A Modern Gift Card Program that fits your Restaurant

Easy to Sell, Track & Manage
✓ E-Commerce Sale
  ✓ Sell Gift Cards in your restaurant & Online
✓ Simple to Redeem
  ✓ Scan or Key-In the gift card number to pay with a gift card

Let your guests choose the option that works for them.
✓ Email & Text Gift Cards
  ✓ Increase revenue with easy-to-give digital gift cards
✓ Physical Cards
  ✓ Offer your guests branded physical gift cards tailored to your restaurants brand
✓ Gift Card Balance lookup
  ✓ Guest can manage and access gift card balances online
Run your restaurant at full speed with technology partners certified to work with Toast
✓ LABOR
✓ RESERVATIONS
✓ INVENTORY
✓ ACCOUNTING
✓ SECURITY
✓ ANALYTICS
✓ MARKETING & CRM
✓ ONLINE ORDERING
✓ LOYALTY & REWARDS
✓ PAYROLL
✓ MOBILE PAY
✓ GIFT CARDS

toast

PARNTER INTEGRATIONS

Restaurant365
PAYTRONIX
GRUBHUB
YELLOW DOG
HotSchedules
LevelUp
SHIFTS
GUEST REWARDS & LOYALTY

Simplify Loyalty Program Management

Intuitive Loyalty Opt-in
✓ Opt-in on checkout screen
  ✓ Enter an email when checking out to sign up.
✓ Rewards points lookup
  ✓ Diners can log in to check loyalty progress anytime.

Easy Access to Loyalty Points
✓ Points-based rewards
  ✓ Customize sign up bonuses, set accrual and redemption rates, and offer birthday rewards.
✓ One flat fee per month
  ✓ Don't be surprised by your loyalty program fees.

Customer Order History & Info
✓ Credit Card-linked program
  ✓ Guests seamlessly accrue points with each swipe of their credit card. No need to carry a loyalty card or sing-in on each visit
✓ Loyalty Reporting
  ✓ Get a clear picture of your regulars with Loyalty Reporting.
GIFT CARDS

A Modern Gift Card Program that fits your Restaurant

Easy to Sell, Track & Manage
✓ E-Commerce Sale
  ✓ Sell Gift Cards in your restaurant & Online
✓ Simple to Redeem
  ✓ Scan or Key-In the gift card number to pay with a gift card

Let your guests choose the option that works for them.
✓ Email & Text Gift Cards
  ✓ Increase revenue with easy-to-give digital gift cards
✓ Physical Cards
  ✓ Offer your guests branded physical gift cards tailored to your restaurants brand
✓ Gift Card Balance lookup
  ✓ Guest can manage and access gift card balances online
toast

CLIENT REFERENCES

MISSION Taco Joint

Pastaria

17th STREET BBQ

Crushed Red
Artfully Chopped Craft Salads
toast

CLIENT REFERENCES

Three Kings

SALT + SMOKE
BBQ BOURBON BEER

DRUNKEN FISH
SUSHI RESTAURANT & LOUNGE

Companion

CIRCLE 7 RANCH
Both DCRS and Toast live by the motto to be obsessed with Restaurant Success.

The core of Toast's vision for hospitality says it best, guest first and data driven to allow your team to deliver an amazing guest experience. From a stability standpoint, Toast continues to attract the top investment firms out there, with their latest round (D) of funding led by T. Rowe Price.

"The way restaurants serve their customers is going through a fundamental change, and the technology that enables restaurant operations must respond to these new demands, Toast does this" said Henry Ellenbogen, portfolio manager of T. Rowe Price New Horizons Fund.

Together, we look to show you why so many other multiunit restaurants in the St. Louis market & beyond have made the move to DCRS and Toast.

We appreciate the opportunity and look forward to learning more about how we can help you achieve your goals!
### The Basics

**What is Offline Mode?**
In the case of a network or internet disruption, Offline Mode allows you to continue to place orders, print receipts, and take credit card payments until the connection is reestablished.

**How does it work?**
When a loss of connectivity is detected, your terminals will automatically shift into Offline Mode. The Toast app will notify you when your system is operating in Offline Mode.

**How do I take payments in Offline Mode?**
Credit card payments can be taken as usual. However, payments will not be authorized until the internet connection is restored. This means that you will not be notified of rejected payments until your system is back online.

*Keep in mind that you are responsible for any declined, expired, or disputed payments while operating in Offline Mode.*

#### What works in Offline Mode?
- Sending orders to kitchen printers
- Printing receipts at terminals
- Opening cash drawers
- Processing credit cards as "offline"*
- Entering credit card or non-cash tips onto payments

#### What doesn't work in Offline Mode?
- Clocking in or clocking out on separate devices
- Logging in or logging out of the Toast app
- Syncing and sending orders between tablets and KDS screens
- Syncing and accessing customer data and online reports
- Shift Review
- Processing gift cards for payments
- Looking up customer information for take-out or delivery orders

For training material and status updates, visit hub.toasttab.com | Contact Toast Support at 617.682.0225
Best Practices

Auto-Capturing Payments
Auto-capturing payments is a process that occurs automatically every night. Credit card payments authorized throughout the day are captured into a batch and sent to the processor. After this happens, payments cannot be updated with tips or otherwise adjusted in any way.

If your system does not reestablish connectivity by the end of your business day, please contact Toast support to temporarily disable the auto-capture process. We want to ensure that we do not capture your payments until you've had the time to properly update them.

Toast Support can be reached by email at support@toasttab.com or by phone at 617.682.0225.

1. Each employee should choose a single terminal to place and update orders.
   Since your terminals can't sync with each other in Offline Mode, orders taken on one terminal won't appear on other terminals. We recommend that each employee choose a single terminal to place and update orders. More than one server can work on a single terminal, but it's important that they only use one while in Offline Mode.

2. Make sure to have a back-up printer if you use Kitchen Display Screens.
   If you use a KDS in your kitchen, it's important to have a printer set up as a back-up to print kitchen tickets because KDS requires the internet to display orders. Printing kitchen tickets while in Offline Mode can be configured in Kitchen Setup in Toast's backend.

3. Do not clear app data or uninstall the Toast app.
   Do not uninstall the Toast app, command Toast to resync data, or clear the app data. This will result in a loss of data - including credit card payments - that cannot be recovered.

4. Contact Toast support with your device ID.
   In the event that you cannot repair your internet connection, contact Toast support with your device ID. This can be found on your device's dashboard. Scroll to Support > Device Info > App > Device ID.

Note
In Offline Mode, enter credit card tips as you normally would. Do not log out of the Toast app. Once you log out, you cannot go back in.

Troubleshooting Tips

1. Ensure your device is using Toast's secured network.
   If your system normally runs on WiFi, make sure your device is using Toast's secured network. Open your WiFi settings and ensure that you've selected the network that contains securedtoastnetwork in its name.

2. Turn off the connection you're not using.
   If your system normally runs through Ethernet, it's important that your WiFi settings are OFF. Alternatively, if you are connected via WiFi, make sure that your Ethernet settings are OFF.

3. Check the condition of your router.
   Make sure your router is lit up with a white light. If it shows a different colored light, try un-plugging the power cord, plugging it back in. If the problem persists, unplug the ethernet cord, then plug it back in.

For training material and status updates, visit hub.toasttab.com | Contact Toast Support at 617.682.0225
Attachment #1
PCI Data Security Standards REQUIREMENTS and RESPONSIBILITIES

DCRS recommends all Merchants take the time to review the terms of the "Merchant Agreement" that they signed with their Credit Processor (or Acquirer), to determine their specific responsibilities and liabilities. The responsibility for meeting the Requirements for PCI Compliance rests with the Merchant.

However, a DCRS Support Plan is designed to assist with a portion of these 12 major PCI Requirements. When a Support Plan site requests assistance, DCRS can connect remotely to confirm the current status of specific items related to some of the PCI Requirements. Findings can be provided via email by a specific DCRS individual that is knowledgeable in most of the general PCI Requirements.

For Non-Support Plan sites, DCRS can confirm the software version, the validation status of the version, and explain the areas of responsibility that the DCRS Support Plan is designed to assist (as noted below), including Managed Services that provide secure remote connections, as well as protect and update our SonicWall Firewalls and AntiVirus offerings.

The PCI Requirements that a POS Vendor can best assist the Merchant are the following (a maximum of 7 out of the 12 high-level Requirements, as outlined in PCI PA-DATA Security Standard document), listed in DCRS order of importance:

- **Requirement 3**: Protect stored cardholder data. Insure a PCI-Validated Payment Application software version is installed. The 'availability' of such relates to the Payment Application software manufacturer (typically POS Vendor). Merchants must insure their system is updated with a properly validated version, and are responsible for annual rotation of encryption keys.

- **Requirement 6**: Develop and maintain secure systems and applications. Both the Payment Application software and Operating System should have the latest security patches installed. The 'availability' of such relates to the Payment Application software manufacturer (POS Vendor) and the Operating System manufacturer (typically MICROSOFT). Merchants must insure their system is updated with both the Application and Operating System security patches, when available.

- **Requirement 4**: Encrypt transmission of cardholder data across open, public networks. Having a PCI-validated POS software version installed will help provide this (see Requirement 3).

- **Requirement 2**: Do not use vendor-supplied defaults for system passwords and other security parameters. Although the POS Vendor should communicate this at installation, Merchants are responsible to ensure secure passwords are being used by their employees after installation.

- **Requirement 1**: Install and maintain a firewall configuration to protect cardholder data. Insure the POS Payment system is installed inside an internal network zone, segregated from any demilitarized zone (DMZ), with a separate Firewall that has packet filtering with Internet traffic restrictions. DCRS can install a SonicWall firewall to meet this requirement. Merchants that install their own firewall, allow their SonicWall Subscription to expire, or after the installed SonicWall configuration—take sole responsibility.

- **Requirement 5**: Use and regularly update anti-virus software or programs. DCRS can install AntiVirus Subscription Services to meet this requirement. Merchants that install their own (or allow their Antivirus Subscription to expire) take sole responsibility.

- **Requirement 8**: Assign a unique ID to each person with computer access. DCRS can install Live Alert & Connect and Live Manager, which has two-factor authentication for remote access. Merchants that install their own Remote Access, or allow other vendors remote access, take sole responsibility. Merchants remain responsible for the other multiple responsibilities associated with this requirement.

The remaining 5 high-level Requirements are exclusively Merchant-Responsible. Over 200 sub-requirements are part of the 12 high-level Requirements. There is a limit to what a POS Vendor can do, other than to advise:

- **Requirement 7**: Restrict access to cardholder data by business need to know
- **Requirement 9**: Restrict physical access to cardholder data
- **Requirement 10**: Track and monitor all access to network resources and cardholder data
- **Requirement 11**: Regularly test security systems and processes
- **Requirement 12**: Maintain a policy that addresses information security for all personnel

True security requires 100% consistency in the execution of procedures. However, not all security can be totally automated and some security practices must involve people. Unfortunately, people are fallible, so 100% consistency is not possible when people are involved. Security is not perfect, but is about managing and minimizing risks.

The PCI Security Standards Council certifies organizations that assess and validate adherence to PCI Security Standards. Qualified Security Assessors (QSA) are organizations qualified by PCI to assess a Merchant's compliance to PCI DSS. Merchants seeking this type of assessment should contact a QSA.

6.14.14
2605 METRO BOULEVARD # ST. LOUIS MO 63049  www.DCRS.com  314.739.8868  800.291.0168
Customer Support User's Guide
Customer Information & Support Level Guidelines

Updated: 2.8.18
# Table of Contents

**TABLE OF CONTENTS**  ................................................................................................................................. 2

**GENERAL INFORMATION** ............................................................................................................................. 3

- OUR COMMITMENT TO SUPPORT .................................................................................................................. 3
- QUESTIONS TO ASK YOURSELF ..................................................................................................................... 3
- BENEFITS OF A SUPPORT PLAN .................................................................................................................... 3
- SUPPORT PLAN CHOICES ................................................................................................................................. 4
- PLAN A. ON-SITE (9-DAY) REPAIR, LIVE HELP with applicable MANAGED SUBSCRIPTION SERVICES ....... 4
- PLAN B. ON-SITE (5-EODAY) REPAIR, LIVE HELP with applicable MANAGED SUBSCRIPTION SERVICES .... 4
- PLAN C. DEPOT REPAIR, LIVE HELP with applicable MANAGED SUBSCRIPTION SERVICES ...................... 6
- PLAN A, B, C. Inclusions & Exclusions ............................................................................................................... 6
- PLAN D. LIVE HELP with applicable MANAGED SUBSCRIPTION SERVICES .................................................. 6
- RENEWAL, PAYMENT SCHEDULES, CANCELLATION .................................................................................. 6
- PARTS REPAIR .................................................................................................................................................. 9
- DEFINITIONS ...................................................................................................................................................... 7

**LIVE HELP PROCEDURES** ............................................................................................................................... 8

- LIVE HELP ..................................................................................................................................................... 8
- WHO CAN CALL? ........................................................................................................................................... 8
- BEFORE YOU CALL ....................................................................................................................................... 8
- CALL NUMBER ............................................................................................................................................. 9
- RESPONSE AND RESOLUTION TIMES ........................................................................................................... 9
- PRIORITY LEVELS ......................................................................................................................................... 9
- ESCALATION AND RESOLUTION .................................................................................................................. 9 & 10
- CALL CLOSURE/RESOLUTION ......................................................................................................................... 10

**LIVE HELP CENTER INFORMATION** .............................................................................................................. 11

- HOURS OF OPERATION .................................................................................................................................... 11
- CONTACTING THE LIVE HELP CENTER ......................................................................................................... 11
- ESCALATION .................................................................................................................................................... 11
- POSITIVE FEEDBACK ...................................................................................................................................... 11

**SERVICE LEVEL MEASUREMENT** .................................................................................................................. 12

- AVERAGE SPEED OF ANSWER ..................................................................................................................... 12
- FRONT LINE RESOLUTION RATE .................................................................................................................... 12
- CALL RESOLUTION RATE ............................................................................................................................... 12

**SCOPE OF LIVE HELP & MANAGED SUBSCRIPTION SERVICES** ..................................................................... 13

- WHEN IS SUPPORT AVAILABLE? .................................................................................................................... 13
- WHO IS SUPPORTED? ..................................................................................................................................... 13
- WHAT IS SUPPORTED? .................................................................................................................................... 13
- LIVE ALERT & CONNECT (REMOTE ACCESS) and LIMITATION OF LIABILITY .................................................. 13
- APPLICATION SUPPORT & SOFTWARE UPDATE LICENSE (SUL) ...................................................................... 14
- OPERATING SYSTEM AND NETWORK SUPPORT ............................................................................................ 15
- INTERFACE SUPPORT ..................................................................................................................................... 15
- THIRD PARTY APPLICATION SUPPORT .......................................................................................................... 16
- HARDWARE DISPATCHING AND SUPPORT ..................................................................................................... 17
- CREDIT AUTHORIZATION APPLICATION SOFTWARE SUPPORT ....................................................................... 17
- MANAGED SUBSCRIPTION SERVICES ............................................................................................................... 16
- TIME & MATERIAL CHARGES (NON-COVERED SITES or BILLABLE SUPPORT) .................................................. 16
- HOURLY TRAVEL & LABOR RATES .................................................................................................................... 19

**CUSTOMER RESPONSIBILITIES** ...................................................................................................................... 20

- GUIDELINES .................................................................................................................................................... 20
- NOTE .................................................................................................................................................................. 20
General Information

Our Commitment to Your Support

We understand the demands and pressures of the retail and hospitality industries and know your success depends on how effectively you can put our products to work. Sharing information, being responsive as well as accessible, keeping your system up-to-date, and working through problems and solutions together are a part of our commitment to providing you with an effective, comprehensive support plan.

Questions to Ask Yourself

Can your company afford to be without this system for a day or more?

Would you agree that proper planning for support, as with planning to build a home or planning just about anything else, is necessary to be successful?

Knowing we cannot respond on a moment’s notice without proper planning, what do you tell your staff and customers when the system cannot be fixed quickly because you have not considered a Support Plan?

Are you aware that we offer several Support Plan choices after your warranty period expires?

What about future software versions, software maintenance and corrections, and their availability?

If you are using integrated Credit Authorization Software, did you know the Merchant Agreement you signed with your Credit Processor (or Acquirer) holds you responsible and liable to maintain PCI Compliance requirements?

Even with a PCI-Validated Payment Application software version installed by us, how will you maintain your Firewall subscription, Anti-Virus subscription, Anti-Spyware, Intrusion Protection, and Operating System updates, which are just a few of the 12 requirements (with over 220 sub-requirements) necessary to maintain PCI Compliance?

Benefits of a Support Plan

- A Plan budgets your maintenance and support expenses accurately, providing a fixed cost for a period of time and passing the risk of failure to us.

- A Plan reduces your maintenance and repair costs, since the Plan fee is based on the estimated average repair costs and the major repair risk is spread over many years.

- A Plan avoids the costly expense of having to replace a major component.

- A Plan provides LiveHelp, for 7 days per week up to Midnight, for 365 days per year, to answer your software questions.

- A Plan includes Managed Subscription Services: Annual software subscriptions to maintain LiveProtect (for the SonicWall firewall), LiveAlert&Connect, LiveManager Connection Option, Disaster Recovery Protection option, LiveAntiVirus (to Servers & PCs), LiveBackup option (office backup service for ORACLE|MICROS RES), Credit Help option (Merchant Link Network Credit Support for Oracle|Micros or Retail Software Credit Support), and more.

- By planning for support, you will get preferred response time, since we have anticipated your needs.

- Software Update License with Software Vendor Support (SUL): ADDITION to Support Plans. Oracle Micros SUL, or other Software vendor, provides access to Software Corrections and Escalations, as Oracle and others provide support only to systems covered by an SUL. SUL should be included with a DCRS Support Plan.
Support Plan Choices

To assure you support when you need it, we offer 4 Plan choices: 2 Onsite, a Depot (Ship-In), and our LiveHelp Plan. All 4 plans include applicable Managed Subscription Services. These Plans provide you with the convenience of contacting us for assistance to your problems that occur, as well as the maintenance of the many necessary Managed Subscription Services. Oracle Micros Software Update License with Software Vendor Support (SUL) is a suggested ADDITION to Oracle Micros Support Plans (or for any other Software vendor).

We provide coverage for 24 hours a day, 365 days per year, via a toll free 800 number. Our Support Center is made up of industry and product specialists who understand retail and hospitality businesses and have either come directly from within, or have received training specific to, the hospitality or retail industries. You will be speaking with not only someone who understands the product you are using, but also someone who understands the details of your business. Someone who understands how impacting problems can be and the urgency in getting those problems resolved.

Plans can be customized for national and regional accounts with multiple remote sites, large single sites, or sites with unusual needs. Remote site plans may include utilizing our Depot Plan for hardware service—or onsite hardware support plans through national third-party firms—in combination with our LiveHelp Plan. Rates can vary in remote markets (200 miles from o St. Louis). Your Account Representative can provide details.

You, as End-User and Merchant, acknowledge that the security and protection of your System and Data, including protections against unauthorized access, obtaining and maintaining compliance with the PAYMENT CARD INDUSTRY (PCI) PAYMENT APPLICATION DATA SECURITY STANDARDS (PA-DSS), as well as any Credit or Debit Card Rules, Regulations and Laws, is solely and entirely your responsibility.

Plan A. ONSITE (6-DAY) FULL: 7-Day LiveHelp & Parts, 6-Day Onsite Labor, and applicable MANAGED SERVICES (Software Update License OPTIONAL)

Service to covered equipment is provided from 8am-6pm Central, Monday-Saturday, with travel to and from your site included. Service to Mobile hardware can only be provided directly from the Manufacturer. Full LiveHelp staffing (Level 1 & 2) is available from 8am-6pm Central, Monday-Friday, and on-call Technicians are available outside of those hours. Applicable Managed Subscription Services are included. LiveHelp from Midnight-8am is chargeable with our standard plan. This Plan is available for sites within 200 miles* of DCRS. To proactively perform tasks necessary to execute Plans, Customers subscribing to LiveAlert&Connect authorize DCRS personnel to remotely access their supported system at will. Customers preferring not to authorize DCRS personnel this access must not only take responsibility to communicate this desire to DCRS, but also acknowledge that the alternative may cause delays in the execution of these Plans.

Plan B. ONSITE (5-DAY) WEEKDAY: 7-Day LiveHelp & Parts, 5-Day Onsite Labor, and applicable MANAGED SERVICES (Software Update License OPTIONAL)

Service to covered equipment is provided from 8am-6pm Central, Monday-Friday, with travel to and from your site included. Service to Mobile hardware can only be provided directly from the Manufacturer. Full LiveHelp staffing (Level 1 & 2) is available from 8am-6pm Central, Monday-Friday, and on-call Technicians are available outside of those hours. Applicable Managed Subscription Services are included. LiveHelp from Midnight-8am is chargeable with our standard plan. This Plan is available for sites within 200 miles* of DCRS. To proactively perform tasks necessary to execute Plans, Customers subscribing to LiveAlert&Connect authorize DCRS personnel to remotely access their supported system at will. Customers preferring not to authorize DCRS personnel this access must not only take responsibility to communicate this desire to DCRS, but also acknowledge that the alternative may cause delays in the execution of these Plans.

*MILEAGE NOTE: There are no response time guidelines for sites outside of Zone 3 (125+ miles from Servicing Office). Service is provided on a “reasonable effort” basis and arrival should not be expected sooner than 24 hours from time of request. To avoid delays, consider purchasing Spares and choosing Plan C. DEPOT.
Plan C. DEPOT (Ship/Carry-In): 7-Day LiveHelp, 5-Day Depot Repair & Parts, and applicable MANAGED SERVICES (Software Update License OPTIONAL)

Service to covered equipment is provided at our facility from 8am-5pm Central, Monday-Friday. Service to Mobile hardware can only be provided directly from the Manufacturer. Full LiveHelp staffing (Level 1 & 2) is available from 8am-5pm Central, Monday-Friday, and on-call Technicians are available outside of those hours. Applicable Managed Subscription Services are included. LiveHelp Labor from Midnight to 8 am is chargeable with our standard plan. To proactively perform tasks necessary to execute Plans, Customers subscribing to LiveAlert&Connect authorize DCRS personnel to remotely access their supported system at will. Customers preferring not to authorize DCRS personnel this access must not only take responsibility to communicate this desire to DCRS, but also acknowledge that the alternative may cause delays in the execution of these Plans.

For this Plan to be successful, you should purchase Spares for critical components (loaned equipment is not provided while service is performed), take an active role in performing a portion of their overall hardware support, and have Service Management training or approval, prior to the start. You are responsible for incoming freight costs, and we are responsible for return ground freight. See your Account Representative for our separate documents entitled "DEPOT SUPPORT PLAN" for more details.

For Plan A, B, or C, "Service to covered equipment" INCLUDES:

- All parts repaired, exchanged or replaced. Supplies are excluded. Replacement parts may be manufacturer's new or reconditioned parts.
- All labor to determine the problem, and labor associated with repair, exchange or replacement.
- Travel to your site for onsite plans. It is understood that your equipment is in good working order on the effective date of any Hardware Support Plan. We reserve the right to use new or reconditioned parts in order to make repairs to the hardware. Equipment out of Warranty or Support Coverage is subject to a chargeable inspection and you are then responsible for any necessary repairs prior to acceptance and start.

For Plan A, B, or C, "Service to covered equipment" does NOT Include:

- Repair costs (parts and labor) resulting from improper use, foreign objects, tampering, unauthorized parts, liquid, fire, lightning, wind, storm, act of God, accidental damage, or other perils. Some of these may be covered by your business insurance. Additionally, repair costs (parts and labor) caused by power fluctuations, improper electrical wiring, or improper data cabling, is not included.
- Service on Mobile products covered by DIRECT MANUFACTURER WARRANTIES for all 3rd Party products include: Micros Tablet-E Series (Dell), DT Research Tablet, Motorola Handheld, Epson Handheld Printer, Toast Handheld (Samsung), MobileBytes iPad (Apple) etc. (details on our website).
- Manufacturer Warranty Claim Procedures must be followed when a problem appears in any of these 3rd Party products, as Service is unavailable for these products through DCRS.
- Services necessitated by computer viruses and/or security breaches.
- Supplies consisting of ribbons, keys, drawer insert tills, keyboard covers, batteries, magnetic cards, and other accessories: Replacement of etched monitors, or a Coin Dispenser's "magazine/canister" accessory.
- Labor outside of designated Plan hours and on certain designated Holidays as follows: New Year's Day (January 1st), unless it falls on a Saturday or Sunday), Memorial Day (last Monday in May), Independence Day (July 4th), Labor Day (first Monday in September), Thanksgiving Day (fourth Thursday in November), Christmas Day (December 25th unless it falls on a Saturday or Sunday). When January 1st or December 25th falls on a Saturday (or Sunday), the corresponding Friday (or Monday) is designated as a Holiday.
- See "Scope of LiveHelp & Managed Subscription Services" (on page 13 of the FULL VERSION of the Customer Support User's Guide) for specific details on what is and is not covered under these Plans, and a Software Update License with Software Vendor Support (SUL) is suggested.
Plan D. **LiveHelp: 7-Day LiveHelp, and applicable MANAGED SERVICES (Software Update License OPTIONAL)**

Full **LiveHelp** staffing (Level 1 & 2) is available from 8am-5pm Central, Monday-Friday, and on-call Technicians are available outside of those hours. Applicable Managed Subscription Services are included. **LiveHelp** from Midnight-8am is chargeable with our standard plan. To proactively perform tasks necessary to execute Plans, Customers subscribing to **LiveAlert&Connect** authorize DCRS personnel to remotely access their supported system at will. Customers preferring not to authorize DCRS personnel this access must not only take responsibility to communicate this desire to DCRS, but also acknowledge that the alternative may cause delays in the execution of these Plans.

This program does not include any hardware repair labor, parts, or any onsite visits necessary to correct problems, and Software Update License (SUL) is an OPTION to all Oracle Micros (and other Software Vendors) Support Plans.

- See "Scope of LiveHelp & Managed Subscription Services" (on page 13 of the FULL VERSION of the Customer Support User’s Guide) for specific details on what is and is not covered under these Plans, and a **Software Update License with Software Vendor Support** (SUL) is suggested.

Renewal, Payment Schedules, Cancellation

Renewal payment is due 30 days prior to warranty expiration or renewal date. Plans are renewed each period at the prevailing rate automatically after your full payment is received. Sites are not under Plan coverage when payments are not received prior to renewal date. Managed Subscription Services expire immediately to unpaid sites, as subscription payments must be made in advance to 3rd Party software vendors, and most require reinstatement fees to renew unpaid subscriptions, and all are non-refundable. Unpaid sites are subject to COD status if a Billing Agreement is not in place and/or the unpaid site has past due amounts. Either of us may cancel a Plan with 30 days written notice, however all annual advanced fees are non-refundable.

Plan rates are Annual and quotations are based on a discounted, single Annual payment. If Semi-annual (or Quarterly) payments for a hardware-inclusive Plan (A, B, or C) are preferred, the Plan rate is 110% (or 120%) of the Annual rate. **LiveHelp** Plan (D) is based solely on single annual payments (as subscription payments to third-party software companies must be made annually in advance and non-refundable).

A 5% Discount can be considered for a single advance payment to a 2-Year hardware inclusive Plan (A, B, or C) period for Systems having all current (non-discontinued) components from the hardware or software manufacturers, providing those components are expected to be supported by those manufacturers during the specific 2-Year period. *Oracle Software is excluded from this discount.*

Parts Repair

Parts Repair options for sites that do not have a Hardware support plan (sites "without a Plan" or with **LiveHelp** Plan only), or for sites encountering an Accidental Damage occurrence while under an Onsite or Depot plan, include:

*"Exchange" means that we will install a working whole unit to replace your non-working whole unit, adding installation and travel labor. We will keep your non-working whole unit (it will not be returned). Because we are supplying an immediately-stocked used replacement, your cost is higher than "material repair", but less than buying a new replacement with no exchange. In addition, labor (time) on an exchange is usually only 1 trip (for uninstall and reinstall) for a lower labor cost. All parts exchanged are warranted for 90 days from installation date.

*"Material Repair" means we will pick up your non-working whole unit, to be sent into our repair center for an extended period of time (or to manufacturer's repair center, sometimes up to 8 weeks) to repair only the portion that is broken. A replacement unit is not left or reinstalled, as is the case of "Exchange". This option is available only if you can accept operating without the unit for an extended period of time (up to 8 weeks). If so, your account has purchased spare parts and accepts this form of repair. The cost is less than "Exchange" due to replacements not being installed. However, this does require higher labor (time) costs, because it requires a minimum of 2 trips (de-install/pickup and deliver/reinstall). Shipping (if necessary to manufacturer) is added to the "Material Repair" cost, and then labor (time) cost is added, which determines the total cost. Material Repairs are warranted for 90 days from reinstallation date.*
Definitions

Level 1/Front Line Support: Assistance provided by one of our LiveHelp persons. The analyst will document your support request, gather pertinent information, attempt first-call resolution and escalate your request, if necessary, to one of our Level 2 Support Analysts.

Level 2/Back Line Support: Assistance initially provided by one of our Application Support Specialists and escalating through to one of our Technical Support Managers.

Technician: A local technician who typically responds to your dispatched breakfix problems or configuration issues, and is available to provide service at your site.

Response Time (LiveHelp): The time that it takes our Support Center to contact you to provide initial contact on a case. Response times are only implemented when the issue is not resolved on the first call. The expected First Call Resolution rate is 65%.

Resolution Time: The time it takes to resolve an issue. Expected resolution time is different for each situation or issue and cannot be determined until the appropriate support professional has evaluated your problem.

Site Expert: Your employee that has been trained by us, and designated by you to handle basic programming and administration tasks as they relate to your product. This person acts as your primary contact for issues reported to our Support Center.

Managed Subscription Services: Subscriptions (and 3rd Party fee payments made by us on your behalf) for your annual usage, as well as to update, maintain and manage those software subscriptions. For software and/or subscription services originally purchased from us, annual usage and subscription updates may include:

- **LiveProtect** (AntiVirus, AntiSpyware, Intrusion Protection, Content Filtering and updates for the SonicWall firewall)
- **LiveAlert & Connect**: To proactively perform tasks necessary to execute Plans, Customers subscribing to LiveAlert&Connect authorize DCRS personnel to remotely access their supported system at will. Customers preferring not to authorize DCRS personnel this access must not only take responsibility to communicate this desire to DCRS, but also acknowledge that the alternative will cause significant delays in the execution of these Plans.
- LiveManager Connection option
- Disaster Recovery Protection option
- **LiveAntiVirus** (to Servers & PCs)
- LiveBackup option (offsite backup service for Oracle/Micros RES system)
- CreditHelp (Merchant Link Network Credit Support for Oracle/Micros, or Retail Software Credit Software)
- And more!

Software Update License with Software Vendor Support (SUL) is a suggested ADDITION to Support Plans: Separate License fees, paid to Oracle Micros and other POS Software vendors—not included in the standard Support Plan—are necessary to gain access to Software Vendor Updates, Fixes, Corrections, Maintenance Repairs, Security Enhancements, New Functionality, New Features, gain assistance with 3rd Party Operating System or Database issues, and gain assistance in maintaining PCI-Validation for an End User’s PCI-Compliance. Software Vendors not only provide access to updates, but also accept software problem escalations on an end-user’s behalf, providing a Software Update License is purchased in advance, making an SUL a suggested addition to any Support Plan.
LiveHelp

High quality LiveHelp is provided via a toll free 800 number, to help you make the best use of your investment in your hardware and software products. LiveHelp via telephone is handled using our own call tracking system, to provide maximum operating efficiency and the highest level of customer satisfaction.

Contacting the LiveHelp Center via Email can provide NEXT BUSINESS DAY Support, as email is NOT MONITORED after Business Hours. We respond to these email requests on the Next Business Day, by contacting you by phone. For Immediate service, always contact the LiveHelp Center by phone.

Who Can Call?

Anyone from your site may place a call to our LiveHelp Center to request support. However, it is recommended that a Site Expert be identified at each of your sites, and will act as a Primary Contact for that site. Primary Contacts are usually your more senior staff members that are knowledgeable about your software and/or hardware and how it is used in your specific environment.

If you need to change the name of a designated contact, please notify us immediately to ensure that we maintain accurate and complete contact information for your site(s). Our LiveHelp Center can be contacted to request an update to your site information. Please be prepared to provide the following details:

- Your Company/Site Name
- Your Former Contact Name
- Your New Contact Name
- Your Address
- Your Phone, Fax, and Email Information

Before You Call

Support is as easy as picking up the phone. However, there are a few things you should know before you call. These guidelines will help you make the most effective use of our LiveHelp Center — and help us resolve your problem in the fastest, most accurate way possible.

If something isn’t working the way you expected, we recommend that you explore the problem before you call our LiveHelp Center. Try the following suggestions — you may find you don’t need to call after all:

- Verify that the problem is related to the Software or Hardware that was purchased from us. Your problem may be with your Network, Power, Internet Service Provider, or 3rd Party product, in which case you will need to contact the appropriate 3rd Party vendor for support. If necessary, we will work with you and the 3rd Party vendor to track down the problem.

- Attempt to reproduce the problem to ensure that it isn’t just a simple error, misstep, or a procedural problem.

- Check the obvious things like cabling, power, internet, login information, etc. Often the solution lies in the process, or the procedure, and not the software.

- Review all relevant documentation — including any manuals and online help if available.

- If the problem is reproducible, check to see if any changes have recently taken place in your operating environment that might be responsible for the problem.
Call Number

Each support request coming into our LiveHelp Center is logged in our call tracking system and assigned a call number. This unique identifier enables you and our support analysts to track your call until the problem is resolved.

Call Priority

All calls created by our LiveHelp Center are assigned a priority level. Priority level guidelines and the corresponding response times specify how quickly our LiveHelp Center will respond to you if the request is not resolved on the first call, and the amount of time in which your call is expected to be resolved.

All service level standards and measurements are based on the priority assigned to each case.

The following guidelines used to determine the appropriate priority level for each issue received by our LiveHelp Center.

Our LiveHelp Center will be responsible for making the final decision regarding priority level based on the information collected from your users.

<table>
<thead>
<tr>
<th>Priority Level</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Major System Disruption</td>
<td>A major disruption in business-critical system operability or functionality, server crash or total system failure.</td>
</tr>
<tr>
<td>P2</td>
<td>Severe System Disruption</td>
<td>A severe disruption in business-critical functionality that does not impact the entire system such as:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Significant number of terminals unable to perform or post transactions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Loss of ability to perform payment functions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Total loss of reporting (local or centralized)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Loss of all remote printing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Failure to reset totals or complete EOD/SCD</td>
</tr>
<tr>
<td>P3</td>
<td>Single Function Failure</td>
<td>A minor disruption in operability or functionality that does not impact the entire system such as:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Timekeeping issues</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Isolated printing failure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Isolated workstation/terminal failure</td>
</tr>
<tr>
<td>P4</td>
<td>Minor/Procedural issue or question</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Programming or configuration related questions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Questions relating to functionality, operability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Formatting or cosmetic problems</td>
</tr>
<tr>
<td>P5</td>
<td>Customization/Programming</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Browsable remote support or significant programming or configuration assistance requiring scheduling of dedicated support resources.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Any non-covered or out-of-scope issue.</td>
</tr>
</tbody>
</table>
Response and Resolutions Times

While we attempt to resolve most support requests during our initial contact with you, some issues may require additional time to research or require the assistance of more senior level support analysts. In these cases, the amount of time we expect to respond and resolve your reported issue is dictated by the priority assigned to your call. The following guidelines are used to determine the maximum amount of time before work is to begin on a call, and the duration of time that a call is expected to remain open:

<table>
<thead>
<tr>
<th>Priority Level</th>
<th>Response Time Goal</th>
<th>Resolution Time Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Immediate/1st Available</td>
<td>2 hours</td>
</tr>
<tr>
<td>P2</td>
<td>2 hours</td>
<td>4 hours</td>
</tr>
<tr>
<td>P3</td>
<td>4 hours</td>
<td>24 hours</td>
</tr>
<tr>
<td>P4</td>
<td>24 hours</td>
<td>48 hours</td>
</tr>
<tr>
<td>P5</td>
<td>24 hours</td>
<td>10 days</td>
</tr>
</tbody>
</table>

From time to time it may become necessary to suspend or lower the response or resolution time goals on a specific case. Some situations that can result in suspension of resolution time tracking may include:

• Tasks requiring additional information from you, a servicing agent, or a third-party
• Situations that require remaining in a monitoring state for an extended period of time
• Escalation to Level 2 Support or Software Development for further research: Software Update License with Software Vendor Support (SUL) is required for escalation to, and corrections from, the Software vendor
• Programming or consultative issues requiring scheduling of resources not available in LiveHelp Center
• Support requests for items outside the scope of our LiveHelp Center
• Feature enhancement or development requests (SUL required*)
• Your appropriate customer resources cannot be allocated to assist us with the reported issue as required

Response and Resolution time adherence is measured using the above published goals. The expected resolution time shown above for each priority is what we perceive as the maximum time expected to find resolution to a specific case. We regularly resolve calls 95% (or better) of the time prior to the stated goals.

Escalation and Resolution

After a call is created, an attempt to resolve the issue on the front-line is made. It is expected that 85% of all issues will be resolved on the front-line. If the call cannot be resolved in a timely manner, it will then be escalated. The Level 2, or "Back-Line" group, is made up of product specific Application, Product, System, and Technical Support Specialists. Resolution times are based on the priority assigned to each call as outlined earlier in this document. During the course of "Back-Line" research toward resolution of an issue, it may be determined that the issue will be escalated to the Software Developer/Manufacturer. *Due to the complexity of issues that are normally worked on by the Software Developer/Manufacturer, resolution time guidelines are no longer in effect upon escalation. Additionally, a Software Update License with Software Vendor Support (SUL) is required for any escalation to, or resolution from, the Software vendor.

Call Closure Resolution

The following criteria will be used to determine when a support issue can and/or will be closed:

1) A solution is given and your employee acknowledges acceptance and satisfaction with the given solution.
2) A fix is implemented by our Support Analyst or Servicing Agent, and your employee has accepted the resolution.
3) We have failed to receive a response, after at least two attempts in two days, from your employee contact.
LiveHelp Center Information

Hours of Operation
Our LiveHelp Center is available 24 hours a day, 365 days a year.

Contacting the LiveHelp Center
Telephone 314-739-6666 x2, or 1-800-231-0166

Escalation of Service Level Adherence Issues
If at any time you feel that the level of support you are receiving does not meet the defined service level guidelines, you are encouraged to escalate your needs. This escalation process is expected to be used after a call has been created.

Escalation Process
If escalation is needed during normal business hours (M-F, 8am-5pm Central), the first step is to contact any Manager.

Support Manager: Dan Krise
Assistant Support Manager: Dan Lonaro
Director of Professional Services: Mathew Schultz
Sales Manager: Justin Wells
Controller: Guy Unverferth
President: Matt Krane

The number is: 314-739-6666 x2, or 1-800-231-0166

Contacting the LiveHelp Center via Email for NEXT BUSINESS DAY Support
The email address is Support@DCRS.com

This email address is NOT MONITORED after Business Hours.

We respond to these email requests on the Next Business Day, by contacting you by phone.

For immediate service, always contact the LiveHelp Center by phone.

Positive Feedback
If, at any time, you or your employees would like to express positive feedback about a support or service transaction, an email address is in place for this type of correspondence. Email messages sent to this address are shared with the entire department.

The email address is info@dcrs.com
Service Level Measurement

The following service level standards apply to our LiveHelp Center.

Average Speed of Answer
Average Speed of Answer is the average length of time a call to our LiveHelp Center waits before being answered by a support agent.

- At least 95% of all calls are expected to be answered within five (6) minutes. This includes the alert time for any calls made after hours.

Front Line Resolution Rate
The first contact resolution rate is the percentage of issues that are resolved upon your initial call to our LiveHelp Center.

- Expected First Call Resolution rate is 85% or better.

Call Resolution Rate
The Call Resolution Rate is the percentage of calls resolved within the Service Level Guidelines based on priority level assignments.

- Current Call Resolution Rate expectation is 95% or better.
Scope of LiveHelp & Managed Services

When is LiveHelp Available?
Our products are supported on a 24-hour, 365 days/year basis.

Who is Supported?
Our customers who have purchased any of our Support Plans, including our LiveHelp Plan, are entitled to support provided by our LiveHelp Center, within the hours of 8:00 A.M. to 12:00 Midnight (with our standard plan), 7 days a week, 365 days/year, at no charge, via phone or remote access. Support via email is provided on a Next Business Day basis.

What is Supported?
LiveHelp is defined below by addressing the following support areas:

- **Software Application Support** (for software purchased from us—with limitations without an SUL).
- **Software Update License with Software Vendor Support** (SUL) is a suggested ADDITION to Support Plans: Separate license fee paid to Oracle Micros and other POS Software vendors—not included in the standard Support Plan—necessary to gain access to Software Vendor Updates, Fixes, Corrections, Maintenance Repairs, Security Enhancements, New Functionality, New Features, gain assistance with 3rd Party Operating System or Database Issues, and gain assistance in maintaining PCI-Validation for an End User's PCI-Compliance. Software Vendors provide access to updates, and accept software problem escalations on an end-user's behalf, only with a Software Update License. Without an SUL, we are prevented access to the Software Vendor to obtain software corrections, or escalating any problems, on your behalf.
- **Interface Support**
- **3rd Party Application Support**
- **Hardware Dispatching and Support**
- **Credit Authorization Software Support at the POS operations level** (Please note: Subscription Service to the Merchant Link Network for Oracle/Micros POS is offered as a Managed Subscription Service, below)
- Managed Subscription Services (where applicable; may include Merchant Link Network Subscription Service for Oracle/Micros POS—but LiveHelp is required for sites with Merchant Link Network Support)

*LiveAlert&Connect (Remote Access)*

- DCRS maintains systems which allow remote access to the Customers' POS system (*Remote Access*). Provided that the Customer has subscribed to *LiveAlert&Connect* or a DCRS Support Plan, Customer will allow Remote Access to DCRS support personnel at will, to perform tasks necessary to execute the Support Plan. The Customer shall have the right, with three (3) days prior written notice to DCRS, to de-authorize and prohibit all DCRS employees from Remote Access. DCRS shall have the right to alter the means for Remote Access, including designating the means of access and user names/numbers and passwords.
- To proactively perform tasks necessary to execute Plans, Customers subscribing to *LiveAlert&Connect* authorize DCRS personnel to remotely access their supported system at will.
- Customers preferring not to authorize DCRS personnel this access must take responsibility to communicate this desire to DCRS, but acknowledge this alternative does cause some connection delays in the execution of these Plans.

*Limitation of Liability.* DCRS shall have no liability to the Customer resulting from or connected with the access to Customer's system via *LiveAlert&Connect*, as Customer has authorized DCRS in accordance with the purchase of this subscription and plan. Customer indemnifies and hold DCRS harmless from any loss, fee, cost, expense, damage, liability or claim (including, without limitation, reasonable attorneys' fees and costs) resulting from the access to Customer's POS System via *LiveAlert&Connect*, which has been authorized by Customer in accordance with this Agreement.
Software Application Support (for Software purchased from us) & Software Update License (SUL—a suggested ADDITION)

Covered

- Resolution or explanation of your application generated error messages
- Assistance with your problems that occur during normal system and desktop operations
- Guidance with your procedural and system capability questions
- Researching and reporting your software bugs to Research & Development (SUL required)
- Assistance reloading your applications from Full System Backup(s)
- Assistance reloading your Database(s) from backup
- Assistance with installation of application release supplements or patch releases (SUL required)
- Assistance with identification of programming changes that may need to be performed by you, to correct your reporting or functionality issues
- Reprinting of your current day’s reports and journals
- Upgrades are required to maintain covered support (SUL required)
- Software Update License with Software Vendor Support (SUL) is a suggested ADDITION to Support Plans: Separate license fee paid to Oracle Micros and other POS Software vendors—not included in the standard Support Plan—necessary to gain access to Software Vendor Updates, Fixes, Corrections, Maintenance Repairs, Security Enhancements, New Functionality, New Features, gain assistance with 3rd Party Operating System or Database issues, and gain assistance in maintaining PCI-Validation for an End User’s PCI-Compliance. Without an SUL, we are prevented access to the Software Vendor to obtain software corrections, or to escalate any problems, on your behalf.
- Plan includes discounts to installation fees that may be applicable to SUL. Media costs, added software fees associated with different Operating Systems, and onsite installation services, are not covered.

Not Covered [Billable]

- Remote Programming changes to your database, to meet requirements not specified in installation survey
- Remote resolution of problems resulting from changes to the database performed by you or your agent
- Accounting for, or balancing of, the product’s Standard or Custom reports, or the identification of areas where a reporting imbalance may exist within a report
- Training performed onsite or over the phone, or installation of new modules
- Software Update License (SUL) releases require SUL addition
- Upgrade to a different Operating System
- Reloading your applications from scratch when a full system backup is not available
- Programming new POS devices such as Workstations, printers, etc.
- Programming new revenue centers, touch screens, keyboards, and menus, or Programming new reports and auto sequences. Reprinting reports and journals from active
- Issues corrected in later software releases, patch releases, or release supplements that can be corrected by the installation of appropriate patch release or release supplement
- Rebuilding of database tables, totals files, re-posting of totals, or any manual manipulation of database files
- Re-posting of any sales totals, including credit card sales
- Software Manufacturers support current versions and typically past versions not exceeding two (2) previous Major Release Versions. Support for older software versions is at the sole discretion of the Software Manufacturer. Fixes are only provided to software having a Software Update License (SUL). Updates to current versions are typically required to maintain support.
- Onsite visits to LiveHelp Plan sites
- Services necessitated by computer viruses and/or security breaches

NOTE: Reloading backups and installing new modules or patch releases should be performed by a system-trained property expert or the local servicing agent. Onsite visits are paid by you and must be scheduled in advance.
Operating System and Network Support

Our LiveHelp Center will provide support for Operating System and Network related issues within the following guidelines as they relate to products purchased from us:

Covered

- Explanation and resolution of your operating system generated error messages
- Assistance with your problems that occur during normal system and desktop operations
- Guidance with your procedural and system capability questions
- Root cause analysis of your Server crashes and problems during boot
- Resolution of your printer problems directly related to applications purchased from us
- Assistance reloading your system from a full system backup in the event of hard disk failure
- Re-routing your printers when there are printer problems
- Assistance with your backup issues or problems unrelated to hardware
- Resolution of network configuration problems directly related to hardware purchased from us

Not Covered [Billable]

- The cost of your operating system version upgrades, patch releases, or release supplements
- Assistance with loading operating system upgrades, patch releases or release supplements
- Assistance with configuration, installation, or addition of new hardware or peripherals
- Assistance loading and supporting third party applications not sold by us
- Resolution of problems directly related to non-supported third party applications
- Pre-installation network consultation or configuration including network design and evaluation
- Resolution of network problems caused by addition of or changes in network configuration or hardware by the user
- Post-installation network consultation including evaluation and/or reconfiguration
- Reinstallation of your Operating System from scratch when a full system backup is not available
- Restoration of any of your files or programs after a system crash, not available on the site’s full system backup
- Performing system administration tasks including but not limited to adding users, maintaining file system integrity, monitoring system resources, performing backups, and storing software
- Creation or installation of custom applications, batch files, shell scripts not part of our standard installation
- “Imaging” of the operating system onto any machine other than the machine where the image or backup was created
- Assistance with correcting issues on systems where an image, backup, or hard disk from another system was installed
- Software Update License (SUL) releases require SUL addition
- On-site visits to LiveHelp Plan sites
- Customer Supplied Servers of Virtual Machines
- Services necessitated by computer viruses and/or security breaches

NOTE: Reloading backups and installing new modules and operating system upgrades should be performed by a system-trained property expert or by the local servicing agent. A service agent’s onsite visit is paid by you and must be scheduled in advance. Exceptions are if you have an Onsite Support Plan Agreement, which covers the onsite visit to reload a system (from backup only), as well as hardware repair. DCRS is not responsible for any charges related to 3rd party hardware providers.
Interface Support
Our LiveHelp Center will provide support as outlined below for various interfaces used with our products, if purchased from us.

Covered

- Resolution of our product’s generated error messages. Software Update License with Software Vendor Support (SUL) addition required.
- Assistance with your problems that occur during operations as they relate to applications purchased from us
- Guidance with procedural and interface capability questions
- Resolution of interface problems/errors related to standard interface scripts and/or programs purchased from us. Software Update License with Software Vendor Support (SUL) addition required.
- General information concerning interface specifications for products purchased from us

Not Covered [Billable]

- Programming of database files and scripts required for back office applications or other interfaces
- Changes to the interface configuration as a result of an upgrade to another vendor’s software
- Programming of the PMS/Interface files and testing of the interface with the third-party vendor
- Programming of, or testing of, third-party interfaces to the application(s) or workstation application(s) purchased from us
- Creation or installation of interface scripts or files not part of the our standard installation
- Software Update License (SUL) releases require an SUL addition
- Onsite visits to LiveHelp Plan sites
- Services necessitated by computer viruses and/or security breaches

Third-Party Application Support
Third-Party Applications refer to those sold by us, for use with our products (i.e. Diskkeeper Defragmentation, Acronis Disaster Image, BarTender Barcode Label, etc.). Support is provided based on the following guidelines:

Covered

- Resolution of application generated error messages
- Assistance with your problems that occur during normal and standard operations
- Guidance with your procedural and documented capability questions
- Assistance with the installation or configuration of third party software according to our approved installation guidelines

Not Covered [Billable]

- Subscription updates for firewall, virus, and spyware protection, not purchased from us
- Cost, upload, distribution, and/or installation of product updates or patch releases for products no longer supported by us, including, but not limited to, pcAnywhere and Norton Anti-Virus, or without an SUL
- Assistance with applications not purchased from us
- Assistance with applications not covered under a support plan
- Activation of new features within the application
- Third-Party software fees associated with, or applicable to, an upgrade to a different Operating System
- Installation or configuration of third party software via remote dial in
- Onsite visits to LiveHelp Plan sites
- Services necessitated by computer viruses and/or security breaches
Hardware Dispatching and Support

Covered

- Dispatch of our local, authorized service organizations, for onsite support
- Assistance with swapping POS devices such as printers and Workstations with onsite spares
- Assistance with swapping Workstations with loaded and configured onsite spares
- Assistance with device diagnostics
- Assistance with basic trouble-shooting to possibly avoid an unnecessary onsite support call

Not Covered [Billable]

- Installing new POS devices such as printers and Workstations
- Installation/Configuration of new/used hardware, devices, peripherals or other hardware
- Installation of equipment that has been relocated from a location other than that where it was originally installed
- Onsite visits to LiveHelp Plan sites
- Service on Mobile products covered by DIRECT MANUFACTURER WARRANTIES for all 3rd Party products include: Micros Tablet-E Series (Cell), DT Research Tablet, Motorola Handheld, Epson Handheld Printer, Toest Handheld (Samsung), MobileBytes iPad (Apple) etc. (details on our website).
- Most Mag Card Readers (all "add-on" type) are considered a consumable, non-repairable item
- Manufacturer Warranty Claim Procedures must be followed when a problem appears in any of these 3rd Party products, as Service is unavailable for these products through DCRS.
- Customer Supplied Servers or Virtual Machines
- Services necessitated by computer viruses and/or security breaches

NOTE: Hardware support as defined above is related only to application support and dispatching for hardware service. What hardware services are covered, and not covered, is specifically stated in "SUPPORT PLAN CHOICES" (page 4). DCRS is not responsible for any charges related to 3rd party hardware providers.

Credit Authorization (CA) Application Software Support at the POS operations level

Covered

- Resolution of application generated error messages
- Assistance with your problems that occur during operations
- Guidance with your procedural CA capability questions
- Patch Release Upgrades as needed to resolve issues affecting system performance (SUL required).

Not Covered [Billable]

- Installation of new CA Driver Application
- Changing from one CA Driver to another, changing Merchant ID, adding Merchant ID to a new Revenue Center
- Activation of new features
- Changes to the driver configuration as a result of upgrade to another vendor's software
- Onsite visits to LiveHelp Plan sites
- Attempts to resolve your problems related to your Internet Service Provider (ISP)
- Resolution of your Oracle|Micros POS Credit authorization and batching problems (Coverage is included when subscribed to Oracle|Micros CreditHelp (which includes the Merchant Link Network Credit Support Subscription Service))
- Services necessitated by computer viruses and/or security breaches
- Support does not include annual rotation of encryption keys, Compliance with Credit or Debit Card Rules, Regulations and Laws. You, as End-User, are solely responsible for PCI-DSS Compliance.
Managed Subscription Services (when applicable)

Managed Subscription Services refers to the following third-party products and software subscription services approved, sold, and installed by us, for use with our products. They include, but are not limited to, annual usage and subscription updates to maintain LiveProtect (for a SonicWall firewall), LiveAlert&Connect, LiveManager Connection option, Disaster Recovery Protection option, LiveAntiVirus (to Servers & PCs), LiveBackup option (offsite backup service for Oracle/Micros – RES), Credit Help option (Merchant Link Network Credit Support for Oracle/Micros or Retail Software Credit Support), and more. Support for these products and services are provided based on the following guidelines:

Covered

- Annual subscription service fees for the Merchant Link Network Credit Support for Oracle/Micros, which includes resolution of your authorization and batching problems, and the re-keying of lost batches. LiveHelp is required for sites with Merchant Link Network Credit Support.
- Annual subscription service fees for LiveProtect, which includes automatic updates to the SonicWall firewall's AntiVirus, AntiSpyware, Intrusion Protection, Content Filtering, and firmware.
- Annual subscription fees for LiveAntiVirus to Servers and PCs, which includes AntiSpyware and automatic updates from SonicWall.
- Annual license usage and bandwidth access fees for LiveAlert&Connect, which includes automatic updates. To proactively perform tasks necessary to execute Plans, Customers subscribing to LiveAlert&Connect authorize DCRS personnel to remotely access their supported system at will. Customers preferring not to authorize DCRS personnel this access must not only take responsibility to communicate this desire to DCRS, but also acknowledge that the alternative will cause significant delays in the execution of these Plans.
- Annual license usage and bandwidth access fees for LiveManager Connection option, which includes automatic updates.
- Annual subscription service fees for Disaster Recovery Protection option.
- Annual subscription service fees for LiveBackup option (offsite backup service for Oracle/Micros – RES).
- Other Managed Subscription Services as added in the future.
- Installation or configuration of the above listed products, via remote dial in access.
- Resolution of application generated error messages.
- Assistance with your problems that occur during normal and standard operations.
- Guidance with your procedural and documented capability questions.
- Activation of new features within the above listed products, via remote dial in access.

Not Covered [Billable]

- Software Update License (SUL) releases optional.
- Subscription updates for any product not purchased from us.
- Cost, distribution, and/or installation of product updates or patch releases for products not purchased from us, and for products no longer supported by us (including, but not limited to, pcAnywhere, Norton Anti-Virus, products running on non-supported Operating Systems like Windows XP, etc.)
- Assistance with any application not purchased from us.
- Assistance with any application not covered under a support plan.
- Third-Party software fees associated with, or applicable to, an upgrade to a different Operating System.
- Onsite visits to LiveHelp Plan sites.
- Resolution of your authorization, batching, and re-key issues if not subscribed to the Merchant Link Network for Oracle/Micros (resolution to these issues are between you and your Credit Processor).
- Services necessitated by computer viruses and/or security breaches.
Time & Material Charges (Non-Covered Sites or Billable Support)

Non-Covered Sites (without a Support Plan) can receive Time & Materials* (T&M) support by providing a valid credit card in advance of the work performed. Customer Support accepts Visa, Master Card or Discover. After verifying your credit card over the telephone, our LiveHelp Center provides the requested support. There is a minimum T&M charge for each support request. Priority assignments on T&M cases are made at the discretion of Customer Support. The scheduling of T&M work to be performed is dependent on availability of our support resources and our existing support workload. Covered Sites with Support Plans are given top priority.

*Time & Material support is NOT AVAILABLE from the Software Vendor for sites not having a Software Update License (SUL), including Updates, Fixes, Corrections, Maintenance Repairs, Security Enhancements, assistance with 3rd Party Operating System/Database issues, assistance maintaining PCI-Validation for an End User's PCI-Compliance.

Covered Sites (with a Support Plan) can receive Time & Materials billable support for requests not covered by their Plan by providing a valid credit card (Card brands noted above) in advance of the work performed. If a Covered Site has an existing credit relationship in good standing, Time & Materials billable support may be performed with a signed Billing Agreement, and charged to an open account. Please contact our Controller to complete a Billing Agreement.

Hourly Travel & Labor Rates effective January 1, 2017

The following are our rates Without Plan Coverage, or Outside of a Plan's Hours or Coverage:

- **LiveHelp WITH a Plan, but OUTSIDE of PLAN HOURS (12:00 Mid. to 7:59 am, any day):** LiveHelp Rate 1, $95.00 PER INCIDENT, up to 30 minutes assistance.

- **LiveHelp WITHOUT a Plan, anytime:** LiveHelp Rate 2, $185.00 PER INCIDENT, up to 80 minutes assistance (minimum incident fee does not apply to Plan users). PLEASE NOTE: Software Maintenance and correction is not available on an incident or time basis without a Plan.

- **Onsite, 8:00 am to 5:00 pm Monday to Friday:** Onsite Rate 1, $370.00 PER INCIDENT, up to 2 hours assistance including travel to site, plus Parts (minimum incident fee does not apply to Plan users).

- **Onsite, 5:01 pm to 7:59 am Monday to Friday, or anytime weekends or holidays:** Onsite Rate 2, $450.00 PER INCIDENT, up to 2 hours assistance including travel to site, plus Parts (minimum incident fee does not apply to Plan users).

- **Drop Off Depot Repair WITH a LiveHelp Plan, Monday to Friday:** Depot Rate 1, $95.00 per ½ Hour, or $185.00 per Hour, plus Parts. ½ hour rate available only to LiveHelp Plan users.

- **Drop Off Depot Repair WITHOUT a Plan, Monday to Friday:** Depot Rate 2, $185.00 per Hour, plus Parts.

Onsite rates begin with travel time to your site. All time periods are Central Time. Onsite and Depot Repair Plans exclude the following designated Holidays: New Year's Day (January 1st, unless it falls on a Saturday or Sunday), Memorial Day (last Monday in May), Independence Day (July 4th, unless it falls on a Saturday or Sunday), Labor Day (first Monday in September), Thanksgiving Day (fourth Thursday in November), Christmas Day (December 25th, unless it falls on a Saturday or Sunday). When January 1st or December 25th falls on a Saturday or Sunday), the corresponding Friday (or Monday) is designated as a Holiday.

The scheduling of Time & Materials work is dependent on our existing support plan customers workload and availability of our resources. CUSTOMERS WITH a SUPPORT PLAN ARE GIVEN TOP PRIORITY. Software Update License with Software Vendor Support (SUL) is a suggested OPTION to all Support Plans, and is available on a prepaid--fixed--annually fee basis. Any required onsite Installation is additional. Support for CREDIT AUTHORIZATION to sites using the Merchant Link Network for Oracle fusions (but without Coverage) can be provided on a TIME & MATERIALS basis with our Support Manager's approval and your completion of the agreement covering the special procedures and flat rates associated with this type of support.

2605 Metro Boulevard • St. Louis MO 63043  •  www.DCRS.com  •  314.739.6566 •  800.231.0166
Your Responsibilities

To take full advantage of our applications and services, we urge you to follow the guidelines below:

- You will designate a "Site Expert" responsible for maintaining your system, including such duties as: the initial contact for trouble-shooting your user issues, the point of contact for our LiveHelp Center, the maintenance of hardware and software libraries, and the knowledge regarding the installed applications and system configuration.
- You will perform regularly scheduled system and database backups and have those backups available.
- You will secure and maintain virus and spyware protection software, including firewalls, passwords, physical security, access control policies, etc. We can assist in the maintenance portion by providing the "Managed Subscription Services" portion outlined and included with all Plans, but you have responsibility for the security, password, access control policies, annual rotation of encryption keys, and all PCI-DSS compliance.
- You will be responsible for the security and protection of your system and data. We cannot assure you that, after the initial installation, your system or your data will remain secure and virus-free.
- You will be responsible for providing a working Internet connection and router (or some remote connection method), and a dedicated analog phone line and serial modem (if backup credit option is available).
- Unless you have purchased LiveAlert&Connect and remain on our LiveHelp plan, you are responsible for any software required to remotely support your site and your site’s administration.
- To proactively perform tasks necessary to effectively execute these Plans, Customers subscribing to LiveAlert&Connect authorize DCRS personnel to remotely access their supported system at will. Customers preferring not to authorize DCRS personnel this access must take responsibility to communicate this desire to DCRS, and acknowledge the alternative may cause delays in the execution of these Plans.
- Unless you have subscribed to the Merchant Link Network Credit Support for Oracle/Micros POS, resolution to your credit authorization, batching, and re-key issues are between you and your Credit Processor (or Acquirer).
- You will use our approved, secure and supported connection methods.
- You will maintain access to all required software, including operating system installation media, our application software and patch release software, system specific driver files, as well as any applicable license or software key codes. We DO NOT cover the replacement cost of this software and cannot guarantee replacement availability.
- You will maintain appropriate disaster recovery software, backups, boot disks, etc.
- You will assist us with the resolution of your problems. You may need to dedicate some time to assist us in resolving your problems and questions.
- When asking for assistance from support, you be prepared to provide all information needed and answer questions as needed. Your accurate documentation of any error messages or system notices will help us expedite your resolution.
- You will plan and schedule ahead of time for services not covered under each support plan.
- We will not perform any items in the "not covered/billable" sections without being scheduled.
- Your Support Plan does not include a Software Update License with Software Vendor Support (SUL) unless listed on your invoice, which is a suggested ADDITION to any Software Support Plan.
- Your support does not include PCI Compliance with any Credit or Debit Card Rules, Regulations and Laws. You, as End-User Merchant, are responsible for all PCI-DSS Compliance.
- Your account is current, so we can render support.

PLEASE NOTE
This document is not intended to detail every item covered or not covered by our LiveHelp Plan, Credit Authorization Support Plan, or Managed Subscription Services. We make no guarantees, either expressed or implied, that your support request will result in the resolution of any problem or difficulty.
PCI DSS 3.2 CERTIFICATE OF VALIDATION – July 27, 2017

Dara Security is pleased to provide this Certificate of Validation regarding the PCI Assessment and Accreditation for Toast, Inc., a Level 1 Service Provider located at 401 Park Drive Suite 601 Boston, MA 02215. Based upon the validation effort, Dara Security has determined that Toast is COMPLIANT with the PCI DSS 3.2.

Documentation review, preliminary interviews, and technical & physical inspections were completed from May - July 2017. Dara Security, a certified QSA, conducted this audit pursuant to PCI DSS v3.2 requirements, standards and guidelines and in accordance with PCI DSS Security Audit Procedures v3.2 and generated the PCI DSS Report of Compliance on July 27, 2017.

Toast is a service provider offering an end-to-end hosted POS solution for merchants. The solution provides the merchant with hardware and a hosted software solution that interacts solely with the Toast payment gateway. Toast is a super-merchant with each of their clients classified as a sub-merchant.

The scope of the assessment included Toast' infrastructure, systems, and supporting network components involved in transmitting payment card data. The environment on which the assessment focused was on all networks and systems handling or supporting the Toast service. This included the Boston office and third party connections. Review areas included: Policy and Procedures; Data Flow Analysis; System Inventory and Documentation; Physical Environmental Security; Personnel and IT Staff Training and Awareness; Internal Vulnerability Assessment; Host/Network Diagnostic; Access Control; Data Storage; Wireless Network Analysis; Testing of Deployed Security Measures; and Monitoring/Response Assessment.

Dara Security reviewed results of Toast’ most recent quarterly scans, completed by a certified ASV vendor (Qualys) to confirm they covered all externally accessible (Internet-facing) IP addresses within the scope of the PCI DSS review and that the results of these scans were passing. Reviews of these security scans indicate that Toast is compliant with the PCI ASV Scan validation requirements.

All requirements in the Report on Compliance are marked “in place”, thereby Toast has demonstrated full compliance with the PCI Data Security Standard v3.2.

A summary of Toast’ overall compliance with PCI DSS v3.2 guidelines and requirements is provided in the table below:

<table>
<thead>
<tr>
<th>Payment Card Industry (PCI) Section Number and Title</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Install and maintain a firewall configuration to protect data</td>
<td>Yes</td>
</tr>
<tr>
<td>2. Do not use vendor-supplied defaults</td>
<td>Yes</td>
</tr>
<tr>
<td>3. Protect stored data</td>
<td>Yes</td>
</tr>
<tr>
<td>4. Encrypt transmission of CHD across public networks</td>
<td>Yes</td>
</tr>
<tr>
<td>5. Use and regularly update antivirus software</td>
<td>Yes</td>
</tr>
<tr>
<td>6. Develop and maintain secure systems and applications</td>
<td>Yes</td>
</tr>
<tr>
<td>7. Restrict access to data by business need-to-know</td>
<td>Yes</td>
</tr>
<tr>
<td>8. Assign a unique ID to each person with computer access</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>---</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>10.</td>
<td>Track and monitor all access to network resources and CHD</td>
</tr>
<tr>
<td>11.</td>
<td>Regularly test security systems and processes</td>
</tr>
<tr>
<td>12.</td>
<td>Maintain a security policy that addresses information security for employees and contractors</td>
</tr>
</tbody>
</table>

All data and information provided and all analyses completed have been carefully reviewed by Toast and Dara Security. All inputs and reports related to this PCI Assessment and Accreditation, to the best of our knowledge, accurately reflect Toast's current state of PCI compliance.

Barry Johnson, President
Dara Security
775.622.5386
barryj@darasecurity.com
Audit Clause for Contracts

Examination of Records

The Contractor's records must include, but not be limited to, accounting records (hard copy, as well as computer readable data), written policies and procedures, subcontractor files, indirect cost records, overhead allocation records, correspondence, instructions, drawings, receipts, vouchers, memoranda, and any other data relating to this contract shall be open to inspection and subject to audit and/or reproduction by the County Auditor, or a duly authorized representative from the County, at the County's expense. The contractor must preserve all such records for a period of three years, unless permission to destroy them is granted by the County, or for such longer period as may be required by law, after the final payment. Since the Contractor is not subject to the Missouri Sunshine Law (Chapter 610, RSMo), information regarding the Contractor's operations, obtained during audits, will be kept confidential.

The Contractor will require all subcontractors under this contract to comply with the provisions of this article by including the requirements listed above in written contracts with the subcontractors.

Vendor Information

Company Name: DCRS Solutions

Business Address: 2605 Metro Blvd
Maryland Heights, MO 63043

Business Hours: Office -- 8-5, M-F; Support -- 24/7/365

Phone: 314.739.6666 Fax: 314.739.8619

Email address: danny.mccarthy@dcrs.com

Contact Person: Danny McCarthy

Authorized Signature:  

Date: 10/15/19

(Indicates acceptance of all bid terms and conditions)
Customer References

1) St. Louis Symphony Orchestra
   Bob Olimpio
   bobolimpio@slso.org

2) Anheuser Busch
   James Meskill
   James.meskill@brewerscollective.com

3) St. Charles Convention Center
   Al Beltranena
   abeltranena@stcharlesconventioncenter.com
PCI DSS Solution Overview and Implementation Guide

Toast, Inc.

Date: January 18, 2017
Toast POS PCI Solution v1.1

PCI DSS Overview

Toast, Inc. (Toast) is a PCI DSS approved service provider offering the Toast POS solution. As a service provider, Toast has overall responsibility for the design and implementation of our solutions, and we manage the solutions for our customers.

The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information. Four major credit-card companies created the PCI DSS jointly in 2004: Visa, MasterCard, Discover and American Express. The PCI DSS specifies and elaborates on twelve (12) major requirements that address six major objectives:

1. A secure network must be maintained in which transactions can be conducted.
2. Cardholder Information must be protected whenever it is stored.
3. Systems should be protected against the activities of malicious hackers by using frequently updated antivirus software, anti-spyware programs, and other anti-malware solutions. All applications should be free of bugs and vulnerabilities that might open the door to exploits in which cardholder data could be stolen or altered.
4. Access to system information and operations should be restricted and controlled.
5. Networks must be constantly monitored and regularly tested to ensure that all security measures and processes are in place, are functioning properly, and are kept up-to-date.
6. A formal information security policy must be defined, maintained, and followed at all times and by all participating entities.

Toast has taken steps to address the PCI DSS requirements in regards to the Toast POS through our own validation efforts. Understand that utilizing our Toast solutions does not remove you from the scope of your own PCI DSS requirements. In addition, if you capture cardholder data in other manners beyond the offered solution, the systems and environment utilized by these secondary methods are fully within scope of PCI DSS and are solely your responsibility.

It is critical that you never store cardholder information in an insecure manner. Toast recommends that you store information as securely as possible and as little as possible. Under no circumstances should Track data, pin blocks, or CVV values EVER be stored.

It is the user's responsibility to comply with any PCI requirements. Please see https://www.pcisecuritystandards.org/ for more information. We recommend that you use a PCI qualified Assessor to be sure that your environment is compliant.
Table of Contents

PCI DSS Overview .......................... 2
Introduction ................................ 4
Installation and Connecting of Point-of-Interaction (POI) Devices .......................... 6
   Wireless Networks ......................... 7
   Remote Access ............................. 8
   Data Capture and Removal ................. 9
   Cryptographic Materials .................. 9
   Data Purging ................................ 10
   Required Services, Protocol, and Dependent Software .......................... 10
   Transmitting Cardholder Data ............... 10
Device Physical Security ...................... 12
   Receiving ................................ 12
   Storage .................................. 13
   Transit .................................. 14
Detection of Unauthorized Alterations or Replacement of Devices .................. 15
   Prior to Deployment ....................... 15
   Post Deployment ........................... 16
Appropriate Deployment Locations ............. 17
Third-Party Access Monitoring ................ 17
Securing Devices Removed From Service ........ 18
Troubleshooting ............................ 19
Contact and Support Information ................ 3
PCI DSS Requirements Addressed by Toast for the Toast POS

Build and Maintain a Secure Network and Systems
  Requirement 1: Install and maintain a firewall configuration to protect cardholder data
  Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Stored Cardholder Data
  Requirement 3: Protect stored cardholder data
  Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program
  Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs
  Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures
  Requirement 7: Restrict access to cardholder data by business need to know
  Requirement 8: Identify and authenticate access to system components
  Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks
  Requirement 10: Track and monitor all access to network resources and CHD
  Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy
  Requirement 12: Maintain a policy that addresses information security for all personnel

Introduction

The purpose of this manual is to provide you instruction to ensure your deployment of the Toast POS solution is performed in manner to enable you to achieve PCI DSS compliance as it relates to the Toast solution. In addition, this manual will provide you guidelines governing:
Toas t POS PCI Solution v1.1

- Inventory Control and Monitoring Procedures
- Installation and Connecting POI Devices
- Physical Security of Devices
- Detection of Unauthorized Alterations or Replacement of Devices
- Appropriate Deployment Locations for POI Devices
- Monitoring of Third-Party Personnel access to POI Devices
- Securing of Devices Removed from Service
- Disposal of Devices
- Guidance for Managing Device Failure
- Troubleshooting
- Detection of Tempering

Finally, an appendix is provided that details what PCI DSS requirements are directly addressed by Toast as it pertains to the Toast POS solution.

It is of utmost importance that you adhere to the guidelines detailed within this guide. Failure to do so will impact your PCI DSS compliance and may impact the security of the deployed solution implemented within your environment.
Installation and Connecting of Point-of-Interaction (POI) Devices

It is imperative that you follow the guidelines detailed below for the deployment of the Toast solution. Failure to do so may impact your PCI DSS compliance and the protections afforded to you.

Prior to deployment, you must understand that any modification to the deployment can and will impact your compliance. Such modifications may include:

- Attempting to enable any device interfaces or data-capture mechanisms that were disabled on the POI device
- Attempting to alter security configurations or authentication controls
- Physically opening the device
- Attempting to install applications onto the device

Based on your hardware selection, the Toast POS solution may consist of cash drawers, receipt printer, et al. However, at a minimum the solution will consist of at least one (1) Android OS tablet and one (1) card reader. Our tablets come from various manufacturers and are standard consumer based tablets or tablets designed for enterprise use. Our card readers come from respected manufacturers and apply industry standard security methods. Each of these card readers comes to you pre-injected with a key that enables encryption of cardholder data upon swipe. This encryption upon swipe provides you a higher level of security and can reduce the impact of PCI DSS to you. The specific type of readers you may receive are detailed in the table below:

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Device Model / Description</th>
<th>Device Model</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAGTEK</td>
<td>Dynamag</td>
<td>21073062</td>
<td>AES &amp; 3DES using DUKPT</td>
</tr>
<tr>
<td>MAGTEK</td>
<td>BuLeT</td>
<td>21073062</td>
<td>AES &amp; 3DES using DUKPT</td>
</tr>
<tr>
<td>MAGTEK</td>
<td>oDynamo</td>
<td>21076802</td>
<td>AES &amp; 3DES using DUKPT</td>
</tr>
<tr>
<td>Ello</td>
<td>Encryptable MSR Kit for Series AIO</td>
<td>E001002</td>
<td>AES &amp; 3DES using DUKPT</td>
</tr>
<tr>
<td>Ingenico</td>
<td>ICMP</td>
<td>ICMJ22-UST1ID</td>
<td>AES &amp; 3DES using DUKPT</td>
</tr>
</tbody>
</table>
Toast POS PCI Solution v1.1

For deployment, the devices are shipped directly to you. You will need to power on the tablets and connect them to your deployed wireless or ethernet network. The tablets provided will come pre-installed with the Toast solution. This software will communicate with our hosted solution to meet your needs.

For a payment card transaction, you will initiate payment through the Table POS solution. When prompted, you will swipe the patron’s payment card through the card reader attached to the tablet. The card reader will encrypt the patron’s card data with a pre-injected encryption key and transmit the captured data to Toast’s PCI DSS validated payment gateway for authorization and payment capture over an 128-Bit TLS 1.1+ (AES) connection. If you are required to manually enter the patron’s card data, the application will automatically encrypt the data with a pre-loaded RSA2048 public key. As with the swiped data, this data is transmitted to Toast’s PCI DSS validated payment gateway for authorization and payment capture over an 128-Bit TLS 1.1+ (AES) connection. Toast’s payment gateway will return the results of the transaction attempt to the tablet. A receipt will be generated and printed if you have a receipt printer deployed. All transaction activity is recorded within our cloud solution for you to review as needed.

Protected (Credit Card Number) and sensitive cardholder data (track1/track2 data) is securely wiped from all devices upon authorization. Furthermore, the components deployed in your locations have no access to the cryptographic keys needed to decrypt the captured cardholder data. This greatly reduces the impact of PCI DSS to you.

To ensure the Toast POS can communicate with the Toast payment gateway, you must enable outbound HTTPS (TCP/443) connectivity from the tablets to the Toast payment gateway through your Internet firewall. No inbound access is required for the solution to operate. Note: It is imperative that you do not allow unrestricted inbound access from outside networks to the Toast solution. Doing so will imperil your PCI DSS compliance.

Wireless Networks

If using Toast handhelds or using WiFi with Toast Terminals, a wireless network is required to operate the system. Therefore, for you own PCI DSS compliance and overall protection, you must ensure your wireless network is deployed in a manner consistent with PCI DSS requirements. The secure deployment of a wireless network is solely your responsibility. In order for you to achieve PCI DSS compliance, the following guidelines must be followed for deployment of a wireless network:

- Wireless encryption keys must be changed from default at installation, and must be changed anytime anyone with knowledge of the keys leaves.
Toast POS PCI Solution v1.1

the company or changes positions;
- default SNMP community strings on wireless devices must be changed;
- default passwords/passphrases on access points must be changed;
- firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks;
- other security-related wireless vendor defaults must be changed, if applicable; and
- wireless networks transmitting cardholder data or connected to the cardholder environment must use industry best practices to implement strong encryption for authentication and transmission.

If you have wireless network deployed within your environment and it is not part of your cardholder network, a firewall is required between any wireless networks and the cardholder data environment. The firewall must be configured to deny or control (only authorized business purposes) any traffic from the wireless environment into the cardholder data environment.

Remote Access

The solution does support remote access capabilities. You, as a merchant, may choose to utilize these remote access capabilities, but in order to maintain PCI DSS compliance only remote access technology supporting two-factor authentication may be used. Two-factor authentication consisting of something you have, know, or are is required for remote access in order for you to maintain your PCI DSS compliance. In addition to the use of two-factor authentication, it is important to remember that the remote access capability should only be enabled when needed, monitored while in use, and disabled when no longer required. Furthermore, your remote access software must provide for the following features or configuration settings:

- You must ensure changes are made to the default setting in the remote access software;
- Remotes access software must be configured to only allow access from specific IP addresses;
- Encrypted data transmissions such as IPSec VPN, SSH, 128-Bit TLS must be enforced;
- Access to customer passwords must be restricted to authorized personnel;
- Logging of remote access must be enabled;
- Systems must be configured so a remote user must establish a Virtual Private Network ("VPN") connection via a firewall before access is allowed;
- Unique user IDs must be used for each user account;
- Authentication composed of passwords and two-factor authentication must be used for non-console and remote access;
- Remote access must not require or use any group, shared, or generic accounts or passwords;
- Set unique passwords for first-time use/password reset and require immediate change upon login;
- Passwords must change every ninety (90) days or less;
Passwords must be a minimum of seven (7) characters;
- Passwords must contain both numeric and alphabetic characters;
- Password history of the last four (4) passwords must be kept and new passwords must be different than any of the last four (4) passwords;
- Account lockout must occur after six (6) invalid login attempts;
- Remote access accounts must be locked out for no less than thirty (30) minutes or until reset by a system administrator; and
- Remote access sessions must time out after no more than fifteen (15) minutes of inactivity.

Data Capture and Removal

The solution will capture the magnetic stripe (located on the back of the card, contained in the chip, or elsewhere) within volatile system memory of the provided devices. The solution does not store, and may not be configured to store, sensitive authentication data (magnetic stripe data [located on the back of a card, contained in a chip, or elsewhere]), card verification values or codes (the three-digit or four-digit card-validation code printed on the front of the card or the signature panel [CVV2, CVC2, CID, CAV2 data]), PIN, Encrypted PIN Block, or the Primary Account Number (PAN) after authorization.

The application automatically deletes the full contents of any track from the magnetic stripe (located on the back of the card, contained in the chip, or elsewhere), card verification values or codes (the three-digit or four-digit card-validation code printed on the front of the card or the signature panel [CVV2, CVC2, CID, CAV2 data]), PIN, Encrypted PIN Block and PAN upon authorization from volatile memory, per DOD 5220.22-M guidelines, in which storage areas are overwritten with a random bit pattern five (5) times.

Cryptographic Materials

There is no stored cardholder data (sensitive authentication data [magnetic stripe data [located on the back of a card, contained in a chip, or elsewhere]], card verification values or codes [the three-digit or four-digit card-validation code printed on the front of the card or the signature panel [CVV2, CVC2, CID, CAV2 data]], PIN, Encrypted PIN Block, or the Primary Account Number [PAN]) post-authorization by the solution.

For offline and manually entered transactions, the application will encrypt the captured data with a RSA2048 public key. This key cannot be used to decrypt any captured cardholder data. As you the merchant have no ability to decrypt the cardholder data, key management requirements do not apply. Toast handles all key management requirements for keys involved with the deployed solution. If you, as the merchant, decide to retain cardholder data in an electronic means outside of the application using third party methods, you must ensure that you meet PCI DSS requirements for the secure storage of this data and adhere to the cryptographic key management guidelines identified in the latest PCI DSS standard.
Data Purging

As previously stated, the solution does not store and may not be configured to store cardholder data (sensitive authentication data [magnetic stripe data [located on the back of a card, contained in a chip, or elsewhere]], card verification values or codes [the three-digit or four-digit card-validation code printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data)], PIN, Encrypted PIN Block, or the Primary Account Number (PAN)) after authorization within your environment. As such, there is no need for you, as the merchant, to purge cardholder data from the solution provided to you onsite. However, as you may decide to retain cardholder data outside of the solution using third-party means (Secondary payment method, Excel spreadsheet, written hardcopy, etc.), you must understand that any cardholder data collected by you that exceeds the defined retention period must be purged based upon business, legal, and regulatory requirements in order for you to achieve and maintain your own PCI DSS compliance requirements.

Required Services, Protocol, and Dependent Software

The solution does not require any additional software beyond that delivered to you as part of the overall solution.

The solution communicates over the TCP/IP protocol suite and does not rely on any other communication protocol for functionality. The application utilizes HTTPS (TCP port 443) to communicate with the Toast PCI DSS validated payment gateway over the internet for authorization and payment capture.

Note: Communication with the payment gateway only requires Internet outbound HTTPS (TCP port 443) access. No Internet inbound access of any type is required for functionality. It is recommended that you disallow all Internet inbound access to the environment supporting the solution. You are required by PCI DSS to disallow all Internet inbound access to the device supporting the solution. Failure to do so will jeopardize your PCI DSS compliance.

The aforementioned protocols and services are the only protocols and services enabled by default "out-of-the-box". No unnecessary or insecure services, daemons, protocols or components are enabled by default by the solution on supporting systems, nor are any required by the solution to function properly.

Transmitting Cardholder Data

The solution transmits cardholder data over the Internet using 128-bit TLS (AES) for encryption to the Toast payment gateway. This is done by default and cannot be disabled. This secure, encrypted transmission is required for you to maintain PCI DSS compliance. This is the only means of transmitting cardholder data supported by the solution; the application does not support and/or facilitate sending of PANs by end-user messaging technologies. Note:
Toast POS PCI Solution v1.1

Understand that the transfer of cardholder data across public networks must be encrypted in order for you to maintain your PCI DSS compliance.

Inventory Control and Monitoring

In order for you to maintain your compliance you must maintain an inventory of the provided Point-of-Interaction (POI) devices. You must track which devices are deployed, which are awaiting deployment, those that have been removed from service for repair or otherwise not in use, and those in transit for deployment or return for repair. It is recommended that you designate a Job Role or personnel responsible for maintaining the POI inventory and for inspection of devices.

For each area identified the following information must be recorded. It is recommended that you record this information upon receipt of your POI device and then update the location of each device as it transitions from storage, transit, deployment, and repair or return.

- Manufacturer of device;
- Make and Model of device;
- Serial Number of Device;
- Internal Inventory Number (if applicable);
- General Description of Device (Color, Secure Seals, Labels, Hidden Marking, etc.);
- Number and type of physical connections (Network, Serial, etc)
- Device Location (Storage, Where Deployed, In Transit, Availing Repair or Returned);
- Date of Location Inspection (Last Date device location was confirmed);
- Date of Last Inspection (last date device was inspected for tampering);
- Name of Job Role of personnel performing inspection; and
- Date inventory was last updated

Device inventories are to be performed no less than annually to confirm that inventory of devices is being catalogued and performed correctly; however, inventory must be updated as device transition in and out of service and from one location to another. This inventory must also be completed to confirm that all devices identified as being within your environment are currently within your possession and not missing.

Access to device inventory and to the devices themselves must be restricted to authorized personnel. The method for maintaining a device inventory is determined by you, however, the method utilized must enable you to restrict access to the inventory tracking information and allow you to record who has had access to the inventory tracking information. Failure to do so will impact your PCI
DSS compliance. In addition, you must be able to restrict access to stored devices and record who has accessed said devices and when access occurred.

During your inventory process, you must investigate the POI devices to identify unauthorized removal, tampering, or substitution of devices. Detection of these events may be an indication of a compromise of your environment. Inspection of device should compare information located on the device itself with the inventory information previously recorded. In addition, the inspection should look for indications that the device has been tampered with. Indications of tampering may include, but is not limited to, attachment of unauthorized devices to the POI device, breakage of security seals, cracks within the seal of the device itself, or insertion of a "skimmer" device within the Magnetic Stripe Reader (MSR) of the device. Skimmers are devices used by attackers to capture cardholder data prior to the POI device reading the card. Skimmers may be inserted in the MSR of the device or overlaid on the device itself. It is recommended that you train personnel interfacing with the POI devices on a regular basis to inspect deployed POI devices daily.

Should you detect a compromised device or find that your inventory indicated a missing or substituted device, you must report this information to Toast immediately. Contact information may be found in the Support section of this manual.

Device Physical Security

Maintain proper physical security of POI devices is required for you to maintain your own PCI DSS compliance and for you to ensure that devices have not been tampered with. Physical security of devices must be addressed in four key areas prior to receiving, during storage, and while in transit.

Receiving

Toast takes all necessary precautions to ensure devices are not tampered with or compromised prior to being shipped to you. However, there are steps that you must undertake to ensure that devices have not been tampered with during transit.

First you must confirm that shipment of devices originated from the following location:

411 Waverley Oaks Road, Ste 123
Toot POS PCI Solution v1.1

Waltham MA 02452
DCRS Solutions, 2805 Metro Boulevard, Maryland Heights, MO 63043

If using devices purchased from Toast, Inc., in order to remain compliant, you may only deploy POI devices that are shipped from one of the aforementioned locations. Confirmation that devices were shipped from an authorized source may be performed by comparing the shipping information with the information listed above.

If you cannot confirm the device was shipped from an authorized source, DO NOT deploy the device.

In addition to confirm shipping origination, you must confirm that neither the packaging nor the device has been tampered with. All POI devices will be shipped using tamper-evident packaging. This packaging will be evident on the shipping package itself and internally. Examples of said packaging include:

- Sealed Tamper Evident Bags: like Tamper Evident Deposit Bags
- Tamper Evident Tape used on all seams of the box

You must also inspect the device. You should look for broken security seals and cracks around device’s seals to determine if the POI device itself has been compromised. If you believe the packaging or the device has been tampered with, DO NOT deploy the device.

For device confirmation or reporting of tampering, please contact us immediately. If it is determined that a device or package has been tampered with, we will provide you an address for the return of the POI device so we may conduct a further investigation.

Storage

All devices being stored, be it prior to deployment, shipment, or while awaiting repairs, must be held in a secure area with restricted access to ensure they are not tampered with. Though the storage location of devices within your control is your responsibility, the location must include the following measures:

- Device must be stored in a locked room or container;
- Storage location must support restricted access;
- Must restrict access to authorized personnel.
Example includes:

- Door/container requiring key access in which defined personnel have access to the key or
- Door/container required knowledge of cipher lock code in which defined personnel have knowledge of the cipher lock code.
- Access to room or container storing device must be logged. This logging may be manual (written access log) or automatic (proximity card system that records access);
- Access to room must be monitored (cameras or physical sight).

Transit

When you are shipping devices to your location for deployment or for return, devices must be shipped securely. They must be packed in tamper-evident packaging and shipped in a secure manner. All devices either being shipped to a location for deployment or for return, must be shipped using a secure transport method such as a secure courier or bonded carrier (e.g., UPS, FedEx). For deployment to sites, it is permissible to use employees for transport; however, they must be authorized to deliver the devices, the recipient must be notified of who will be delivering the devices to them, and the serial numbers of the devices logged and communicated to the recipient. Be it a bonded carrier, secure courier, or internal employee, you must log the following information:

1) Personnel providing shipping (if employee, record name and job role);
2) Date of pickup
3) Device being shipped (to include serial number)
4) Confirmation Date of Site delivery

When packaging devices for transit, they must be packed in tamper-evident packaging. You determine the type of packaging; however, the recipient must be notified as to how to determine if the package has been tampered with during transit. As with your inspection of POI device received from us, your deployment sites must perform the same inspection on device shipped from your storage location. They must be notified of authorized shipping locations, notified of how the device will be shipped, and trained in how to inspect the packaging and device for tampering. For example, they must be trained to investigate for breakage of tamper-evident seals on the external packaging and to investigate the device itself for cracks or breakage of security seals. Finally, they must be instructed that if they receive devices without prior confirmation from the shipping location or they are delivered in a
Toast PCS PCI Solution v1.1

manner unexpected, they must confirm prior to deployment of the devices.

Special Note: If using internal employees for device shipment, they must be instructed to not leave devices in public areas unattended, for example, in the front or back seat of a car. This may lead to unauthorized access or theft of the device.

Detection of Unauthorized Alterations or Replacement of Devices

You must implement procedures for the detection of unauthorized alterations or replacement of devices prior to use and once deployed. This is imperative to maintaining the security of the solution and in enabling you to maintain your PCI DSS compliance.

Prior to Deployment

While awaiting deployment, the device must be deployed in a secure storage location with restricted access. Though the storage location of devices within your control is your responsibility, the location must include the following measures:

1) Device must be stored in locked room or container;
2) Device must remain in its original, tamper-evident packaging or in a physically secure storage until ready for use;
3) Storage location must support restricted access;
4) Must restrict access to authorized personnel. Example include:
   a. Door/Container requiring key access in which defined personnel have access to the key; or
   b. Door/Container required knowledge of cipherlock code in which defined personnel have knowledge of the cipherlock code.
5) Access to room or container storing device must be logged. This logging may be manual (written access log) or automatic (proximity card system that records access);
6) Access to room must be monitored (Cameras or physical sight).

Once the device is removed from storage and is being prepped for deployment, the following steps must be implemented:

1) The serial number on the device must be matched with the recorded serial number of the device removed from storage and shipped to the location. This information must be recorded within inventory tracking at the deployment location and at the shipping location at the time of deployment;
2) A pre-installation of the device must be performed to ensure the device has not been tampered with. This must include physical inspection of the device to search for breakage of seal and security tampering seals; and
3) Prior to final deployment into production, functionality must be tested to ensure that the device communicates and captures data properly.

Special Note: It is recommended that a list of device and serial numbers approved for a defined location be delivered to the location separate from the devices themselves. This will circumvent an individual from being able to substitute devices with differing serial numbers and updating the inventory list to reflect the compromised devices.

Post Deployment

Once devices have been deployed, periodic inspection must be made at deployment locations to ensure devices have not been tampered with or substituted. The type of location for deployment will drive the frequency for inspections. For high traffic, visible areas, it is recommended inspections occur twice a year. For locations that are remote or unattended, it is recommended that inspections occur every ninety (90) days.

When inspecting devices the first step should be to compare the serial number of the device with the serial number recorded for the location. If the serial numbers do not match, this could be the result of an unauthorized substitution. The individual should contact the personnel responsible for the storage, shipping, and installation of the POI device to confirm if the documentation is incorrect or if indeed a device has been substituted. Once the serial number has been confirmed, the device should undergo a physical inspection for tampering. Tamper and security seals should be examined to see if the seals are broken. The connection to the device should be inspected to ensure no extraneous devices are attached. The device should be inspected for missing screws, holes, or the addition of labels or covering that could be used to mask damage. Finally, the card DIP or magnetic stripe reader of the POI device should be investigated to ensure a “skimmer” or other type of device has not been inserted. If tampering is suspected, one should contact the personnel responsible for the storage, shipping, and installation of the POI device to report the tampering. The device should be taken offline. You should contact us (Toast) to report the tampering and we will provide remote assistance regarding the removal and return of the device for further investigation.
Appropriate Deployment Locations

When deploying a POI device, you must deploy them in the most secure manner possible. The following recommendations for deployment are provided:

1) Public access (non-employee) to devices must be limited such that they only have access to portion of the device needed to complete the transaction. For example, they should only have access to the card reader.
2) If the devices are stationary, they should be physically secure to prevent theft. For example, they should be bolted down.
3) Finally, they should be placed in an area easily viewable by employees and management. This will reduce the chances that a device is tampered with.

If the devices are deployed in a remote location or unattended, it is recommended that the devices be monitored with a camera so that one may review footage to determine if someone has attempted to tamper with the device. In addition, during off-hours, the device should be move to a secure location to reduce chance of theft and/or tampering.

Third-Party Access Monitoring

Access to POI devices by third-party personnel for repair/maintenance must be monitored. This monitoring is required to ensure there is no unauthorized access to device that could result in tampering, theft, or substitution of the device. To ensure proper third-party access monitoring, you should have a policy in place that requires the following steps:

1) Maintenance/repair of the device must be pre-arranged with date and time frame of third-party personnel defined. Unexpected visits for repair/maintenance must be verified. If they cannot be verified, access to the device must be denied;
2) Prior to granting access to a device, personnel must be identified and authorized to access the device;
3) Third-party personnel access must be recorded and include personnel name, company, time of access, and purpose of access. Log must be maintained for no less than one year;
4) Personnel must be escorted and observed at all times; and
5) Personnel may not remove or replace a device without prior authorization. If authorized, new devices must be properly inspected and inventoried.
Securing Devices Removed From Service

When devices are removed from service either for repair, being returned, being replaced, or being returned to storage, this must be done in a manner that allows for the tracking and security of the device. The following initial steps are required regardless of the reason a device is removed from service:

1) Removal of device must be pre-arranged prior to removal;
2) Location of device removal must confirm personnel removing device are authorised;
3) Personnel performing removal must be documented to include name, company, and line of removal; and
4) Inventory must be updated to indicate that the device was removed and reason for removal.

If the device is to remain at the deployment location for future deployment, the device must be securely stored at the location in a manner as described earlier within this manual.

If the device is to be returned to your shipping location, the device must be packed in a tamper-evident package and shipped using an authorized source that can be tracked. Methods for shipping and tracking are described in previous sections of this manual.

If the device is to be returned to us for repair or replacement, you must take the following steps:

1) Perform the steps provided to you via the support contact below or as indicated in the Toast support documentation accessed via the web to wipe the device of all sensitive data.
2) Pack the device within a tamper-evident packaging; and
3) Notify us that the device is being returned. You will need to provide us the serial number of the device and a tracking number of the package as provided by the carrier.

Disposal of Devices

Disposal of devices will be handled by Toast or our authorized parties. If you have device for disposal, please follow the instruction regarding the removal of device for repair and return the device to us.
Troubleshooting

In the event of an issue, we will work with you to troubleshoot the issue. Prior to any troubleshooting, we will confirm that the individual contacting us is an authorized individual within your organization for troubleshooting purposes as defined to us during the initial deployment of the solution.

During our troubleshooting process:

1) Primary Account Number or Sensitive Authentication Data will never be outputted to your systems;
2) We will only collect the Primary Account Number or Sensitive Authentication Data as need to resolve the issue;
3) Data collected will be encrypted upon storage;
4) Data will be stored in specific, known locations with access restricted to those individuals charged with resolving your issue;
5) We will only collect limited amounts of data needed to solve the issue; and
6) All data will be securely removed from storage immediately after use and the issue is resolved.

Contact and Support Information

Customers may contact Toast for support in troubleshooting the provided solution. Toast support consists of phone and, when needed, remote access support. Toast support may be contacted at:

Phone: 1-314-739-8566 DO NOT call Toast unless instructed by DCRS 1-617-882-0228

Email: support@dcrs.com DO NOT email Toast unless instructed by DCRS Support@toasttab.com

Note: Toast will not collect sensitive authentication data (magnetic stripe data, card validation codes or values, and PINs or PIN block data) or Primary Account Numbers (PAN) for any reason, even upon customer request. To do so may compromise Toast's own PCI DSS validation and, in return, your PCI DSS compliance.

If you, as a customer, decide to collect sensitive authentication data as part of your own troubleshooting process, you must adhere to the following guidelines or risk compromising your PCI DSS compliance:

- You must only perform the collection of sensitive authentication data when needed to solve a specific problem;
- You store such data in a specific, known location with limited access;
Toast POS PCI Solution v1.1

- You must perform collection of only the limited amount of data needed to solve a specific problem;
- You must provide for the encryption of sensitive authentication data as required upon storage; and
- You must perform secure deletion of such data immediately after use, using tools which utilize the DoD 5220.22-M military grade secure deletion process.

PCI DSS Requirements Addressed by Toast for the Toast POS

Toast addresses the following requirements for the Toast POS only. Full adherence to PCI DSS is solely your responsibility for all payment acceptance methods.

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 1 addresses the security of your network environment. The security of your network is solely your responsibility.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

<table>
<thead>
<tr>
<th>PCI DSS Requirement</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to all default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.</td>
<td>For the Toast provided devices, all vendor-supplied defaults have been removed or disabled.</td>
</tr>
</tbody>
</table>

2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited | For the wireless network connectivity, all vendor defaults have been changed |
<table>
<thead>
<tr>
<th>2.2 Develop configuration standards for all system components. Assume that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.</th>
<th>Toast has developed configuration standards for the devices to be deployed in your environment. These standards are based on SANS and NIST guidelines.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sources of industry-accepted system hardening standards may include, but are not limited to:</td>
<td></td>
</tr>
<tr>
<td>• Center for Internet Security (CIS)</td>
<td></td>
</tr>
<tr>
<td>• International Organization for Standardization (ISO)</td>
<td></td>
</tr>
<tr>
<td>• SysAdmin Audit Network Security (SANS) Institute</td>
<td></td>
</tr>
<tr>
<td>• National Institute of Standards Technology (NIST)</td>
<td></td>
</tr>
<tr>
<td>2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)</td>
<td>Toast has designed the solution so that each device performs a single purpose function.</td>
</tr>
<tr>
<td>Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.</td>
<td></td>
</tr>
<tr>
<td>2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.</td>
<td>The Toast solution only supports those services, protocols, daemons, etc. that are necessary for functioning system.</td>
</tr>
<tr>
<td>2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPM, or SSL/TLS for web-based management and other non-console administrative access.</td>
<td>Non-console access to devices is permissible through the use of SSH or over HTTPS.</td>
</tr>
</tbody>
</table>

**Protect Stored Cardholder Data**

**Requirement 3:** Protect stored cardholder data

The access solution does not retain cardholder data (protected or sensitive post-authorization) and all captured cardholder data is securely wiped upon authorization. Protection of cardholder data outside the Toast solution through secondary payment measures are your sole responsibility.

**Requirement 4:** Encrypt transmission of cardholder data across open, public networks
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSec, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following:</td>
<td>The Toast Solution encrypts cardholder data upon swipe and transmits the cardholder data to our payment gateway through an 128-bit TLS tunnel.</td>
</tr>
<tr>
<td>* Only trusted keys and certificates are accepted.</td>
<td></td>
</tr>
<tr>
<td>* The protocol in use only supports secure versions or configurations.</td>
<td></td>
</tr>
<tr>
<td>* The encryption strength is appropriate for the encryption methodology in use.</td>
<td></td>
</tr>
<tr>
<td>Examples of open, public networks include but are not limited to:</td>
<td></td>
</tr>
<tr>
<td>* The Internet</td>
<td></td>
</tr>
<tr>
<td>* Wireless technologies, including 802.11 and Bluetooth</td>
<td></td>
</tr>
<tr>
<td>* Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)</td>
<td></td>
</tr>
<tr>
<td>* General Packet Radio Service (GPRS)</td>
<td></td>
</tr>
<tr>
<td>* Satellite communications</td>
<td></td>
</tr>
<tr>
<td>4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11) to implement strong encryption for authentication and transmission.</td>
<td>The Toast Solution encrypts cardholder data upon swipe and transmits the cardholder data to our payment gateway through an 128-bit TLS tunnel.</td>
</tr>
</tbody>
</table>

Note: The use of WEP as a security control is prohibited.
Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

Toast has validated our adherence to PCI DSS requirement 5 through our own PCI DSS validation process performed by an independent, third-party QSA firm. Adherence to requirement 5 for your systems and applications outside of the Toast environment is solely your responsibility.

Requirement 8: Develop and maintain secure systems and applications.

Toast has validated our adherence to PCI DSS requirement 8 through our own PCI DSS validation process performed by an independent, third-party QSA firm. Adherence to requirement 8 for your systems and applications outside of the Toast environment is solely your responsibility.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

Toast has validated our adherence to PCI DSS requirement 7 through our own PCI DSS validation process performed by an independent, third-party QSA firm. Adherence to requirement 7 for your systems and applications outside of the Toast environment is solely your responsibility.

Requirement 8: Identify and authenticate access to system components

Toast has validated our adherence to PCI DSS requirement 8 through our own PCI DSS validation process performed by an independent, third-party QSA firm. Adherence to requirement 8 for your systems and applications outside of the Toast environment is solely your responsibility.

Requirement 9: Restrict physical access to cardholder data

Toast has validated our adherence to PCI DSS requirement 9 through our own PCI DSS validation process performed by an
Toast POS PCI Solution v1.1

Independent, third-party QSA firm. Adherence to requirement 9 for your systems and applications outside of the Toast environment is solely your responsibility.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and CHD

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1 Implement audit trails to link all access to system components to each individual user.</td>
<td>The Toast solution supports proper audit capabilities to link access to individual user.</td>
</tr>
<tr>
<td>10.2 Implement automated audit trails for all system components to reconstruct the following events:</td>
<td></td>
</tr>
<tr>
<td>10.2.1 All individual user accesses to cardholder data.</td>
<td>The Toast solution supports proper audit capabilities to link access to individual user in order to reconstruct required events.</td>
</tr>
<tr>
<td>10.2.2 All actions taken by any individual with root or administrative privileges.</td>
<td>The Toast solution supports proper audit capabilities to link access to individual user in order to reconstruct required events.</td>
</tr>
<tr>
<td>10.2.3 Access to all audit trails.</td>
<td>The Toast solution supports proper audit capabilities to link access to individual user in order to reconstruct required events.</td>
</tr>
<tr>
<td>10.2.4 Invalid logical access attempts.</td>
<td>The Toast solution supports proper audit capabilities to link access to individual user in order to reconstruct required events.</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>10.2.6 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.</td>
<td>The Toast solution supports proper audit capabilities to link access to individual user in order to reconstruct required events.</td>
</tr>
<tr>
<td>10.2.6 Initialization, stopping, or pausing of the audit logs.</td>
<td>The Toast solution supports proper audit capabilities to link access to individual user in order to reconstruct required events.</td>
</tr>
<tr>
<td>10.2.7 Creation and deletion of system-level objects.</td>
<td>The Toast solution supports proper audit capabilities to link access to individual user in order to reconstruct required events.</td>
</tr>
<tr>
<td>10.3 Record at least the following audit trail entries for all system components for each event:</td>
<td></td>
</tr>
<tr>
<td>10.3.1 User identification</td>
<td>The Toast solution supports proper audit capabilities to ensure proper details are captured for each event.</td>
</tr>
<tr>
<td>10.3.2 Type of event</td>
<td>The Toast solution supports proper audit capabilities to ensure proper details are captured for each event.</td>
</tr>
<tr>
<td>10.3.3 Date and time</td>
<td>The Toast solution supports proper audit capabilities to ensure proper details are captured for each event.</td>
</tr>
<tr>
<td>10.3.4 Success or failure indication</td>
<td>The Toast solution supports proper audit capabilities to ensure proper details are captured for each event.</td>
</tr>
<tr>
<td>10.3.5 Origination of event</td>
<td>The Toast solution supports proper audit capabilities to ensure proper details are captured for each event.</td>
</tr>
<tr>
<td>10.3.6 Identify or name of affected data, system component, or resource</td>
<td>The Toast solution supports proper audit capabilities to ensure proper details are captured for each event.</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>10.4</td>
<td>Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. Note: One example of time synchronization technology is Network Time Protocol (NTP).</td>
</tr>
<tr>
<td>10.5</td>
<td>Secure audit trails so they cannot be altered.</td>
</tr>
<tr>
<td>10.5.1</td>
<td>Limit viewing of audit trails to those with a job-related need. The Toast solution has been designed to limit access and viewing of audit trails to authorized individuals.</td>
</tr>
<tr>
<td>10.5.2</td>
<td>Protect audit trail files from unauthorized modifications. The Toast solution has been designed to protect audit trail files from unauthorized modifications.</td>
</tr>
<tr>
<td>10.5.3</td>
<td>Use file-integrity monitoring or change-detection software on logs to ensure that adding log data cannot be changed without generating alerts (although new data being added should not cause an alert). The Toast solution has been designed to detect unauthorized changes to log files.</td>
</tr>
</tbody>
</table>
Requirement 11: Regularly test security systems and processes

Toast has validated our adherence to PCI DSS requirement 11 through our own PCI DSS validation process performed by an independent, third-party QSA firm. Adherence to requirement 11 for your systems and applications outside of the Toast environment is solely your responsibility.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

Toast has validated our adherence to PCI DSS requirement 12 through our own PCI DSS validation process performed by an independent, third-party QSA firm. Adherence to requirement 12 for your environment outside of the Toast environment is solely your responsibility.
ATTACHMENT #5

DCRS solutions
RETAIL • HOSPITALITY • RESTAURANT

CUSTOMER INFORMATION

PERTINENT INFORMATION.................................................................2
INTRODUCTION TO PLANNING & PREPARATION AND SECURITY................2
NETWORK CABLEING...........................................................................3
INTERNET FIREWALL/ROUTER..............................................................3
DIAL MODEM CABLEING.................................................................3
SERIAL CABLES (FOR SERIAL HOTEL PROPERTY MANAGEMENT SYSTEMS).........4
HARDWARE PLACEMENT CONSIDERATIONS........................................4
MANAGED SUBSCRIPTIONS...............................................................4
ANTIVIRUS / ANTISPYWARE SUBSCRIPTIONS......................................5
SECURITY: VIRUSES AND THE INTERNET........................................5
PAYMENT CARD INDUSTRY PAYMENT APPLICATION DATA SECURITY STANDARD........5
PCI QIR IMPLEMENTATION STATEMENT, EFFECTIVE 3/31/16.....................6
FREIGHT / DELIVERY / DOCUMENTATION........................................6
TRAINING..........................................................................................6
SYSTEM IMPLEMENTATION SCHEDULE.............................................6
STANDARD WARRANTY........................................................................7
LIVE SUPPORT PLANS (see full details on web: “Customer Support User’s Guide”)......7
LOWEST PRICED SUPPLIES.............................................................8
SYSTEM CARE CONSIDERATIONS.......................................................8

If you are considering a POS vendor
that has not provided a Planning & Preparation document,
why would you invest in that vendor?

01.20.16

2005 METRO BOULEVARD • ST. LOUIS MO 63043  WWW.DCRS.COM  314.739.6565 • 800.231.0166
PERTINENT INFORMATION

The terms and conditions of the DCRS Sales Order and various Software License Agreements apply to proposals. The rights and responsibilities of both the Customer and DCRS are detailed in the DCRS Sales Order Agreement and Software License Agreements, as well as any Perpetual Software License and/or Cloud Service Agreements that are required by the Manufacturer.

Recommendations for hardware, software and services contained in proposals are estimates based on the data you have furnished us and our observations. While we believe our estimates to be sound, the degree of success with which hardware, software and services can be applied to data processing is dependent on numerous factors, many of which are not under our control. Therefore, our estimates as to the results to be obtained must not be regarded as expressed or implied warranties.

- Proposal pricing is valid for 30 days from their date
- Sales Orders for Systems are secured with a 30% deposit and authorized signatures
- Sales Orders for Upgrades are secured with a 50% deposit and authorized signatures
- Sales Orders cancelled, or not accepted for delivery within 12 months, are subject to a minimum restocking fee of 25% of the purchase price of the Hardware, and a cancellation fee of 100% of the non-returnable purchase price of Software and/or Cloud Service
- Blanket Sales Order Agreements may be subject to Manufacturer's price increase in the interim
- Sales tax is charged where applicable, unless an Exemption form has been received in advance
- Customers are responsible for payment of their State's Use tax, where applicable

If balance of contract is to be paid by a 3rd Party Leasing Company, an approved lease contract must be received prior to System order, and all documents must be completed prior to delivery. Delays in the installation of a new System, when caused solely by you or your agents once the System is ordered, may require a 2nd deposit equal to 30% of the purchase price on the date of the originally requested installation.

Installations are typically performed during the regular business hours of Monday to Friday, 8 am to 5 pm; Installations outside of those hours can be subject to additional charges. Additional labor time incurred due to customer changes after the Sales Order Agreement is accepted, or significant differences in your requirements from those originally disclosed, will be billed at our prevailing rate.

INTRODUCTION TO PLANNING & PREPARATION

To ensure the continued reliability of your system, planning and preparation should include proper Network Cabling, Electrical wiring, following the Implementation Schedule, 3rd party installation of certain items, Hardware Placement and Care, and most important—Security—including the PCI Data Security Standard.

Reliable operation is dependent on insuring your electrical power corresponds to the specifications outlined in our AC POWER REQUIREMENTS (see our website or your DCRS rep for this document). All outlets must have good isolated earth grounds, dedicated conduit, with no other equipment of any kind (other than computer hardware) connected to the same lines. Power fluctuations caused by electrical motors, heating and refrigeration equipment, etc., will cause loss of memory, improper operation and damage. Damage, resulting from failure to adhere to these requirements, is not covered under the Warranty or subsequent Support Plan.

NETWORK (and Cabling) is as important as AC power. Placement prepares for hazards to avoid, while Care prepares for maintaining your system. System Implementation Schedule covers steps you take prior to delivery, up to live. These (and the separate AC POWER REQUIREMENTS) should be reviewed in advance or immediately after your order is placed. Some hardware may require 3rd Party Installation due to specific tools needed or union labor requirements: display brackets hung from ceilings or walls, counter modification or cash drawer mounting, etc. We will consult with you and your contracted 3rd party resources, and to help ensure the work was performed properly, we will perform an on-site inspection of the Electrical, Network and Communication systems, once the work is completed at your local site. However, we cannot be responsible for malfunctions or damage to your system due to incorrect power or network installation of 3rd Parties. Power line and network systems installed by others are excluded from the Warranty coverage or Support Plan.
SECURITY is the MOST IMPORTANT aspect your System when used as a PAYMENT APPLICATION. For any System with connections to, or that processes credit or gift card transactions over the Internet, or otherwise has connections to any other network where there is potential for unauthorized access, you remain solely responsible for security.

*Please carefully note all references to the INTERNET, and review the headings entitled: ANTI-VIRUS / ANTI-SPYWARE; SECURITY; and PAYMENT CARD INDUSTRY (PCI) PAYMENT APPLICATION DATA SECURITY STANDARD (PA-DSS)—to properly prepare for these responsibilities.

- "Merchant Agreements" signed with Credit Processors (or Acquirers) spell out your specific responsibilities and liabilities, pertaining to Security. Please make Security your priority, as compliance with PCI PA-DSS is solely the responsibility of the Merchant.

NETWORK CABLING: 100 BaseT Networks
Networks dedicated to the POS System are recommended—REQUIRED when POS is used as with a Payment Application—as this insures maximum performance, minimum traffic disruption, and improved security. Failure to setup your network differently may result in periodic communication drops. PCI PA-DSS includes details for Network segmentation—to isolate the Payment Application system components that store, process or transmit cardholder data—from systems that do not.

Use CMP000424-FAX-B06 (EIA-TIA-568-A), 4 pair, 24 gauge, Shielded PLENUM Cable, available from DCRS or other suppliers (Category 5, speeds up to 100 mps).
- Each Workstation and Server must have its own separate cabling, from itself to the Network Switch.
- For MICROS 67 and RES (only), 2 separate cable runs are required for each Workstation (or each Remote Device) to the Network Switch.
  - The maximum total length of any Workstation-to-Switch "cable segment" is 300' (when using wall jacks), or 60' (when direct connecting with jumper cable).
  - The cable must never run near, in, or across power lines, fluorescent lights, or neon signs.
  - The distance between Network cable and AC wiring should be at least 2' (except at entry point).
  - When pulling cable for wall jacks, extend a minimum 18" of cable at each Workstation and Switch. The extended cable will be connected to 2 wall jacks installed at each end (Workstation-end and Switch-end). This will be supervised (and can be optionally performed) by our personnel.
  - Since the Network Switch is generally located next to the Server, the Server may not require a wall jack, but rather a jumper cable, to directly connect to the Switch.
  - If there is a long run from multiple Workstations to the Switch, we may suggest a Switch be installed nearer the multiple Workstations area instead of at the Server, and then run cable from the Switch back to the remote Server, to reduce cable runs. Please contact our Project Implementation Manager or Support Manager for questions.

INTERNET FIREWALL/ROUTER CABLING: DSL or CABLE
Our SonicWall Firewall/Router includes a cable to connect to your incoming DSL or Cable modem. Have DSL/Cable modems installed close to the Server and Firewall, as the Firewall cable is less than 6'. See below if you are adding a Dial Modem as a backup to Internet Payment. Never use a Payment Application Server for Email or Internet surfing! PCI COMPLIANCE requires the Internal POS network be isolated, with a separate firewall, from any other network (i.e. as a demilitarized zone or DMZ). Any USER-SUPPLIED FIREWALL must be INSTALLED & DEDICATED solely to the Payment Application System!

DIAL MODEM CABLING: Dial Modem for Backup to Payment Application
Some MICROS payment software products, and UnifyPOS (when using Mercury Payment Systems), can switch over to a dial backup modem if your Internet connection fails. If interested, you must install a modular RJ-11C phone jack and ANALOG Phone Line in advance to accommodate this. Install the jack in close proximity to the computer, as the modem cable is less than 6'. Our dial backup modem includes a Phone Splitter, to enable using just one single phone line.
SERIAL CABLING: POS to Serial Hotel Property Management Systems

Use BELDON #6540 cable and run in conduit. If cabling without conduit, use BELDON #88105 PLENUM cable, available from us, but apply all the same specs. The total length has been tested at 200'. Boosters are available when running beyond 200'. Never run near, in, or across power lines, fluorescent lights, or neon signs. The distance between Network cable and AC wiring should be at least 2' (except at entry point). 2x4 metal electrical junction boxes are recommended at both points. Extend enough wire at each location to reach each device comfortably. Installation of wall plates and connectors will be supervised (and can be optionally performed) by our personnel. Please contact our Project Implementation Manager or Support Manager if you have any questions.

HARDWARE PLACEMENT CONSIDERATIONS

This section describes the potential hazards of static, temperature extremes, and noise inducing equipment, when planning the location of your system components.

Location: Keep hardware away from heat lamps, glass racks, steam tables, water stations and never share electricity with microwave and noise inducing equipment such as blenders, standalone credit card devices, copy machines, etc. Locate all hardware so it is easily accessible to support personnel. To help in your planning, we can provide you with the dimensions of each module purchased. Before you determine the space each device occupies, take measurements and compare them to ours.

Electrostatic Discharge through Floor Coverings: Floor covering in the area around the hardware is important because tile and carpet have different static build-up characteristics. Severe electrostatic discharge (ESD) can be detrimental to the efficient functioning of the system, so the location of the hardware in relationship to floor surfaces should be carefully considered. Tile is the recommended surface for the area surrounding the modules. However, if the floor covering adjacent to the modules is carpeted, an "anti-static" grade is recommended. This type of carpet can generally be identified by strands of metal or plastic fibers intertwined with the carpet pile. If carpet is not "anti-static" grade, a grounded static mat is recommended.

Temperature: The operating temperature for PC computer devices is 50 to 95 degrees Fahrenheit, and most purpose-built POS devices is 32 to 113 degrees Fahrenheit. Keep this in mind particularly when placing any modules in areas such as kitchens or outdoors. When bringing electronic hardware in from the outdoor cold, you should allow the hardware to be within 15 degrees of room temperature before applying power to the unit.

Ventilation: To maintain a consistent internal temperature within a device, adequate ventilation is required. Consequently, the modules must not be put in an enclosure that would impede air flow to all four sides of the cabinet. A three sided (front and top open) enclosure with 4 inches of clearance on all sides is acceptable.

Noise Induction: With the use of either shielded or non-shielded cable, certain precautions must be observed. The distance between communication cable and AC wiring of any equipment should be at least 2 feet (except at the entry point to the hardware). Microwave ovens, cordless telephones, and radio transmission equipment generate noise which can be inducted into the hardware signal or power lines. Neither the hardware nor its cables should be placed within close proximity to such devices. Failure to observe these precautions may result in faulty operation of the hardware.

MANAGED SERVICES

Managed Services (and the payments made to 3rd Parties on your behalf) for your annual usage, which includes maintenance and updates to those software services, are included in all Live Support Plans. For software and/or services originally purchased from us, annual usage and subscription updates may include: LiveProtect (AntiVirus, AntiSpyware, Intrusion Protection, Content Filtering and updates for the SonicWall firewall), LiveAlert&Connect, LiveManager Connect, any Cloud Reporting or Cloud Gift & Loyalty program, LiveBackup (for RES), LiveAntiVirus (for Servers & PCs), Merchant Link Network Credit Support, Retail Software Credit Support, Software Update License (SUL), and more.
ANTIVIRUS / ANTIPLATFORM SUBSCRIPTIONS
AntiVirus / AntiSpyware software is proposed with your system unless otherwise requested. This Software is only productive when "Definitions" are continually updated (as new Viruses are discovered). When renewing your Support Plan, your AntiVirus/AntiSpyware subscriptions are renewed automatically. If you do not renew this subscription, updates become solely your responsibility. Any merchant processing payment application transactions should be aware of the PCI Payment Application Data Security Standard (PA-DSS) compliance responsibilities, which requires AntiVirus software and updates.

SECURITY: Viruses and the Internet
The security and protection of your system and data, including protections against unauthorized access, is paramount. For any system that has persistent connections to the Internet, or processes credit or gift card transactions over the Internet, or has persistent connections to any network where there is potential for unauthorized access, you are solely responsible for security. You must secure and maintain virus and spyware protection software, including but not limited to, firewalls, passwords, physical security, access control policies, and the like. It is imperative that as a user, you acknowledge that, to be effective, virus protection and other security software requires periodic updates, which you must obtain from your supplier or the manufacturer. We cannot assure you that your system or your data will remain virus-free. Services necessitated by computer viruses, or by a failure or breach of the security to your system or data (which may include damage caused by hackers, persons lacking authorized access, etc.) are not covered under the terms of either the Initial Warranty or any subsequent Support Plan. However, we can provide, on a time-and-materials basis at your request, services to assist you.

PAYMENT CARD INDUSTRY (PCI) PAYMENT APPLICATION DATA SECURITY STANDARD (PA-DSS)
Fraud and identity theft are serious threats to the credit card industry, merchants and consumers. Visa, MasterCard, Amex and Discover adopted the Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS). This standard includes requirements to protect cardholder data in your payment application processing software. FINES for NON-COMPLIANCE are NOT TRIVIAL and will have a serious financial impact on your business. Being "compliant" at time of installation does not ensure your compliance in the future, as this standard continues to change. Although your Acquiring Bank is required to bear all responsibility to inform you about this security standard, we have found this responsibility lacking, so we will continue to act as your additional resource. Becoming compliant with this standard not only includes using a currently "validated" version of software for your POS system, but also requires you meet and maintain many other compliance requirements. The PCI DSS consists of 12 major requirements, supported by more detailed sub requirements (over 200).

For more information, visit the following websites, for advance copies of any PCI PA-DSS documents:

- PCI website: https://www.pcisecuritystandards.org/

Or contact your DCRS Sales Representative.

Your education and implementation of these requirements is imperative, as we cannot be liable for any damages incurred in connection with you using a non-validated software product, non-compliant security products, or following non-compliant procedures. Although we did not mandate these requirements, we will continue to act as your resource on compliance issues, and our software manufacturers will continue to create software to meet future PCI PA-DSS requirements. DCRS also recommends Merchants take the time to review the terms of the "Merchant Agreement" they signed with their Credit Processor (or Acquirer), to understand their specific responsibilities and liabilities.

Effective 3/31/16, Payment Application installations must also include completion of the PCI-QIR implementation Statement by DCRS (a QIR-Certified Company), acceptance by you, and submission of these documents to the PCI Security Standard Council.
FREIGHT / DELIVERY / DOCUMENTATION
The system is provided FOB Origin. Distribution charges are paid by the customer. Documentation is in electronic format. If you require printed documentation or custom manual, it can be quoted separately.

TRAINING
Management or key employee training is provided prior to your system going "live". We prefer to train your management "how to train" your operators, so they understand the process when employee turnover occurs. An adequate amount of training is always included in any initial system proposal, but additional software installation, set up, and training is also available on a cost per hour basis. Travel expenses for installation or training apply to site installs over 75 miles from DCRS offices. Support Plans provide for training at discounted rates, for any of your future new staff members.

SYSTEM IMPLEMENTATION SCHEDULE
Implementation begins well before delivery of hardware. Many significant steps are taken before the actual delivery takes place. The activities for a successful system installation can be categorized as follows:

A. Select a Pivotal Employee to run the System (one of the most important decisions to make).
B. Review Documentation.
C. Data Gathering plus Completion of Worksheets.
D. Physical Installation of Hardware (unless Hospitality POS system, which is performed later).
E. Entry of Data into the Computer.
F. Training for Complete Program Operation.
G. Parallel Runs with Manual System (if applicable).
H. Final System Review.

The activities for each of the above are noted below. When fully operational, the system will provide concise and accurate reporting of business data. Reporting functionality and accuracy depend upon the accuracy and organization of the data files. Careful organization will prevent time consuming corrections later.

A. Select a Pivotal Employee to run your System.
An employee must be selected to maintain and manage the system, called your System Contact. This should be one employee. Ideally, your System Contact will not be an integral part of your store operational management. YOU cannot run your store and business AND a computer software system. Instead, base your selection on someone who can read, type, and operate an adding machine, with some computer knowledge. Ideally, your System Contact has a good working knowledge of your business policies and procedures, and strong ties to office, clerical, bookkeeping, and accounting skills.

The time your System Contact needs to dedicate to the system will be significant in the early stages, but, depending on the size of your business and the system that was purchased, the time should reduce after becoming familiar with the system. Logic states that your System Contact should play an administrative role in the business, dealing with other day to day office activities related to the software system purchased. Another employee (or part of management) should be designated as the secondary operator, becoming familiar with the system and tasks your System Contact performs. The system is a tool, and you should select someone (and a backup) who has the time and understanding to use it.

B. Review Documentation
Your System Contact and secondary operator should familiarize themselves with any documentation (usually electronic), by reviewing it completely. This will provide an overview of the software and information required, and gives them the ability to know what sections to refer, for greater details.

C. Data Gathering & Completion of Worksheets
Gather data and complete worksheets required for system's item files. This procedure and its importance cannot be emphasized too strongly. The only way to receive accurate data from a computer system is to provide it with accurate data. As data is gathered, it will be transmitted to file maintenance worksheets to begin building master files. The worksheets should be filled out as completely and accurately as possible to avoid time consuming corrections. These worksheets will be checked and reviewed by your Installer.
D. Physical Installation of Hardware
The training process begins by reviewing all the hardware components. Care and handling of hardware and other components of the system will be reviewed by your Installer.

E. Entry of Data into the Computer
Information gathered on the worksheets for all major files will be entered into the software. Your Installer will guide your System Contact through a few entries of each master file. Your System Contact will then complete data entry of all master files (primarily for Retail POS systems). File backup procedures will also be covered. Failure to backup data files religiously will cause loss of information resulting in time consuming re-entry of data. We perform the initial data entry for all Hospitality POS systems due to the file complexity, and the added fees are included; this step is typically performed in our offices before the physical installation of hardware.

F. Training for Complete Program Operation
When the master files are complete, your installer will return to continue training. Your System Contact has printed copies of all master files for your Installer’s review. The entire program is reviewed and your System Contact will learn how to operate all modules of the program.

G. Parallel Runs With Manual System (If applicable)
The same source information should be processed by your manual system and by the computer system for one time period (day, week, etc.). The end results will then be checked to make sure there is a perfect match or know reasons why the data is different. Your System Contact shall run the system at the proper time and your Installer will return to review and discuss the results.

H. Final System Review
Your Installer, at this point, goes over all the reports generated during the system run to explain what the computer is doing. If difficulty occurs, the System Contact is instructed to refer first to the Electronic Documentation for clarification, and if still unclear, to contact the Installer. The System Contact and other users cannot become proficient at this stage unless they learn to become less dependent on the Installer.

STANDARD WARRANTY
Unless otherwise stated in the DCRS Sales Order Agreement, for 90 days after delivery, parts are under warranty. During that time, labor cost is covered by the warranty, from 8 a.m. to 5 p.m. Central Time, Monday through Friday. Supplies are excluded. For our DEPOT (ship in) warranty, the customer is responsible for inbound shipping, if necessary. LiveHelp is also available from 8 a.m. to 5 p.m. Central Time, Monday through Friday. On-call technicians are available outside of these hours to provide LiveHelp. Unless otherwise planned, labor cost outside of these hours is charged at the prevailing rate. MICROS Systems can be serviced ONSITE or DEPOT by DCRS, or ONSITE by a Remote MICROS Service Agent. Software sold by DCRS is supported by DCRS LiveHelp. Modification to the hardware or software by the end-user, without the written permission of DCRS, voids all warranties. 3rd Party Hardware Warranties, covered solely by Manufacturer’s Hardware Warranties, will be assigned directly to you. Each Manufacturer’s Warranty Claim procedure must be followed when a defect appears in any of those items. These items typically include mobile hardware products like Tablets and Handheld Terminals & Printers. For full details on your coverage, see our current document entitled CUSTOMER SUPPORT USER’S GUIDE located at http://www.dcrs.com/services for Hardware repair and/or Software Support of the system purchased from us.

LIVE SUPPORT PLANS
We offer these for acceptance prior to your warranty expiration. A Plan can budget maintenance costs of the hardware and pass the risk of failure to us, as well as insure you get the finest LiveHelp and Managed Subscription Services available for your needs. See our website for our document entitled "CUSTOMER SUPPORT USER’S GUIDE" located at http://www.dcrs.com/services for full details.
LOWEST PRICED SUPPLIES
POS printers come with a starting paper roll (and ribbon, if applicable). Added supplies are available through our office during business hours Monday through Friday, delivered by UPS ground, special carrier, or your pick-up at our offices. With a Plan, you may be billed for supplies, others are shipped COD unless you have an approved credit application. Supplies include POS Printer Paper/Ribbons, Cash Drawer Tills/Lids and Keys, Magnetic Cards, Cleaning Cards for magnetic stripe readers, Batteries for UPS devices, Belt Zips (SkiZip) for magnetic cards, Barcode Labels and Tags, POS Touchscreen Overlays, etc.

SYSTEM CARE CONSIDERATIONS
In order to protect your system, the following guidelines have been established for proper care of the system. The leading causes of COMPUTER DATA LOSS, per the Computer Security Institute, are:
1. Human Errors 55%
2. Physical Security problems 20%
3. Employees who profit from attacks 10%
4. Disgruntled employees 9%
5. Computer viruses 4%
6. Outsider attacks 2%

Install hardware where there is minimal traffic. Put it on a sturdy table or desk and leave it there. NEVER move the system while the power is on. If you must re-position your system after installation, please call us to insure proper procedures and placement.

- Choose a location out of the direct sunlight, away from heating vents, radiators or open windows. Ideal conditions: temperature, 75; humidity, 50 percent.
- Ban eating and drinking to avoid crumbs or spills. If a spill should occur, call us at once.
- Vacuum the printer periodically. Wipe any touchscreen surface with a cotton cloth, after first spraying a mild cleaner on the cloth, not directly on the touchscreen. Never use any part of the system; bearings are sealed—oil will only attract dust and cause clogging. Unplug hardware before cleaning.
- Once you turn it on, let your computer run continuously for 24 hours over 7 days, BUT WE SUGGEST RE-BOOTING YOUR SYSTEM WEEKLY (shut it down, and then bring it back up). This improves the performance of the Windows Operating System.
- Be sure your power supply is adequate. Don’t share a power line with other equipment that could cause voltage variations. A ground power conditioner, to protect against surges, is available when necessary. Follow the specifications as we have supplied.
- If your system includes DVD’s, treat them gently. Do not store them near anything that may be magnetized, as this will cause data loss. Don’t subject them to temperature extremes, leaving them in an auto, for example. Avoid touching the surface.
- If a problem occurs, describe which part of the system is malfunctioning over the phone to our support center. Do not take anything apart yourself.
- Disaster Recovery Software is available for Servers with Dual hard drives. This protection solution can recover your entire system in minutes, versus many hours or days.
- LiveBackup (offsite backup service) is also available for MICROS RES for (uncompressed) unlimited storage of POS Critical files.
- Lastly, parts that generally require the most service will be (first) printers, (second) card readers, (third) hard disk drives, (fourth) keyboards, (fifth) monitors and touchscreens, and (sixth) the computer processor itself.
Attachment #6
DCRS PLANNING MEETING FORM

Preferred Attendance: Owner/GM (person making final decisions), Customer's delegated Site Rep for installation and on-going system management, DCRS Sales Manager, Installation & Support Specialist, and Project Manager.

PRE-INSTALLATION REVIEW: Check off each line

- Review the customer's expectation of the System purchased
- Review EVERY LINE ITEM of Sales Order and Riser Diagram, to ensure configuration accuracy or evaluate possible changes
- Review (if applicable) the Security requirements for a Dedicated Payment Application Server: Load NO OTHER SOFTWARE; Install in a secure location; isolated on a separate network; DO NOT USE for Email or Internet search (separate PC required).
- Review Extended Support Plan Offer on Sales Order: Accepted, or understand the date of expiration if not accepted
- Review the PCI QIR Implementation Statement for understanding that any Payment Application installation on or after 3/31/16 will require "QIR Reporting" by DCRS, acceptance by Customer, and this document must be submitted to the PCI Security Standards Council upon completion of the final installation.

Distribute & Review the importance of the PCI Implementation Guide, applicable to product(s) being installed

Review all items in Customer Information document:
- PCI Data Security Standard: Review Customer being solely responsible for security of using the Internet for any purposes, that responsibilities include preventing unauthorized access to, or damage as a result of unauthorized access, and about the many responsibilities that are part of the Merchant Agreement that was executed with their Credit Processor/Acquirer.
- Site Preparation: Include a review of the AC Power Requirements document
- Warranty: Length and coverage
- Training: Length and coverage
- Supplies: Review any items needed that are not part of the Sales Order
- Documentation: All electronic; most products have no hard copy manuals
- Hardware Placement & System Care Considerations: Heat, water, electrical devices that produce noise induction, etc.
- System Implementation Schedule: Select a pivotal Employee to manage the system. Review Tentative Schedule and discuss the site prep's deadlines (that must be met to fit the schedule), the responsibilities (who does what, by what date), and the rescheduling impact (should any delays occur with the scheduled dates). Show a current Project Schedule with Customer to help them understand the impact of delays on their part does create delays on our part.

Review Cable/DSL/Phone Lines for Routers/Modem, and IP address. A Serial Modem can be installed on a user-provided dedicated Analog Phone Line, available as an optional back-up to some of our Payment Applications.

Security for Internet, Antivirus, Wireless: Review the Customer being solely responsible for keeping the maintenance up-to-date for Virus Definitions (of Antivirus software) and Security Subscriptions (of SonicWALL device), and the security of Wireless connectivity, beginning immediately at time of installation.

Schedule dates for the following:
- Electrical inspection:
- Network Cabling pulled:
- Cable/DSL or Phone Line installation (for router or modem):
- Program, Database, Sales Tax Rate Information received:
- Program review:
- Final Inspection of Electrical, Cabling, and Cable/DSL/Phone Lines:
- Network cable connectors installed:
- Physical Delivery:
- Training:
- Live Support:
- Tax Rate, Database Programming, Auto Gratuities. Review the Customer being solely responsible for: Accuracy of all Tax Rate and Database Programming, including checking and testing in advance of use, both at install and in the future; Auto Gratuities are no longer considered "Tips" and are considered Income, subject to tax and withholdings, per IRS effective January 1, 2014.

DCRS HAS ADEQUATELY COVERED ALL THE ABOVE TOPICS

Date

Printed Name

Customer Signature

Site Contact Email Address

ORiGINAL (top) to DCRS    SECOND COPY to CUSTOMER

2605 METRO BOULEVARD • ST. LOUIS MO 63043  WWW.DCRS.COM  314.739.9666  •  800.231.0186
Attachment #7
DCRS FINAL INSTALLATION FORM

Business Name ____________________________

Address _________________________________ CITY __________________ ST _____ ZIP ____

Bus # ____________________________ Key Contact(s) ____________________________

Software Version __________________________

Reviewed at PLANNING MEETING: User’s expectation of System; Sales Order line items; Risers Diagram; Dedicated Payment Application Server (if applicable) has NO other software loaded, Installed in secure location, isolated Network, Not Used for Email or Internet Search; Extended Support Plan Offer (accepted, or understood if not); PCI QIR Implementation Statement (effective 3/31/18): Customer Information covering Site Prep, Warranty, Support Plans, Training, Supplies needed, Electronic Documentation (Not paper), HW Placement/ Care, Network Cabling, Cable/DSL/Phone Lines for Routers & Modems; Dedicated Analog Phone Line & Serial Modem can back-up some Payment Applications. Once Installed, User’s System Management Responsibilities include, but are not limited to: Future updates to Antivirus software and Sonicwall (or other firewall device); Security for Payment Systems & Wireless connectivity; Meeting Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS) and all Merchant Agreement responsibilities with Credit Processor; Accuracy of Database & Tax Programming; IRS Tax & Withholding responsibilities of Auto Gratuity Programming. See Customer Support User’s Guide for details.

FINAL INSTALLATION REVIEW: YES or N/A

_____All previously reviewed items (noted above) have been re-reviewed and are fully understood.

_____All Hardware listed on Delivery Form is installed and functioning correctly.

_____All Software listed on Delivery Form is installed, fully configured to our satisfaction, and functioning properly.

_____All Interfaces listed on Delivery Form are functioning correctly and personnel have been trained on those interfaces.

_____All non-DCRS HW & SW provided by the End-User is installed, functioning correctly, and is not covered by DCRS support.

_____Remote Support Access has been tested and is working.

_____Backup Hard Drive (if applicable) has been tested and is working.

_____All End-User Training, as scheduled for this installation, has been completed to our satisfaction, and included:
   Business Date ____________________________
   Perform Window Upgrade
   Paper/Ribbon change ____________________________
   Employee File maintenance
   Item/Price File maintenance ____________________________
   Tax File maintenance
   POS Data Backup ____________________________
   Power Loss recovery
   Redundancy/Backup Server Mode ____________________________
   Manual Setting of CC Batches
   Automatic Settlement of Credit Card Batches ____________________________
   Virus Definitions
   Reports & Report Balancing (Shift, End of Day) ____________________________
   Sales & Labor Totals Retention (# of days below)
   LiveMgr (email if app.) ____________________________
   Reports Detail, Labor Detail, Historical Totals

   Custom Report and/or Scripts explained:

Payment Application SECURITY REVIEW: YES, NO, or N/A

_____Properly-configured Firewall

_____Operating System Login Passwords changed from default

_____Anti-virus software installed and up-to-date, and plan in place to keep Anti-virus software updated

_____Each person has a unique user ID

_____Security Log is recording changes and is being properly archived

_____Wireless Access Points (if applicable) use complex passwords & changed from defaults

Credit Card # and Expiration Date masking

Vendor-supplied passwords changed from default

Complex password settings are in compliance with PCI PA-DSS requirements

Server in secure location with restricted access

User responsible for Encryption Key rotation

Credit Card DEMO MODE turned off (if applicable)

QIR Implementation Statement accepted (3/31/18)

SALES TAX HAS BEEN PROGRAMMED CORRECTLY AS NOTED ON DCRS TAX CONFIRMATION FORM.

CUSTOMER ACCEPTANCE AND CONFIRMATION OF INSTALLATION SATISFACTION

Exceptions or Notes: ____________________________

Date ____________________________ Printed Name ____________________________ Customer Signature ____________________________

Site Contact Email Address: ____________________________

ORIGINAL (top) to DCRS SECCND COPY to CUSTOMER FOLLOW-UP DATE by INSTALLER ____________________________

Sup927 01.20.18
What is a PCI-SSC Qualified Integrators and Resellers (PCI-QIR) Company?
Organizations qualified by PCI SSC to implement, configure and support PA-DSS validated Payment Applications on behalf of merchants are referred to as "Qualified Integrator and Reseller Companies" or "QIR Companies." The quality, reliability and consistency of a QIR Company's work provide confidence that the application has been implemented in a manner that supports the merchant's PCI DSS compliance. VISA has issued a mandate that all Payment Application Installs are performed only by QIR Certified Companies as of March 31, 2018.

What are A+ and Network+ Certifications?
A+ Certification is sponsored by Computing Technology Industry Association (CompTIA) to certify tech competency, and backed by major hardware & software vendors, including IBM, HP, Microsoft, and Association of Field Service Management. To become certified, you must pass tests covering configuring, installing, diagnosing, repairing, upgrading & maintaining computers. CompTIA has named DCRS "A+ Authorized Service Center" every year since 1998, for having our staff A+ Certified, a Customer Satisfaction Program in place, and multiple individuals with CompTIA's Network+ Certification (for computer network skills).

What is a Microsoft Certified Partner?
Microsoft's Certification program recognizes companies with a certified staff and competencies, as well as satisfied customers. DCRS has maintained MCP status since 2000. Certification requires testing of multiple employees to ensure competency, Microsoft contacting customers.

What is an Electronics Transaction Association Certified Payments Professional (ETA-CPP)?
The Electronic Transaction Association created the certification program to recognize industry professionals who demonstrate knowledge of payment processing. Merchants can be sure an ETA-CPP is knowledgeable about payment processing products and services.

Why are Certifications Important?
PCI-QIR, A+, Network+, Microsoft, SonicWall, ETA-CPP, MICROS and RSPA Solutions Provider Certifications mean that DCRS possesses the knowledge and customer relation skills essential for successful technical support, as defined by experts from companies across the industry. Certificated Technicians are more likely to meet your expectation and increase your satisfaction.

Wouldn't you prefer to do business with...
- MICRO Certified Service?
- PCI-Qualified Integrators & Resellers (PCI-QIR) Certified Company?
- A+ Authorized Service Center?
- Network+ Certified Staff?
- Microsoft Certified Partner?
- SonicWall Certified Security Administrator?
- Electronic Transaction Association Certified Payments Professional (ETA-CPP)
- Retail Solution Provider Association (RSPA) Certified Solutions Provider?

01.27.16