CUSTOMER INFORMATION

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

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 insure 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 insure 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 e7 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 <u>never run</u> 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 <u>separate</u> 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 <u>ANALOG Phone Line</u> 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 #9540 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 interwoven with the carpet pile. If carpet is not "anti-static" grade, a grounded static mat is recommended.

Temperature: The operating temperature for <u>PC computer devices is 50 to 95 degrees</u> Fahrenheit, and <u>most purpose-built POS devices is 32 to 113 degrees</u> 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 Connection,** 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 / ANTISPYWARE 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**. <u>**If you do not renew this subscription, updates become solely your responsibility**</u>. Any merchant processing payment application transactions should be aware of the PCI Payment Application Data Security Standard (PA-DSS) compliance responsibilities, <u>which requires AntiVirus software and updates</u>.

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. <u>**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.**</u> 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. <u>**FINES for NON-COMPLIANCY are NOT TRIVIAL and will have a serious financial impact on your business.**</u> Being "compliant" at time of installation does not insure 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 <u>you</u> meet and maintain many other compliancy 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/
    DCRS website: http://www.dcrs.com/services/pci-data-security-standard-emv/

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.

<u>**Effective 3/31/16, Payment Application installations must also include completion of the PCI-QIR Implementation Statement**</u> 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 <u>on the cloth,</u> not directly on the touchscreen**. Never oil 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.