

COMPUTER SYSTEM AGREEMENTS

Prepared by

Raymond R. Bonnabeau and Jen C. Salyers

Bonnabeau, Salyers, Stites & Doe, LLC

821 Marquette Ave S, Suite 1600

Minneapolis, MN 55402

Telephone: 612-341-3000

www.bssdlaw.com

	<u>Page</u>
I. INTRODUCTION	1
II. COMPUTER SYSTEM AGREEMENTS	1
III. PRE-CONTRACT CONSIDERATIONS	1-2
IV. IMPLEMENTATION PLAN	2-3
V. ACCEPTANCE	3-4
VI. SYSTEM WARRANTIES.....	5-7
VII. SYSTEM SUPPORT	7-8
VIII. PAYMENT TERMS.....	9
IX. SOURCE CODE.....	9-10
X. TERM AND TERMINATION	10
XI. LIMITATION OF LIABILITY	10
XII. INDEMNIFICATION.....	11
XIII. MODIFICATION	11
XIV. FORCE MAJEURE	11
XV. CONCLUSION.....	12

Computer System Agreements

I. INTRODUCTION

There are a number of issues and risks inherent in all Computer System Agreements. This material addresses many of these issues and risks and will provide both end users (“Users”) and vendors (“Vendors”) with an understanding of such issues and with insight into how to mitigate such risks.

II. COMPUTER SYSTEM AGREEMENTS

Computer System Agreements consist of the integration of hardware, software and third party components, and are often referred to as “turnkey agreements” because, after the Vendor installs the System, the User should only have to “turn the key” to use the System in its business environment. Consequently, Users may find Computer System Agreements attractive, as Users can acquire an integrated solution by entering into an agreement with just one Vendor, as opposed to acquiring products from Vendors under a number of separate agreements. In addition, Computer System Agreements provide Users with the perception that the bulk of the obligations and risks are placed on the Vendor.

Vendors often favor Computer System Agreements as the Vendor’s application may be best marketed as “the” solution, as opposed to only a part thereof. However, as Vendor’s often do not own all parts of a System, Vendors attempt to shift some of the risks and responsibilities to the User.

III. PRE-CONTRACT CONSIDERATIONS

The acquisition of a System is often a major addition to a User’s environment. Consequently, a certain amount of due diligence should be performed by both Vendors and Users.

a. Request for Proposal. As part of a User’s pre-contract due diligence, the User should strongly consider issuing a request for proposal (“RFP”) (or other similar document) to potential Vendors. The issuance of a RFP provides a User, for example, with:

- i.** A means of acquiring a Vendor’s written representations concerning System functionality as such relates to the User’s expectations;
- ii.** A means of acquiring a Vendor’s written representations as to whether the Vendor has integrated with the User’s existing disparate applications;
- iii.** An opportunity to ensure it has a good understanding of the overall costs involved in implementing and maintaining the System on an on-going basis;

iv. An opportunity to convey its expected license rights (e.g. who needs to use the System and from what locations) and to understand how the Vendor expects to license the System (e.g. concurrent users; named user); and

v. An opportunity to convey its expected agreement terms (e.g. acceptance testing; warranties) and to obtain the Vendor's responses to such agreement terms.

Most appropriately, when a User issues a RFP only those Vendors that respond to the RFP will be considered for the project. Consequently, a Vendor who desires to pursue a business deal with such a User should answer the RFP questions truthfully, but with caution. For example, a Vendor should consider qualifying that its responses are based on the Vendor's interpretation of the question being asked. In addition, a Vendor should consider including its standard Computer System Agreement in response to any specific User expected agreement terms.

In the event the User has a RFP containing the Vendor's representations, the User should either attach such document to the Agreement or, at a minimum, incorporate such document into the Agreement. Vendors should resist attaching and/or incorporating the RFP into the Agreement, as the RFP could contain "marketing" or other "puffing." In the event the RFP must be attached and/or incorporated, the Vendor should carefully review the RFP and should only attach and/or incorporate the RFP "functionality sections."

b. Additional Due Diligence. Beyond standard due diligence activities (e.g. ascertaining the Vendor's financial health), Users should also strongly consider conducting site visits or, at a minimum, conference calls with:

i. Existing Users of the Vendor System which are of similar size as the User; and

ii. Third party disparate application providers.

IV. IMPLEMENTATION PLAN

Prior to the installation and implementation of a System, the User and Vendor should complete an implementation plan setting forth respective responsibilities, milestones, and timeframes. In the best of all worlds, both the Vendor and User would complete the implementation plan prior to Agreement execution. However, often the specifics of such a plan can only be determined post-execution. Nonetheless, in the event there are known specific dates and/or other milestones for which the project must adhere to, Users should include such within the Agreement prior to execution. This will protect the User in the event the User and Vendor may later disagree as to such dates and/or milestones. Further, in the event the "scope" of the implementation is also known, it is important to also include such "scope" as part of the Agreement prior to execution. Such is particularly important (from the User's perspective) in the event the Vendor has quoted a "fixed fee" for performance of implementation tasks.

As the implementation plan will govern many of the tasks necessary for a successful implementation, Users should insist on incorporating the implementation plan into the Computer System Agreement. Vendors should initially resist incorporating the implementation plan, as most of the tasks are likely to be the Vendor's responsibility. In the event the User insists on incorporating the implementation plan, Vendors should, at a minimum, include language within the Computer System Agreement that the Vendor will not be liable for delays in the Vendor's performance if such delay is caused by events beyond the Vendor's reasonable control. Such language could be inserted within a force majeure provision (which, by its nature, is usually buried within the "General Provisions" section at the end of a Computer System Agreement). Lastly, both Users and Vendors should use care in drafting and reviewing an implementation plan. Please note, if the implementation plan is not incorporated into the Agreement, both the User and Vendor may not have any contractual recourse in the event the other party fails to perform its implementation responsibilities. See Pearson v. McGowan, 29 N.W. 176 (Minn. Sup. Ct. 1886) (prior oral agreement was superseded by subsequent written agreement although the written agreement omitted certain things that had before been agreed upon).

V. ACCEPTANCE

From a User's perspective, an acceptance provision is one of the most important provisions in Computer System Agreements. The need to develop sufficient and objective acceptance criteria will force the User and the Vendor to come to a clear understanding of what the System is supposed to do in the User's business environment. In addition, warranty provisions can be drafted to incorporate the acceptance criteria, thereby making them standards that the Vendor is committed to maintaining.

a. Acceptance Testing? The User should insist that it have a meaningful opportunity to test the "System" against adequate acceptance testing criteria. Such testing should, at a minimum, be conducted within a test environment and in a subsequent production environment. Although the foregoing may sound reasonable (especially to most, if not all, Users), Vendors should consider whether an acceptance testing provision could preclude the Vendor from "recognizing revenue", especially if the Vendor is a publicly held company.¹ In the event the User is unwilling to forego acceptance testing, the

¹ As a guideline, in order for a Vendor to recognize revenue each element of an arrangement must satisfy the following basic revenue recognition criteria:

- (a) persuasive evidence of an arrangement exists,
- (b) delivery has occurred,
- (c) the Vendor's software fee is fixed or determinable, and
- (d) collectability is probable. See SOP 97-2 ¶ 8

Generally, System price revenue associated with a System that is subject to acceptance testing cannot be "recognized" until acceptance occurs or the User's right to reject for non-acceptance has expired, whichever is earlier. However, System price revenue may be recognized upon "delivery" where (i) the acceptance period is thirty (30) days or less after delivery, and (ii) the Vendor is able to estimate the number of rejections resulting from non-acceptance among all Users of the System with an acceptance testing right.

Vendor should make it clear that the User would have contractual protection under the “performance warranty” provisions within the Computer System Agreement. Although some Users may find performance warranty coverage an acceptable protection, many Users will insist on including an acceptance testing provision. Should the Vendor find itself in such a position (and is willing to partially concede on this point), the Vendor should attempt to limit such acceptance testing to the Vendor’s System components; as opposed to the entire System. Should this not be acceptable, the Vendor could include the entire System as part of testing, but limit the testing criteria for the third party software and hardware to the descriptions contained within the third party licensor’s/manufacturer’s then published documentation.

b. Acceptance Testing Criteria/Conformance. If the User has developed acceptance testing criteria (or other performance requirements) covering the System, such criteria should be provided to the Vendor as soon as possible. Further, as discussed, Users should strongly consider submitting to Vendors a RFP and request that each Vendor submit a written response detailing the System’s capability to meet such performance criteria. Thereafter, the User should either attach or incorporate the Vendor’s response to the RFP into the Computer System Agreement. Just as Vendor’s should attempt to limit any acceptance testing provision to just the Vendor’s System components, the Vendor should also attempt to limit the acceptance testing criteria to the Vendor’s standard documentation (e.g., user manuals).

To what extent the System must conform to the acceptance testing criteria should also be addressed by both Users and Vendors. Users should initially insist on “strict” conformance. This is often problematic for Vendors, as Users could point to “de minimis” non-conformances to support non-acceptance. Conversely, Vendors should initially insist upon “substantial” conformance. However, Users should resist such, as the term “substantial” is quantitative and not qualitative in nature. A fair compromise would be that the System must conform “in all material respects” to the acceptance testing criteria.

c. Remedies. Vendors should attempt to limit a User’s remedies for failure of acceptance testing to a refund of the license fee(s)/purchase price for the Vendor’s non-conforming System components; as opposed to a refund of all sums paid. Users should resist such a limited remedy, as the other System components may likely have little to negative value to the User in the event the System fails to achieve acceptance. With that in mind, Users should strongly insist on receiving a full refund of all sums paid to Vendor.

VI. SYSTEM WARRANTIES

Vendors should attempt to cast Computer System Agreements in the form of a commercial transaction (e.g., the moment you drive it off the lot it is yours with all faults). However, Users should remember that it is acquiring a System with the expectation that it will be able to use the System for many years to come. Although no amount of warranty provisions will “guarantee” System performance, such provisions should be carefully drafted and reviewed to protect the User’s interests and future expectations. Conversely, Vendors should attempt to limit the length of any warranties within the Computer System Agreement.

a. The Warranties.

- i. **Ownership.** Vendor should warrant that it owns the System or, to the extent it does not own the System, it has all rights necessary to provide the System to User under the Computer System Agreement. Although such a warranty should not be problematic to Vendors, Vendors should be sure to limit the remedies for a breach of such warranty to those set forth in the intellectual property indemnification provision within the Computer System Agreement.
- ii. **Disabling Code.** Vendor should warrant that the System will not contain any disabling code. Provided the System does not contain any disabling code (and the Vendor has contractual assurances from the third party software and hardware providers that no disabling codes will exist in such third party components), such a warranty should not be a problem for Vendors.
- iii. **Scanning for Viruses.** Vendor should warrant that it has used its best efforts to scan for viruses within the System. A fall back position could be that the Vendor has scanned for viruses in accordance with standard industry practices. Vendors should not have a problem with warranting pre-delivery “scanning”; provided the Vendor is capable of scanning all System components prior to delivery.
- iv. **Date Compliance.** If applicable, the Vendor should warrant that the System is date compliant.² Vendors, however, should limit this warranty to its own System components and should strongly consider limiting nonconformance issues caused by non-Vendor components (e.g., third party software; third party hardware, etc.).

² Although the new millenium arrived worldwide over five years ago, Users should still insist on including a date compliance warranty provision within Computer System Agreements. Most (if not all) Vendors will assert that a User’s date compliance concerns should not exist as we are well past the year 2000. However, the passage of time will not, in and of itself, render a software application able to correctly and accurately calculate dates among and between different centuries.

v. Non-Infringement. Vendor should warrant that the System will not infringe on any patent, copyright, trade secret, trademark or any other third party proprietary rights. However, as a number of System components may be owned by third parties, Vendors should only warrant that the Vendor's System components will not be infringing. In addition, as a breach of such warranty could provide the User with additional remedies beyond those set forth in any intellectual property indemnification provision, Vendors should also limit the User's remedies for a breach of such warranty to those set forth in the intellectual property indemnification provision. Please note, in the event the Vendor will not extend indemnification coverage to non-Vendor System components, the User should make sure to include a good title warranty for the hardware and a right to license warranty for the third party software. Such warranty coverage would likely provide the User with at least some form of contractual recourse in the event of a third party claim relating to such components.

vi. State and Federal Laws. Vendor should warrant that the System will conform to all state and federal laws and regulations to enable the User to use the System as set forth in the Computer System Agreement. As a number of potential laws and regulations could apply (depending on the nature and use of the System) Vendors should resist this warranty. As a fall back, Vendors should insist on including the applicable laws to which the Vendor's System components must conform and, at most, warrant that such components comply with such laws and regulations as of the effective date of the Computer System Agreement.

vii. System Performance. Vendor should warrant that the System will conform to the descriptions, standards and performance criteria (including the acceptance testing criteria) contained in the Computer System Agreement. However, Vendors should consider only offering a performance warranty for the Vendor's System components. In addition, Vendors should also propose passing through to the User the third party software and hardware suppliers' warranties. In the event the Vendor is unable to do so under its third party agreements, the Vendor could make the same third party software and hardware warranties as the suppliers made to the Vendor.

viii. Response Time. If applicable, Vendor should warrant that the System will meet or exceed a "response time" warranty. In the event such a warranty is desirable, Users should take care in defining what needs to occur within the agreed-to response time. For example, "response time" could be defined as "the elapsed time between (a) the moment the terminal operator pushes a function key (or the equivalent action with a pointing device) on the workstation and (b) the moment at which all meaningful data has been displayed on the workstation and the

workstation is capable of initiating another transaction.” As a number of external factors may impact a System’s response time, Vendors should be sure to exclude such external factors from the response time calculation.

ix. Title. Vendor should warrant that it will convey good and clear title to the hardware being purchased under the Computer System Agreement, free and clear of all liens and encumbrances.

x. Compatibility Warranty. In the event the Vendor will not offer a “System” performance warranty, the User should insist that the Vendor warrant that the hardware provided under the Computer System Agreement is fully compatible with, and will operate successfully with, the software and third party software.

xi. Sizing and Volume Requirements. Vendors should warrant that the System has been sized appropriately to meet the User’s volume requirements. The User’s volume requirements can be set forth in an exhibit to the Agreement. From a Vendor’s perspective, Vendors should be sure to include language in the Agreement that the Vendor’s warranties, support services obligations, etc., do not cover non-conformances due to causes beyond the Vendor’s reasonable control (e.g., a User’s failure to provide an environment which conforms to the Vendor’s environmental specifications).

VII. SYSTEM SUPPORT

Users often give support provisions less consideration than necessary. However, support provisions may provide the User with its only leverage to obtain post-warranty fixes. Vendors usually are most willing to provide support, but whether such support obligations will be part of the Computer System Agreement will likely be a point of negotiation.

a. Part of the Computer System Agreement? Users should include the Vendor’s support obligations within the Computer System Agreement. This would assist in protecting the User’s investment in the event the Vendor fails to perform such services. Conversely, Vendors should seek to separate its support obligations (and the User’s remedies) from those otherwise contained in the Computer System Agreement. This may be done, for example, by executing a separate support agreement. In the event the Vendor’s support obligations are not part of the Computer System Agreement, the Vendor’s liability for failure to perform such services will (most likely) be greatly limited under the separate support agreement (e.g., limited to “repair or replacement” and/or “to support fees paid”). From a User’s perspective, this could prove seriously inadequate, as the User could be left with a non-functional System and inadequate remedies. To protect against such a result, the User should insist on including the Vendor’s support obligations within the Computer System Agreement. Failing that, the User should attempt to have all performance warranties continue as long as the User is receiving support from the

Vendor. Lastly, if the Vendor refuses to extend such warranties, Users should be sure to include language enabling the User to obtain the source code to allow for internal support.

b. Commencement. Although Users may want support, Users should attempt to obtain such support for no cost until expiration of the System warranty period (as the User should not have to pay the Vendor to correct warranty non-conformances). However, as support fees are a revenue stream for Vendors, Vendors should resist such attempts and insist on having support fees commence at a much earlier date (e.g., installation). In the event the Computer System Agreement contains an acceptance testing provision, the User could propose that support fees commence upon acceptance of the System. Should this be acceptable to the Vendor, Users should be sure to include language that the Vendor will correct all warranty non-conformances at no cost to the User.

c. Fees. From a User's perspective, support should not be paid on a time and materials basis (as such costs could escalate). Rather, support should be provided for a fixed annual amount. In addition, as a User may likely be dependent on the Vendor to provide support services, Users should also attempt to cap annual support fee increases. Although an annual cap increase may be acceptable, Vendors should consider the possibility of third party support fees increases (which could, conceivably, exceed the annual cap within the Computer System Agreement). With that in mind, Vendors could propose to cap increases in its support services fees and allow for any third party support fee increases to be passed onto the User.

d. Termination. Users should attempt to obtain the right to terminate support services without cause. In addition, as mentioned, as Users may likely be dependent on the Vendor to provide support services, Users should resist allowing the Vendor to terminate support services without cause. Although some Vendors may believe it will not in the near future sunset a product, Vendors should insist on having a without cause termination right as well. Should the Vendor fail to agree to forego such a right, the User should obtain a minimum support services term commitment from the Vendor.

e. Warranties. Vendor should warrant that all support services will be performed in a good and workmanlike manner consistent with acceptable industry practices and in accordance with the terms of the Computer System Agreement. In addition, the Vendor should warrant that it will provide all support necessary to continue the warranties under the Computer System Agreement at no additional cost to User. In the event the Vendor will not extend the performance warranty period as long as the User is receiving support services, these warranties will provide the User with the same amount of warranty protection.

VII. PAYMENT TERMS

Although the amount of the payments to be made under a Computer System Agreement are often considered in selecting a Vendor, the times at which such payments are to be made are frequently given less consideration than necessary.

a. Payment Dates. Users should tie payments to objective “progressive” milestones (e.g., 20% of the System price invoiced upon successful installation of the System; 30% of the System price invoiced upon successful completion of test environment testing, etc.). This will, amongst other things, provide the Vendor with an incentive to provide the User with an acceptable System. Conversely, Vendors should attempt to “front load” payments (e.g., 50% of the System price payable upon execution of the Computer System Agreement). In addition, Vendors should attempt to tie all remaining payments of the System price to a set number of days after execution of the Computer System Agreement (e.g., the remaining 50% is payable ninety (90) days after execution of the Computer System Agreement). Please note, Users should NEVER tie payment dates to a set number of days after execution of the Computer System Agreement or other “non-progressive” events; as a multitude of factors may affect the User’s implementation.

b. Withholding. Users should attempt to obtain the right to withhold payments based on a good faith dispute. In addition, Users should also obtain the right to prevent the Vendor from terminating the Computer System Agreement or stop performing its obligations in the event of such nonpayment. Although some Vendors may agree to forego the ability to terminate the Computer System Agreement, Vendors should insist that it should not have to continue to perform in the event of a dispute. Should this be acceptable to the User, the User should attempt to limit the Vendor’s ability to discontinue performance to the “task or task(s)” for which the Vendor is not being paid.

IX. SOURCE CODE

In the event the Vendor goes out of business or otherwise fails to support the System, Users may need access to source code in order to continue using the System. Therefore, Users should include a source code provision and broadly set forth the “release events” which would trigger the Vendor’s obligation to deliver the source code to the User. In addition, Users should also require the Vendor to escrow the source code with an impartial third party escrow agent. Such third party escrow will cover the User in the event the Vendor fails to respond to any User “source code” requests. In the event the Vendor is willing to include a source code provision or otherwise escrow the source code, Vendors should attempt to limit the source code “release events” to the Vendor going out of business.

In addition, some Users may not have the internal resources or expertise to utilize the source code. Consequently, Users should also secure the right for third parties to use, copy, modify, maintain, and enhance the source code, documents, and descriptions for

User's [and, if applicable, User's affiliates] internal use only. This should not be a problem for most Vendors, as long as such third parties agree, in writing, to keep the source code in confidence.

X. TERM AND TERMINATION

Users should make sure the Vendor may only terminate the Computer System Agreement upon a material breach by the User which remains uncured for a set number of days (e.g., 30 days) after receipt by the User of written notice of the breach. Conversely, Vendors should consider including an "automatic" termination provision in the event the User breaches certain critical provisions within the Computer System Agreement (e.g., breach of confidentiality as related to the System components). Please note, in the event the User terminates the Computer System Agreement, the User should also obtain the right to terminate any separate support agreement.

Users should also include specific "non-exclusive" remedy provisions within any termination remedy provision. For example, in the event User terminates the Computer System Agreement prior to acceptance, User should receive a refund of all sums paid to Vendor. Further, in the event User terminates the Computer System Agreement after acceptance, User should receive a pro rata refund of any support payments paid to Vendor based on the then-remaining term for which such fees apply; and a pro rata refund of all other sums paid to Vendor based on an agreed-upon useful life calculated from the date of User's acceptance. Vendors should resist a blanket refund provision within the termination section of a Computer System Agreement, as a number of non-System related "material" breaches could give rise to a refund. Users should note that in the event the Vendor will not agree to an express refund provision, the User could forego including such a provision, provided the User makes sure to include language that the remedies set forth in the Computer System Agreement are in addition to and not in lieu of any other legal and/or equitable remedies available to User.

XI. LIMITATION OF LIABILITY

Limitation of liability provisions should be reciprocal. For example, if the Vendor insists on excluding consequential, indirect, special, and incidental damages, such liability exclusion should apply mutually to both parties. However, from a User's perspective, the Vendor's indemnification obligation should always be excluded from any limitation of liability cap. This is fair as the Vendor is in the best position to know whether it's Software (for example) may be infringing and the User should not have to establish that its damages incurred by any such lawsuit were directly caused by the inability to use the Software. In addition to any negotiated "reciprocal" limitation of liability provision, a Vendor should also attempt to limit its liability for damages with respect to the third party software and hardware.

XII. INDEMNIFICATION

As the Vendor is providing the User with a “System”, Users should attempt to obtain “System” indemnification coverage. However, as a number of System components may be owned by third parties, Vendors should attempt to limit its indemnification obligations to the Vendor’s System components. In the event the Vendor will not extend indemnification coverage to non-Vendor System components, the User should make sure to include a good title warranty for the hardware and a right to license warranty for the third party software. Such warranty coverage will likely provide the User with at least some form of contractual recourse in the event of a third party claim relating to such components.

In addition, Vendors should attempt to limit its indemnification obligation to patents and copyrights. However, from a User’s perspective, such a limitation should be unacceptable; as software developers often seek to protect their software through “trade secret” protections. In addition, System components may also, for example, be protected by contract. Therefore, Users should strongly resist a Vendor’s attempt to limit such coverage.

Lastly, Vendors should attempt to “condition” its indemnification obligation upon the User promptly notifying the Vendor of such claims, the User providing reasonable assistance, etc.. Conversely, Users should resist a Vendor’s efforts to condition its obligations, as the Vendor could use such to avoid its indemnification obligations.

XIII. MODIFICATION

The Computer System Agreement between the parties should be as written and care should be given not to allow either party to orally modify the Agreement. Therefore, both the User and the Vendor should make sure to insert a provision stating that the Computer System Agreement may be amended or modified only in a writing signed by duly authorized officers of both User and Vendor.

XIV. FORCE MAJEURE

Users should be weary of force majeure provisions, as such can be used by a Vendor to have the User equally assume all of the Vendor’s risks of doing business (e.g., delay in delivery of the Vendor’s vendors; strikes, etc.). Therefore, from a User’s perspective, force majeure provisions should only contain events the occurrence of which is both equally unpredictable and unpreventable by both parties (i.e., acts of God). However, as the Vendor’s performance may be dependent on the performance of third parties (e.g., third party software and hardware providers), Vendors should attempt to include “events beyond the reasonable control of either party” as an additional force majeure event. In the event the Vendor insists on including an “events beyond the reasonable control of either party” provision, the User should consider limiting the period of non-performance to a set number of days (e.g., 60 days) for the party so affected to resume performance.

XV. CONCLUSION

Although the issues and risks addressed in this article are not intended to be exhaustive, such should provide guidance and information necessary to avoid a number of common “pitfalls” in Computer System Agreements.