IT Best Practices Sample Language for Contract and Solicitation Development

IT Hardware

Maintenance

1. Contractor shall contact the Authorized User within one (1) business hour following an initial trouble call.
2. Contractor shall supply, upon request, loaner equipment of equal or greater value and functionality during the time warranty repairs are being completed. The Authorized User shall incur no additional cost.
3. OEM replacement parts, or comparable components, shall be available for all models that are purchased from the Contract throughout the duration of the equipment's warranty or for a minimum of two (2) years after withdrawal of a Product, whichever is longer.
4. Contractor shall be responsible for coordinating all warranty issues with OEM and making sure the warranty and maintenance service is provided.

Acceptance Language

1. A good or service furnished under this Contract shall function in accordance with the specifications identified in this Contract and Solicitation. If the goods or services do not conform with the specifications identified in this Contract and Solicitation ("Defects"), the Purchasing Entity shall within thirty (30) calendar days of the delivery date ("Acceptance Period") notify Contractor in writing of the Defect. Contractor agrees that upon receiving such notice, it shall use reasonable efforts to correct the Defects within fifteen (15) calendar days ("Cure Period").
2. Once equipment is installed and successfully operational, the Purchasing Entity shall sign an acceptance certificate which shows acceptance of the Product(s) and allows Contractor to invoice for the Product(s). Purchasing Entity agrees to sign and return to Contractor the acceptance certificate (which, at mutual agreement, may be done electronically) within three (3) business days after any Product is installed.

Training

1. An initial, no charge, on-site, one-hour training session for each Device, must be offered by Awarded Vendor(s) for all non-desktop Products placed at each Purchasing Entity's location. For drop-shipped or desktop Products, Awarded

Vendors must offer an initial, one-hour, no charge, web-based, or on-line training session.

2. If Purchasing Entity elects to exercise the training option, then Awarded Vendor shall provide the training within ten (10) Business Days of Purchasing Entity's request.
3. Awarded Vendor(s) may offer additional on-site, one-hour training sessions for a flat rate fee. Additional charges for travel and per diem, if applicable, must be disclosed to the Purchasing Entity prior to Order placement.
4. Awarded Vendor(s) shall provide Product literature, user-manuals, and access to on-line resources, if available, at no charge to the Purchasing Entity.

Hard Drive Removal

1. Hard Drive: With respect to any Contractor manufactured Products which contain a hard drive, the options for hard drive security are as set forth in Section 4.6.5 of the Master Agreement. If desired, Purchasing Entity may engage Contractor to perform the following hard drive services, and the PO shall detail the service:
2. Hard Drive Surrender Service. Under this option, a Contractor service technician can remove the hard drive from the applicable Product (set forth on a PO) and provide Purchasing Entity with custody of the hard drive before the Product is removed from the Purchasing Entity's location, moved to another department or any other disposition of the Product. The cost for the Hard Drive Surrender Services is $200 per device.
3. The Purchasing Entity and Contractor shall agree prior to hard drive handling what the Purchasing Entity needs are.
4. Awarded Vendor(s) will not be permitted to download, transfer, or access print data stored on the Device in either hard drive or chip memory. Only system management accessibility will be allowed.

Software

Data Ownership

1. The State of Wisconsin shall own the rights to all data/records produced as part of the Contract.

   If the Proposer anticipates bringing pre-existing intellectual property into the project, the intellectual property shall be identified in its Proposal. If the Proposer identifies such intellectual property ("Background IP") in its Proposal, then the Background IP owned by the Proposer on the date of the Contract, as well as any modifications or adaptations thereto, remain the property of the Proposer.

Data Ownership – Alternative Language

1. The State owns the rights to all electronic information (electronic data, electronic information systems, electronic databases, etc.) and all supporting documentation created as part of the Contract. The Contractor shall deliver sufficient technical documentation with all data deliverables to permit the State to use the data.

Data Ownership – Alternative Language

1. The State is the owner of all data made available by the State to the Contractor or its agents, Subcontractors or representatives under the Contract. The Contractor shall not use the State's data for any purpose other than providing the Services, nor shall any part of the State's data be disclosed, sold, assigned, leased or otherwise disposed of to the general public or to specific third parties or commercially exploited by or on behalf of the Contractor. No employees of the Contractor, other than those on a strictly need-to-know basis, shall have access to the State's data. The Contractor shall not possess any lien or assert any lien or other right against the State's data. Without limiting the generality of this Section, the Contractor must only use Personally Identifiable Information as strictly necessary to provide the Services and must disclose the information only to its employees who have a strict need to know the information. The Contractor must comply at all times with all laws and regulations applicable to Personally Identifiable Information.
2. The State is the owner of all State-specific data under the Contract. The State may use the data provided by the Contractor for any purpose.

Additional Terms

1. **Additional Terms.** No "Shrink-Wrap," "Click-Wrap" or other terms and conditions or Agreements ("Additional Terms") unilaterally provided with any products or software hereunder shall be binding on the State, even if use of such products and software requires an affirmative "acceptance" of those "additional terms" before access is permitted. All such additional terms shall be of no force or effect and shall be deemed rejected by the State in entirety.

Audit

1. **Audit.** Licensor may audit Licensee usage and compliance with the terms of this Agreement no more than once per calendar year. Upon a ninety (90) day written notice and at its sole cost and expense, Licensor may direct an accounting firm reasonably acceptable to Licensee to audit the number of licenses being used. Licensee shall have the right to reject the auditor selected by Licensor and request a replacement in its sole discretion. The scope of the audit by Licensor shall be limited to a review of Licensee’s written records pertaining to the software licenses under contract. In the event Licensee desires to perform a review of Licensee’s written records pertaining to the software licenses under contract onsite at Licensee’s place of business, including Licensors accounting firm, such onsite audit shall be conducted during Licensee’s normal business hours at the location designated by Licensee. For the avoidance of any doubt, Licensor nor its accounting firm shall be permitted direct or indirect access to Licensee’s internal network or any Licensee hardware to determine the number of licenses in use by Licensee. In the event Licensee has a dispute regarding the quantity of licensed products in use as a result of Licensor’s audit, the parties shall negotiate in good faith to resolve and mutually agree upon reconciliation of amounts due to Licensor, if any. Licensee shall be obligated only to purchase those unpaid licenses found to be in use in an amount not to exceed Licensee's then-existing discounted rate structure and for no other costs, fees, or penalties and per the Payment Terms of the Agreement.
2. Licensor and such auditors shall abide by the confidentiality terms of this Agreement in the care of Licensee information and abide by Licensee’s security regulations. In addition, a mutual non- disclosure agreement shall be presented by Licensee for signature by Licensor and Licensor’s auditors, which shall not be unreasonably refused by Licensor or its auditors. If the mutual non- disclosure agreement is not executed by Licensor and Licensors’ accounting firm within ninety (90) days from its receipt by Licensor, Licensee shall regard the request to audit as terminated.

Viruses, Disabling Devices and Illicit Code

1. Licensor represents, warrants, and covenants that the licensed software and all software upgrades shall not contain any disabling devices or Induced Inhibiting Code (IIC) (as defined below), and Licensor shall not electronically repossess programs licensed to you through remote command activation. Licensor shall use all commercially reasonable measures to screen the licensed Software to avoid introducing any virus or other destructive

programming that is designed (i) to permit unauthorized access or use by third parties to the software installed on your systems, or (ii) to disable or damage your systems. Licensor shall not insert into licensed Software any code or other device that would have the effect of disabling or otherwise shutting down all or any portion of the licensed Software based on the elapsing of a period of time, exceeding an authorized number of copies, advancement to a particular date or numbers or other similar self-destruct mechanisms (sometimes referred to as "time bombs," "time locks," or "drop dead" devices) or that would permit Licensor to access the licensed software to cause such disablement or impairment (sometimes referred to as a "trap door" device). Licensor shall not invoke such code or other device at any time, including upon expiration or termination of this Contract for any reason. For the purpose of this section, a "Disabling Device" shall mean code intentionally embedded in a Program by Licensor for the sole purpose of partially or completely halting use of the Program on conditions set by Licensor. “IIC” is defined as any deliberately included application or system code that shall degrade performance, result in inaccurate data, deny accessibility, or adversely effect, in any way, programs or data or use of the system.

Infringement Indemnification

To the best of Licensor’s knowledge, the State’s permitted use of the Licensed Software shall not infringe the intellectual property rights of any third party. If a third party makes a claim against the State that any information, design, specification, instruction, software, data, or material (“Material”) furnished by Licensor and used by the State infringes its intellectual property rights, Licensor shall indemnify and at its own expense (including payment of attorney’s fees, expert fees and court costs) defend the State against any loss, cost, damage, liability or expense from any and all third party claims that the License Software infringes any patent, copyright, trade secret or other proprietary right of a third party and shall indemnify and hold harmless the State from any amounts assessed against them in a resulting judgment or amounts to settle such claims provided that the State does the following:

- notifies Licensor promptly in writing, not later than thirty (30) days after the State receives notice of the claim (or sooner if required by applicable law);

- gives Licensor sole control of the defense and any settlement negotiations; and gives Licensor the information, authority, and assistance the Provider needs to defend against or settle the claim.
- If Licensed Software is, or is likely to be, the subject of an infringement claim, or, Licensor believes or it is determined that any of the Material may have violated someone else's intellectual property rights, Licensor, at its expense, shall choose to either (i) modify the Material to be non-infringing (while substantially preserving its utility or functionality) (ii) obtain a license to allow for the State's continued use, or (iii) replace the Licensed Software with another system or components of comparable quality and functionality. If Licensor is unable to provide one of these remedies within forty-five (45) days of notice of the claim (unless such period is extended by the State), Licensor shall have the right to terminate this Contract and refund all fees paid hereunder for the Licensed Software. Licensor shall not indemnify the State if the State alters the Material or uses it outside the scope of use identified in Licensor's user documentation or if the State uses a version of the Materials which has been superseded, if the infringement claim could have been avoided by using an unaltered current version of the Material which was provided to the State provided Licensor has notified the State in writing that use of the current version would have avoided the claim. Licensor shall not indemnify the State to the extent that an infringement claim is based upon any information, design, specification, instruction, software, data, or material not furnished by Licensor. Licensor shall not indemnify the State to the extent that an infringement claim is based upon the combination of any Material with any products or services not provided by Licensor. Licensor shall not indemnify the State to the extent that an infringement claim is based upon Third Party Programs that were not a part of any product recommendation made to the State by Licensor.

Software Cloud Services

Data Protection

1. Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of State Data. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of State Data and comply with the following conditions:

a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of State Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

b. All State Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the State Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the Service Level Agreement (SLA), or otherwise made a part of this Contract.

c. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The State shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified by the State.

d. At no time shall any data or processes — that either belong to or are intended for the use of the State or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the State.

e. If the State allows Non-Public Data to be accessed by Contractor personnel by mobile devices, the data shall be encrypted on the mobile devices. Hashing and encryption techniques will be used when sensitive data is stored in all data stores, and secure data transfer protocols. – TLS/SSL with a server certificate, HTTPS, and WS-Security, or SFTP - will be used when data is transferred from one component to another.

f. The Contractor shall not use any information collected relating to the services issued from this Contract for any purpose other than fulfilling the services.

Data Location

The Contractor shall provide its services to the State and its end users solely from data centers in the U.S. Storage of State Data at rest shall be located solely in data centers in the U.S. The Contractor shall identify the location(s) of its data centers where State Data will be processed or stored. This includes locations for Subcontractor and/or business partner processing storage locations, locations of backup data, and disaster recovery locations. The Contractor shall not allow its personnel or contractors to store State Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access State Data remotely only as required to provide technical support.

The Contractor shall provide email notification to designated State point of contact(s) of any changes to the location of State Data.

Security Incident or Data Breach Notification

Security Incident or Data Breach Notification: Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the State Data disclosed.

a. May include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, required by law, or the Contract.

b. Security Incident Reporting Requirements: The Contractor shall report a Security Incident to the State identified contact within 72 hours based on the standards set by NIST 800-61 without reasonable delay, or as defined in the SLA or Contractors System Security Plan ("SSP"). Discussing Security Incidents with the State should be handled as urgent, as part of Contractor's Incident Response: Contractor may need to communicate with outside parties regarding a Security Incident, which communication and mitigation processes as mutually agreed upon, defined by law or contained in the Contract.

c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed Data Breach that affects the security of any of State Data, the Contractor shall (1) within four (4) hours and without out reasonable delay notify the State, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.