Bentley University Vendor Contract Review Checklist

This document provides a review checklist for vendor contract reviews. You can identify if these components are present in the contract and any issues and mitigations. Typically you can mark up a proposed vendor contract and return with requests to change or eliminate clauses. Vendors will not always agree to every proposed change, but requested changes can possibly be used as leverage in further negotiations with the vendor.

Cells in green cover key contract clauses which should at a minimum be reviewed. Depending on the type of contract, you can optionally use the other sections of this document.

Contract item	Present	Issues/Mitigation
• **Payments and Fees** - Contracts should describe the compensation, variable charges, and any fees to be paid for non-recurring items and special requests. Agreements should also address which party is responsible for the payment of any legal, audit, and examination fees related to the activity being performed by the service provider. Where applicable, agreements should address the party responsible for the expense, purchasing, and maintenance of any equipment, hardware, software or any other item related to the activity being performed by the service provider.		
• **Payment Terms –** Contract should clearly state payment terms (preferred Net 60). Attempt to eliminate any late payment/penalty clauses in the contract.		
• **Contract Term –** Contract should clearly state initial and subsequent terms, and annual maintenance or subscription costs. Multi-year agreements should hold annual increases flat, or at a rate of 3% or lower (or annual CPI).		
• **Renewal Fees/Increases** – Contract should stipulate renewal fees and maximum increase for renewal at end of initial term.		
• **Evergreen clauses** - In no event should a contract include an "evergreen" clause that provides for automatic renewal for a period greater than one year without written acceptance of the renewal by		

Bentley. Preferred alternatives to an "evergreen" clause will vary from contract to contract, but include: • An open-ended extension clause providing that the Bentley may terminate with or without cause upon prior written notice to the vendor; • A fixed-term contract; or • A fixed-term contract which may automatically be extended upon the mutual agreement of the parties.		
• **Ownership of Data –** if the service or application stores Bentley data, the contract should be clear that Bentley is the owner of the data. If personally identifiable information, FERPA or other sensitive data is being stored in the service or application, what protections does the vendor put in place?		
• **Data Protection –** Is there language protecting Bentley in the event of a breach? Standard language for Bentley data protection.		
• **Security and confidentiality** - The contract should address the vendor's responsibility for the security and confidentiality of any non-public data entrusted to the vendor consistent with state and federal law and regulations as amended from time to time. The contract should require the vendor to promptly notify the Bentley of any unauthorized access to or use of such data. The contract should require the vendor to take reasonable measures to protect against unauthorized access to or use of such data in connection with its disposal.		
• **Termination and indemnification** - Agreements should define events of a contractual default, list of acceptable remedies, and provide opportunities for curing default. Contracts should include termination and notification requirements that provides Bentley with sufficient time to transfer services to another service provider. Agreements should also address a service provider's preservation and timely return of Bentley's data, records, and other resources. Agreements should provide for service provider		

indemnification of financial institutions for any claims against financial institutions resulting from the service provider's negligence.		
• **Choice of law** – The contract should state the laws of the State of Massachusetts will govern the interpretation of the contract or, in the alternative, should be silent on the choice of law.		
• **Software regulatory compliance** – Software regulatory compliance - The contract should require any software associated with the product or service to be in compliance with all applicable laws and regulations.		
• **Dispute resolution** - If possible, the contract should establish a dispute resolution process for the purpose of resolving problems between the Bentley and the vendor in an expeditious manner, as well as provide for continuation of services during the dispute resolution period.		
• **Forum selection clauses** – A contract generally should state that disputes arising under the contract must be brought in the federal or state courts where the Bentley is located or, in the alternative, should be silent on the issue.		
• **Insurance** - The contract should require the vendor to maintain adequate insurance and to notify the Bentley of material changes in coverage. For example: **Insurance. VENDOR shall carry and maintain at all times during the term of this Agreement, the lines of insurance coverage with minimum policy limits as follows: (i) Workers' Compensation with limits as required by applicable statute; (ii) Employers' Liability with limits of $xxxxxxx, per accident and in the aggregate; (iii) Commercial General Liability with limits of $xxxxxxx, combined single limit bodily injury and property damage, per occurrence and in the aggregate; (iv) Business Automobile Liability with limits of $xxxxxx, combined single limit, each accident; (v) Umbrella/Excess Liability with respect to (ii), (iii) and (iv) above, with limits of $xxxxx per occurrence and in the aggregate; (vi) Professional (Errors and Omissions) Liability coverage with a minimum**		

combined single limit of $xxxxx; and (vii) Fidelity (Bond)/Crime insurance in the amount of $xxxxxx for the joint protection of Vendor and Customer from any loss, theft or embezzlement of Customer's property or funds caused by any officers, employees or agents of Vendor. Vendor shall use an insurance provider having an A.M. Best Company rating of A- or better with financial size category of X or higher. Vendor shall provide Customer certificates of insurance evidencing coverage upon Customer's request. Vendor shall endeavor to provide Customer with 30 days prior notice of cancellation of any of the insurance required under this Section 13.9.		
• **Key deliverables and project timelines** - The contract should specify the "key deliverables" anticipated from the third-party service provider. Project timelines (including any intermediate milestones) should be specified in the contract, thus making it possible for the Bentley to monitor the vendor's completion of its obligations on a timely basis.		
• **Limits of liability** - If the vendor wishes to limit its liability, the Bentley should ensure that the proposed limit is in reasonable proportion to the amount of loss the Bentley might experience as a result of the vendor's failure to perform.		
• **Ownership and license** - The contract should address ownership and allowable use by the vendor of the data, equipment, software, and other intellectual property covered by the contract.		
• **Performance measures** – If applicable, contracts should include performance standards defining minimum service-level requirements and remedies for failure to meet those requirements. For example, the contract may specify system uptime requirements, maximum error rates, and/or deadlines for completion of daily processing.		
• **Subcontractors** - Contract provisions should clearly state that the primary service provider has overall accountability for all services that the service provider and its subcontractors provide. Agreements should define the services that may be subcontracted, the service provider's due diligence process for		

engaging and monitoring subcontractors, and the notification and approval requirements regarding changes to the service provider's subcontractors. Suggested verbiage: **In the event that Vendor uses subcontractors in fulfilling Vendor's obligations in providing the Services under this Agreement, Vendor shall be responsible for each subcontractor's acts, omissions and compliance with, and/or breach of, this Agreement during the course of each subcontractor's fulfillment of the said Services.**		
Outsourced or Managed Service Contracts		
• **Business resumption plans** – Business resumption plans - The contract should address the vendor's responsibility for backup and recovery of the business function. The vendor should be required to test the plans and provide results to the Bentley. Business recovery timeframes should be established that meet the Bentley's business requirements.		
• **Compliance** – The contract should require compliance with regulations and/or standards as applicable: • **Credit Card Compliance** - Contracts with service providers that receive credit cardholder information should contain a clause requiring compliance with PCI-DSS. • **Identity Theft Red Flag clause** - The contract should require the vendor to have policies and procedures in place to detect identity theft red flags that may arise in the performance of the service provider's activities. The contract should further state whether the vendor will contact the Bentley or take its own appropriate steps to investigate, prevent, or mitigate identity theft.		
• **Customer complaints** – The contract should specify whether the Bentley or the vendor is responsible for responding to the complaints. If the vendor is responsible, the contract should require		

that a copy of all responses be forwarded to Bentley. The contract should require that all customer complaints received by the vendor with respect to the product or service be forwarded to Bentley.		
• **Management reporting** - The contract should specify the frequency and types of reports expected, including reports such as the following: o Audited financial statements. o Business resumption testing reports. o Hiring Practices o Security Incident Response testing o Performance-measure reports. o Security, internal control, and other audit reports – e.g. SSAE-16 reports. o Vulnerability scans – network and web application as applicable. ▪ **Vulnerability Scan. Vendor** will use a third-party vendor to conduct vulnerability scan, and will make summary report of the vulnerability scan available upon request (but no more than once per year) to the extent it is applicable and required by law.		
• **Onsite audit coverage** - If considered necessary, the contract should give Bentley personnel the right to perform on-site audits to verify compliance with specific contract terms and with security and/or control requirements.		
Software/Hardware/SaaS contracts		
• **Vendor support –** what are the vendor support commitments and SLAs? Are they clearly stated in the contract? Do vendor support hours coincide with Bentley business hours?		
• **Computer sizing** - If the vendor sizes the equipment and/or the configuration requirements to process our projected activity level, these specifications should be documented. If the solution is inappropriately sized, the vendor should be responsible for any resulting additional costs to the Bentley.		

• **Operating system support** – The vendor will support new operating system software within 12 months of the general availability date of the operating system software. If the vendor fails to support the new operating system in this time period, the customer will be refunded 1/12 of the annual maintenance fees each month until the operating system software is supported by the vendor.		
• **Software license** – The contract should state that the customer will be allowed three installations of the software at no additional charge. The installations will be for the production, test, and disaster recovery environments. Software delivery should be via the Internet to minimize the state tax liability.		
• **Software/Hardware maintenance** – The contract should where possible eliminate the CPU upgrade clause or have the license cover a larger CPU.		
• **Software/Hardware maintenance** – The contract should where possible eliminate per processor charges on open system applications, NT, LINUX, and UNIX and on mainframe systems eliminate CPU upgrade, MIPS, and MSU charges.		
• **Software/Hardware maintenance** – The contract should where possible request maintenance discounts by getting two/three year contracts. Pay in three equal payments or upfront depending on the level of the discount;		
• **Software/Hardware maintenance** – The contract should where possible state we can use the product even when maintenance has been dropped.		
• **System upgrades** – The contract should state that all upgrades for versions and releases are included as long as maintenance is paid. Where possible, the vendor will use online session for access to the servers and/or applications for maintenance purposes.		

• **Security weakness** – The contract should state the vendor will notify the customer when a known or newly discovered security weakness is in their system along with a corrective action plan. Suggested verbiage: **Security Vulnerabilities. Customer's technology division employs well-known scanners (such as Nessus and Qualys) on a regularly scheduled basis to identify and assign industry standard Common Vulnerability Scoring System (CVSS) rating to security vulnerabilities in its systems and software. XXXXXX (Vendor) agrees to use commercially reasonable efforts to resolve the security vulnerability based on the CVSS rating and following timeframes: HIGH-rated security vulnerabilities within 30 days, MEDIUM-rated security vulnerabilities in 60 days, and LOW-rated security vulnerabilities in 180 days. These categories correspond to the CVSS bas scores of :** • **HIGH = 7.0 to 10.0** • **MEDIUM = 4.0 to 6.9** • **LOW = 0 to 3.0** **If the vulnerability is not resolved according to the timeline above Customer has the right to terminate the agreement without obligation or liability of any kind.**		