Data Protection Contractual Language

Version 2.0: September 2009

Table of Contents:

- Purpose
- Disclaimer
- References
- Background
- Criticality
- How to Use This Toolkit
- The Three Steps
- A Word About Requests For Proposals (RFP)
- Decision Tree
- A Word About Third-Party Risk Assessments
- A Word About Contract Monitoring
- Themes
- Appendix 1
- Appendix 2

Purpose:

To provide sample proposal and contract language for common themes related to data protection as well as practical guidance as to when and how to consider the themes when drafting or reviewing a request for information (RFI), request for proposal (RFP) or contract.
Top

Disclaimer:

The data security themes and sample contractual clauses are provided for informational purposes only and are not to be construed as legal advice. The data security themes provided are issues for institutions of higher education to consider when drafting requests for information (RFI), requests for proposal (RFP), or contracts that might involve institution data; however the themes are neither all-inclusive nor exhaustive, nor is every theme applicable to every RFI, RFP, or contract. In addition, federal, state, and local laws and regulations may also have an impact on data security provisions that should be included in a particular RFI, RFP, or contract. Additionally, contract terms dealing with issues other than information security may impact the effectiveness or enforceability of the suggested clauses in this document. The sample RFP requirements and questions as well as contract clauses contained in this document should be seen as a starting point for discussion and may need to be modified as appropriate for the intended use.

For the foregoing reasons, it is essential that any intended use of the sample requirements and contractual clauses be reviewed by appropriate institutional legal counsel in the full context of the proposal requirements and contractual arrangement prior to communication to the other contracting party and during negotiation of terms. Ultimately, the greatest concern should be that the final negotiated result accurately reflects the intention of the parties and the reality of the situation.
Top

References:

The following materials were used as the basis for this document.

- Documents provided by committee members
- EDUCAUSE Policy Discussion Group list references provided by committee members
- SANS (policies references)
- ISO/IEC 27002:2005 Code of Practice for Information Security Management (pertinent language included, Appendix 1)
- NIST Sp. Pub. 800-53, Rev. 2; section 2.4 (Security Controls in External Environments) (pertinent language included, Appendix 2).
    - *See control AC-20 (Use of External Information Systems) for additional guidance.*
- Catholic University of America FERPA page (see Data Security Addendum)
- Solutions Training Group: *"Writing, Evaluating, and Managing Airtight RFPs"* Bruce E. Truitt, Instructor.
- SupplierSelect News *"Writing Good RFP Questions"* 2008
- The University of Texas System Office of General Counsel *"Security and Privacy Requirements for Information Resources / Services Contract"*
- The University of Texas Health Science Center at San Antonio: Third-Party Management of Information Resources Policy
- The University of Texas Health Science Center at San Antonio: Third-Party Risk Assessment Security Standard
- The University of Texas at Austin: Security Checklist for Hosted IT Services
- Northwestern University *Contract language for the secure handling of sensitive data*
- Princeton University *Information Security Policy, Confidential Information Addendum*
- Purdue University *Purdue University Information Security Program, Addendum to Service Provider Agreement*
- University of California *Additional Terms and Conditions - Data Security Appendix*
- University of Southern California *Information Security Policy, Confidentiality Agreement*
- Info-Tech Research Group "retool Requirements Gathering to Ensure Compliance" February 7, 2007

NOTE: Sample RFP requirement questions and contractual clauses have been sanitized and identifying information related to a particular institution of higher education has been removed. In addition, while all of the references provided by working group members were reviewed, the working group stopped adding sample questions and clauses to this document once we accumulated several samples for each theme (unless one of the references included a unique wording or clause that was not already addressed). Institutions of higher education are encouraged to add their own sanitized sample questions and clauses as a way to make this document "living" following the uniqueness principle.
Top

Background:

Institutions of higher education function within a policy and regulatory context uniquely their own. While regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, the Gramm-Leach-Bliley Act (GLBA), the Payment Card Industry Data Security Standard (PCI DSS), and state security breach notification laws belong to our common lexicon, few among the growing body of third-party providers of information services to higher education are aware of FERPA or the rich tapestry of internal policies governing data access and distribution. Further, the seemingly innocuous nature of many contemporary services (such as social networking) has allowed companies to prosper merely by *asserting* rather than *demonstrating* strong security practices.

Conveying the appropriate information security requirements, eliciting meaningful and specific responses to those requirements, assessing potential risks, and, utilizing the appropriate contractual clauses assist in framing the contracting party's role within your institution's regulatory context. For example, by including a section that calls attention to FERPA and to the fact that some of the data the contracting party will be handling qualifies as part of a student's educational record, you ensure that the vendor acknowledges that they will be operating within an environment where FERPA considerations will inform their obligations.

This last point is made to underscore the need for an institution to fully understand the nature and scope of the data it is protecting in any contract. Ultimately, this will be the determining factor in choosing to include any particular proposal requirement or contract language.

The challenge facing individuals responsible for drafting and reviewing RFPs and contracts for the purchase of information technology products and services - often individuals with job functions other than legal counsel - is, considering the nuances and particularities of each contract, knowing what clauses to include or look for in a contract and what clauses could be unnecessary or overburdening.
Top

Criticality:

The decision to include a specific contractual clause is contingent on four primary criteria:

- regulatory requirements (usually State or Federal laws such as the Family Educational Rights and Privacy Act (FERPA)),
- institutional policy (such as strong password formation policy or data classification schemes),
- industry best practices (such as the encryption of sensitive data in transit or at rest), and
- situational considerations, described respectively in the examples below.

Each of the themes listed below have been labeled as to criticality by the working group as appropriate for each rubric. Please note that every institution will need to review these in light of their specific situation in order to ensure alignment with local institutional policy and applicable laws and regulations.

Category 1: Mandatory use in order to comply with Federal, State, or Agency regulations, contains Personally Identifiable Information

Category 2: Mandatory use in order to comply with institutional policies

Category 3: Recommended use in order to comply with generally accepted best practices

Category 4: Recommended to address common situational requirements

Top

How To Use This Toolkit:

The Three Steps

As a practical approach to address the aforementioned challenge, this document divides the procurement of information technology products and services into three steps and organizes proposal and contractual language security themes around a decision tree consisting of four questions that an individual drafting or reviewing an RFP or contract should ask her/himself.

The basic idea is to consider each step and each question at a time in sequence and to select only those steps and themes that apply to the product or service being purchased and the data being protected. Nevertheless, as these processes are not necessarily linear, the individual may find a different approach worthwhile.
Top

The Three Steps:

Assuming that we already know "*what*" we are procuring and that we are now concerned with the "*from whom*" we procure it, the procurement process for information technology products and services can be divided into the following three general steps:

1. Vendor Selection
2. Contract Negotiation

3. Contract Monitoring

Top

A Word About Requests For Proposals (RFP):

Decision Tree

An RFP is an invitation for vendors to submit a proposal on a specific product or service. RFPs are usually designed to get vendors to provide a creative solution to a business problem or requirement, bring structure to the procurement decision, and allow the risks and benefits of a solution to be identified clearly upfront. The creativity and level of detail that vendors choose to include in their proposals **should** be used to evaluate the quality of the vendors' proposals, their understanding of your business and requirements, and as a means of comparison against each other.

More often than not, institutions of higher education are very good at telling vendors what level of security is required or wanted in a product or service but not as good or diligent in asking vendors to describe how they propose to meet those requirements. Consequently, vendors need only to assert rather than demonstrate strong security practices to meet evaluation criteria. It is critical that the RFP conveys the appropriate information security requirements and elicits meaningful and specific responses that describe how the vendor will meet those requirements.

Consider the following when drafting or reviewing an RFP:

- Clearly define the data to be protected.
- Define specifically your information security requirements (needs) and clearly differentiate between what is needed and what is wanted. The items below depend from these first two points.
- To the extent possible, include all security requirements in a separate and clearly identified section of the RFP. If security requirements are dispersed throughout multiple sections of the RFP it is difficult to identify and consider them as a separate evaluation criteria.
- Not only tell vendors what you require but ask them how they propose to meet the requirements. Also, consider asking what alternatives are available in case requirements cannot be met. Just listing the requirement or asking a Yes/No question will not elicit meaningful and specific responses.
- Frame questions in a way to minimize ambiguity. Questions should clearly communicate the institution's requirement priorities and correspond to evaluating criteria.
- Avoid, to the extent possible, subjective requirements such as "highest degree of quality", "according to standards", or "all reasonable means". All these are subject to interpretation and misunderstanding. What is reasonable to one may be unacceptable to others and so on.
- Based on identified requirements, make appropriate use of "must", "should", "shall", and "will". As part of the review process, remove any conflicting, contradictory, or overly onerous criteria.

The Sample RFP Language provided in the themes below are intended to be just that - examples and a memory-jogger to assist in identifying specific items that may need to covered but are not.

Top

Decision Tree:

As a practical approach to address the aforementioned challenge, this document divides the procurement of information technology products and services into three steps and organizes proposal and contractual language security themes around a decision tree consisting of four questions that an individual drafting or reviewing an RFP or contract should ask her/himself.

The decision tree questions are:

1. What should be the Core Language that I should always have in an RFP or contract?
2. Are the process and/or data covered in my RFP or contract impacted by a federal, state, or local law, regulation, or contractual obligation?
3. Are there other common security items that apply to the process, product, service, or data covered in my RFP or contract?

Are there special conditions that I should consider? Am I missing something?

Top

A Word About Third-Party Risk Assessments:

A Word About Contract Monitoring

These days of outsourcing, software as a service, and cloud computing, institutions of higher education are increasingly turning to third-party service providers to maintain, manage, transmit, or store institution-owned information resources to improve delivery of services, gain efficiencies, and reduce cost. ISO/IEC 27002:2005, Reference 6.2.1 *Identify Risks Related to the Use of External Parties* underscores that decision making and action plans to address information security issues are to be "based on risk". In that regard, institutions of higher education are diligent in assessing the risk of critical information resources *already in production* but they are somewhat remiss at assessing and defining the incremental risk to the institution *prior* to engaging a third-party service provider to host or provide a service on behalf of the institution.

To ensure that adequate security controls are in place prior to finalizing any contract agreement, institutions - including their respective schools, departments, clinics, and centers - engaging third-party service providers to procure information technology services ***should*** conduct a third-party risk assessment for all services (applications, hosting, systems, etc) **that would involve the collection, processing, transmission, or storage of Confidential or Sensitive data as defined by the institutions' respective Data Classification Policy**. Consider the following when engaging third-party service providers to procure information technology services:

- Assess the risk of engaging the finalist, or top two third-party vendors. This can be done by requiring finalist vendors to complete a third-party information security assessment survey like the **Higher Education Cloud Vendor Assessment Tool** developed by the HEISC Shared Assessments Working Group.
- Review the answers and identify "weak" points. Do the vendors provide additional documentation? Do responses pass the "smell test"?
- Schedule a conference call with vendor contact person to go over the assessment results and the institution's requirements
- Call vendor references to validate the assessment results and learn if there is evidence of non-performance at other clients sites
- Identify areas needing mitigation and required cure and include them as language in final agreement and/or statement of work.

Resources:

- Higher Education Cloud Vendor Assessment Tool developed by the HEISC Shared Assessments Working Group
- Third-Party Information Security Assessment Survey developed by The University of Texas Health Science Center at San Antonio.
- Shared Assessments provides tools to evaluate third party vendor software and services.

Top

A Word About Contract Monitoring

Themes

Monitoring can mean different things to different people. For the purpose of this document, monitor means to assess, to watch, to keep track of, or to check, usually, with a special purpose. It does not mean or imply to verify or even to test. Actually, monitoring is more of a spectrum that ranges from just "keeping an eye" in the low end to requiring a site audit in the high end. Given the availability of resources at institutions of higher education, verification could be an impractical and significantly costly requirement if applied to all or most third-party contracts.

Effective contract monitoring requires a process or methodology in place that defines the approach to take based on the risk of the contract or engagement - activities should be more stringent and closer to the high end of the spectrum as risk increases or when exceptional situations warrant them. Institutional policy may refer to instances in which the sharing of sensitive data will result in a significant risk. Again, "significant" can mean a number of things but, ultimately, depends on the institution's risk management practices and risk tolerance (i.e., what is acceptable risk). Only in cases of very high risk or when exceptional situations may warrant it should contract monitoring include a requirement to perform a site audit, of results of a Statement on Standards for Attestation Engagements (SSAE) No. 16 (formerly SAS 70) audit, or of results of an audit performed by an independent auditor.

Third, what should an institution do to monitor compliance with agreement requirements in most cases? Again, let's focus on the Section's intent: Define the incremental risk to the institution when engaging third-party IT service providers as well as defining a due diligence process for mitigating those risks - third-party risk from remote access, data transmission and offsite storage.

Consider the following as an outline for a contract monitoring process:

1. **System / Application / Process Implementation**
    a. Identify the individual(s) responsible for monitoring the contract.
    b. During project status meetings:
        i. Assess and review status reports regarding progress made in the implementation of the security requirements included in the contract and/or statement of work.
        ii. Identify new areas or security requirements that may arise from changes in scope
    c. If applicable, perform or request audit of vendor security practices and procedures and/or perform penetration test
    d. During final test and prior to sign-off
        i. Test system/application/process security functionality required in the contract
        ii. Review progress reports and determine if all security requirements included in the contract and/or statement of work were completed.
    e. If applicable, perform application scan
2. **Post Implementation**
    a. Follow up with system/application/process owner.
        i. Require owner to perform a risk assessment based on policy (annual if high risk or mission critical and bi-annual for the rest)
        ii. Review with the owner the risk assessment results. Any concerns? Any problems? Any unknowns that need to be addressed with the vendor?
    b. Follow up with vendor. Access logs available? Any pending items resolved? Are things on their end as expected? Any owner concerns? Risk assessment identified deficiencies?
    c. Based on risk (annually or bi-annually), resubmit third-party information security risk assessment to assess what has changed, what needs closer scrutiny, or identify inconsistencies with previous assessments
    d. Establish a working relationship with your vendor
    e. Participate in vendor's product improvement committee. What changes are been considered? How would they impact the institution's risk and security postures
    f. Review security incidents involving the system/application/process. Are these due to non-compliance?
    g. If applicable, based on the contract, require subsequent assurance tests.

For current signed contracts, assess their risk (if it has not already been done), and start with the steps listed in the Post Implementation section above as needed.

It is important to keep in mind that contract monitoring is the last step of a cascading progression. The initial identification of process and data impacted as well as initial security requirements are used to formulate questions for the RFP. The answers to the RFP are used to evaluate vendors and refine the security requirements. The evaluation and risk assessment of finalists refine the security requirements that will, in turn, be added as language to the contract or statement of work. And, finally, it is the final contract and corresponding risk level that determine the appropriate contract monitoring approach.

Top

Themes

Sample contract clauses are available for each of the following themes:

- Assistance With Litigation
- Credit Card Data
- Data Definition
- Data Protection After Contract Termination
- Data Sharing
- Data Transmission (including Encryption)
- Financial Information
- General Data Protection
- Indemnification as a Result of Security Breach
- Intellectual Property Protection
- Notification of Security Incidents
- Protected Health Information (HIPAA)
- References to Third Party Compliance With Applicable Federal, State, and Local Laws and Regulatory Requirements
- References to Third Party Compliance With University Policies, Standards, Guidelines, And Procedures
- Security Audits and Scans (Independent Verification)
- Security Incident Investigations
- Separate Document Addressing Data Protection
- State Breach Notification Laws
- Student Education Records (FERPA)
- Use of Data

Top

Appendix 1
Appendix 2
