Supplemental Provisions
CSU General Provisions for Information Technology Acquisitions
for
Information Security Requirements

Introduction

This document contains contract language to be used to develop supplemental provisions for CSU General Provisions for Information Technology Acquisition contracts involving the use of CSU information assets. This language is intended to be used when the nature of the information asset or resource requires protection. Use of supplemental contract language is required in order to comply with ICSUAM Policy 8040 Section 200, Payment Card Industry Data Security Standards (PCI DSS), NACHA, FERPA, and the Health Insurance Portability and Accountability Act (HIPAA). Additionally, supplemental language may be used to manage risks associated with allowing contractors to access, store or otherwise manage CSU information assets.

DEFINITIONS

Affiliate - an entity now or hereafter controlled by, controlling or under common control with a Party. Control exists when an entity owns or controls more than 50% of the outstanding shares or securities representing the right to vote for the election of directors or other managing authority of another entity.

Confidential Information - The term "Confidential Information" shall mean this Agreement and all proprietary information, data, trade secrets, business information, any Protected Information regarding students, employees or other individuals or entities, including but not limited to, Social Security numbers, other tax identification numbers, credit card, bank account and other financial information, and other information of any kind whatsoever which:

a) a Party ("Discloser') discloses, in writing, orally or visually, to the other Party ("Recipient") or to which Recipient obtains access in connection with the negotiation and performance of this Agreement, and which

b) relates to:
   i. the Discloser, or
   ii. in the case of Contractor as Recipient, the CSU, its students and employees, and its third-party contractors or licensors who have made confidential or proprietary information available to the CSU.

Party – The CSU or Contractor.

CSU Protected Data - data defined as "Protected Level 1" and "Protected Level 2" in the CSU Data Classification Standard (http://www.calstate.edu/icsuam/sections/8000/8065_FINAL_DRAFT_Data_Classification_CW_V4.pdf)

Representative - an employee, officer, director, or agent of a Party.

Relationship Manager - the respective employees of each Party that each Party shall designate to act on its behalf with regard to matters arising under this Agreement; each Party shall notify the other in writing of the name of their Relationship Manager; however, the Relationship Manager shall have no authority to alter or amend any term, condition or provision of the Agreement; further, each Party may change its Relationship Manager by providing the other Party with prior written notice.

Subcontractor - a third party to whom Contractor has delegated or subcontracted any portion of its obligations set forth herein.

Work Product - All discoveries, inventions, work of authorship or trade secrets, or other intellectual property and all embodiments thereof originated by Contractor within the scope of Services provided under this Agreement, whether or not prepared on CSU's premises.

Contractor – Contractor is any party to an agreement with the CSU along with any Contractor Representative, Subcontractor, Affiliate, or other entity over whom the Contractor has control.

1.0 ACKNOWLEGEMENT

Contractor acknowledges that its contract/purchase order with the California State University ("the CSU") may allow the Contractor access to CSU Protected Data including, but not limited to, personal information, student records, health care information, or financial information. This data may be transferred in various forms, notwithstanding the manner in which or from whom it is received by Contractor subject to state laws that restrict the use and disclosure of such information, including the California Information Practices Act (California Civil Code Section 1798 et seq.) and the California Constitution Article 1, Section 1. Contractor represents and warrants that it will keep CSU Protected Data confidential both during the Term and after the termination of the Agreement.

2.0 DISCLOSURE REQUIREMENTS

Contractor agrees that it will include all of the terms and conditions contained in this agreement in all subcontractor contracts providing services under this Agreement.

Contractor shall not use or disclose CSU Protected Data other than to carry out the purposes of this agreement. Contractor shall not disclose any CSU Protected Data other than on a "need to know" basis and then only:

a. To its representatives, provided however, that each such employee or officer has entered into a confidentiality agreement;

b. To affiliates of or Subcontractors to Contractor, only if previously notified and provided that

   i. Use by such Affiliates or Subcontractor shall be limited to the purpose of this agreement;
   ii. Affiliate or Subcontractor is bound by contract and or confidentiality agreement to protect CSU data from unauthorized access.

If required by a court of competent jurisdiction or an administrative body to disclose Protected Data, Contractor shall notify the CSU in writing prior to any such disclosure in order to give the CSU an opportunity to oppose any such disclosure. Prior to any disclosure of Confidential Information as required by legal process, the Contractor shall:

c. Notify the CSU of any, actual or threatened legal compulsion of disclosure, and any actual legal obligation of disclosure immediately upon becoming so obligated, and

d. Delay disclosure until the CSU has provided contractor with notice that they will oppose or agree to such disclosure or the time specified for legal compliance is reached.

Any access, transmission, or storage of Protected Data outside the United States shall require prior written authorization by the CSU.

2.1 Exceptions to Obligations of Confidentiality

With the exception of the data classified as "Protected Level 1" or "Protected Level 2" under the CSU Data Classification Standard, identified in (http://www.calstate.edu/icsuam/sections/8000/8065_FINAL_DRAFT_Data_Classification_CW_V4.pdf), obligations of confidentiality shall not apply to any information that:

a. Contractor rightfully has in its possession when disclosed to it, free of obligation to the CSU to maintain its confidentiality;
b. Contractor independently develops without access to CSU Protected Data;
c. Is or becomes known to the public other than by breach of this contract;
d. The CSU or its agent releases without restriction; or
e. Contractor rightfully receives from a third party without the obligation of confidentiality.

Any combination of Protected Data disclosed with information not so classified shall not be deemed to be within one of the foregoing exclusions merely because individual portions of such combination are free of any confidentiality obligation or are separately known in the public domain.

Failure by Contractor to comply with any provision of this Section shall constitute a default subject to Paragraph 14 of the CSU General Provisions for Information Technology Acquisitions.

3.0 INFORMATION SECURITY PLAN

3(a) Contractor acknowledges that the CSU is required to comply with information security standards for the protection of Protected Data Information required by law, regulation and regulatory guidance, as well as the CSU's internal security policy for information and systems protection.

Within 30 days of the Effective Date of the Agreement and subject to the review and approval of the CSU, Contractor shall establish, maintain and comply with an information security plan ("Information Security Plan"), which shall contain such elements that the CSU may require after consultation with Contractor. On at least an annual basis, Contractor shall review, update and revise its Information Security Plan. At the CSU's request, use reasonable efforts to accommodate requests by CSU but only to the extent that such requests do not conflict with Contractor's requirements.

Contractor's Information Security Plan shall be designed to:

- Ensure the security, integrity and confidentiality of the CSU Protected Data;
- Protect against any anticipated threats or hazards to the security or integrity of such information;
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to the person that is the subject of such information;
- Protect against unauthorized changes to or use of CSU Protected Data; and
- Comply with all applicable legal and regulatory requirements for data protection.
- Include business continuity and disaster recovery plans.

Contractor's Information Security Plan shall include a written response program addressing the appropriate remedial measures it shall undertake in the event that there is an information security breach.

Contractor shall cause all Subcontractors and other persons and entities whose services are part of the Services which Contractor delivers to the CSU or who hold CSU Protected Data, to implement an information security program and plan substantially equivalent to Contractor's.

The parties expressly agree that Contractor's security procedures shall require that any Protected Level 1 Data transmitted or stored by Contractor only be transmitted or stored in an encrypted form.

In addition, Contractor represents and warrants that in performing the Services, it will comply with all applicable privacy and data protection laws and regulations of the United States including, as applicable, the provisions in the Gramm-Leach-Bliley Act, 15 U.S.C. Section 6801 et seq., the Family Education Rights and Privacy Act ("FERPA"), 20 USC Section 1232(g) et seq., and of any other applicable non-U.S. jurisdiction, including the European Union Directives, and that it will use best efforts, consistent with Federal Trade Commission and other applicable guidance, to protect CSU's Protected Information from identity theft, fraud and unauthorized use.

Failure by Contractor to comply with any provision of this Section shall constitute a default subject to Paragraph 14 of the CSU General Provisions for Information Technology Acquisitions.

3(b) Contractor agrees that it will protect CSU Protected Data according to published information security policy and standards and no less rigorously than it protects its own confidential information but in no case less than reasonable care.

Contractor shall develop, implement, maintain and use appropriate administrative, technical and physical security measures, which may include but not be limited to encryption techniques, to preserve the confidentiality, integrity and availability of all such Protected Data.

In addition, Contractor represents and warrants that in performing the Services, it will comply with all applicable privacy and data protection laws and regulations of the United States including, as applicable, the provisions in the Gramm-Leach-Bliley Act, 15 U.S.C. Section 6801 et seq., the Family Education Rights and Privacy Act ("FERPA"), 20 USC Section 1232(g) et seq., and of any other applicable non-U.S. jurisdiction, including the European Union Directives, and that it will use best efforts, consistent with Federal Trade Commission and other applicable guidance, to protect CSU's Protected Information from identity theft, fraud and unauthorized use.

Failure by Contractor to comply with any provision of this Section shall constitute a default subject to Paragraph 14 of the CSU General Provisions for Information Technology Acquisitions.

4.0 INCIDENT RESPONSE MANAGEMENT

4.1 Notification of a Security Incident.

Contractor shall report, in writing, to the CSU any use or disclosure of CSU Protected Data not authorized by this Agreement or authorized in writing by the CSU, including any reasonable belief that an unauthorized individual has accessed CSU Protected Data. This report shall be made to the CSU's primary contact and its designated information security officer. It shall include details relating to any known or suspected security breach of Contractor's system or facilities which contain CSU Protected Data or any other breach of Protected Data relating to this Agreement. This report shall be made not later than within seventy-two (72) hours after confirmed, if the information was, or is reasonably believed to have been, acquired by an unauthorized person.

4.2 Notification Contents

Contractor's report shall identify:

- The nature of the unauthorized use or disclosure,
- The time and date of incident,
- A description of CSU Protected Data used or disclosed,
- Who made the unauthorized use or received the unauthorized disclosure,
- What Contractor has done or shall do to mitigate any harmful effect of the unauthorized use or disclosure, and
- The corrective action Contractor has taken or shall take to prevent future similar unauthorized use or disclosure.

Contractor shall provide such other information, including a written report, as reasonably requested by the CSU.

4.3 Notification to Parties

Contractor agrees to fully cooperate with the CSU with the preparation and transmittal of any notice, which the CSU may deem appropriate or required by law, to be sent to affected parties regarding the known or suspected security breach, and to be financially responsible for any such notice resulting from Contractor's, its Representatives, Affiliates, or Subcontractors acts or omissions with regard to the data security requirements of this Agreement. Contractor shall take appropriate remedial action with respect to the integrity of its security systems and processes.

5.0 RECORD RETENTION REQUIREMENTS

Contractor shall maintain all records pertaining to the Services provided to the CSU under this Agreement for a period of up to 180 days. Contractor further agrees to provide to the CSU, at its request, a full copy of all such records for the CSU to maintain at a U.S. location which the CSU shall designate. Backup data may not be permanently archived.

6.0 THE CSU RIGHT TO CONDUCT AND/OR REVIEW RISK ASSESSMENTS

A Contractor, with access to the CSU protected data, shall conduct risk assessments and/or audits of its use of CSU protected data at least annually. The Contractor shall provide the CSU with copies of its latest information security risk assessments and/or audits results upon request.

If any assessment and/or audit discloses material variances from the performance requirements set forth in this Agreement or a breach by Contractor of the provisions of this Agreement, Contractor shall be deemed in breach of this Agreement.

7.0 TERMINATING OR EXPIRING THE AGREEMENT – RETURN/DESTROY PROTECTED DATA

Upon the termination or expiration of this Agreement, or at any time upon the request of the CSU, Contractor and its subcontractors shall return all CSU Protected Data (and all copies and derivative works thereof made by or for Contractor). Further, Contractor and all subcontractors shall delete or erase such Protected Data, copies and derivative works thereof, from their computer systems.

The CSU shall have the right to require Contractor to verify, that all CSU Protected Data has been returned, deleted or erased. Contractor agrees to use commercially reasonable efforts to cooperate with the CSU's requests for verification.