CSU FULLERTON AUXILIARY SERVICES CORPORATION (CSUF ASC) POLICY & PROCEDURES **Section: Contracts Agreement A/P 220** **Approved by: CFO, Tariq Marji** 	**Dept:** ASC Business and Financial Services **No: AP 220**
Subject: Information Security Agreements	Date: 4/28/16 Page:

I. PURPOSE:

The purpose of this policy is to provide guidance in developing information security agreements which involve the use of, or provide access to, CSUF ASC confidential information, or resources that require protection, in compliance 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).

II. SCOPE:

This policy applies to all contract agreements involving information security for CSUF ASC administration divisions, commercial services, ASC campus program accounts, grants & contracts, and all other ASC accounts.

III. DEFINITION:

Confidential Information refers to all proprietary information, data, trade secrets, business information, protected information relating to 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 CSUF ASC, CSUF, CSU, its students and employees, and its third-party contractors or licensors who have made confidential or proprietary information available to the CSUF ASC.

IV. SUPPLEMENTAL PROVISIONS FOR INFORMATION SECURITY AGREEMENTS.

The list below contains contract language to be used to develop supplemental provisions for secured information contracts involving the use of CSUF ASC confidential information or resources that require protection.

1.0 ACKNOWLEGEMENT

The acknowledgement requirement ensures that contractor is aware that the data to which they are granted access under the contract is defined as "protected" and subject to laws and regulations.

"Contractor acknowledges that its contract/purchase order with the CSUF ASC may allow the Contractor access to CSUF ASC 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 CSUF ASC Protected Data confidential both during the term of, and after the termination of, the Agreement."

2.0 DISCLOSURE

The disclosure requirement ensures that subcontractors are held to the terms to which they have agreed.

"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 CSUF ASC protected data other than to carry out the purposes of this agreement. Contractor shall not disclose any CSUF ASC 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 approved by the CSUF ASC and provided that:
    i. Use by such affiliates or subcontractors shall be limited to the purpose of this agreement;
    ii. Affiliate or subcontractor is bound by contract and all confidentiality agreements to protect CSUF ASC data from unauthorized access.

If required by a court of competent jurisdiction or an administrative body to disclose Protected Data, Contractor shall notify the CSUF ASC in writing prior to any such disclosure in order to give the CSUF ASC 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 CSUF ASC 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 CSUF ASC 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 CSUF ASC.

3.0 INFORMATION SECURITY PLAN

This section requires the contractor to develop or maintain an information security plan adequate to protect the CSUF ASC data. The CSUF ASC will select one of the two sub-sections to use in their contract. Section 3(a) is to be used for contracts which the CSUF ASC identifies as "high risk" due to the size of the contract, the critical nature of the service or function, and/or the nature of the CSUF ASC Information Assets affected. Section 3(b) is to be used for contracts which the CSUF ASC does not identify as "high risk".

3(a) Contractor acknowledges that the CSUF ASC 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 CSUF ASC'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 CSUF ASC, Contractor shall establish, maintain and comply with an information security plan ("Information Security Plan"), which shall contain such elements that the CSUF ASC may require after consultation with Contractor. On at least an annual basis, Contractor shall review, update and revise its Information Security Plan, subject to the CSUF ASC's review and approval.

Contractor's Information Security Plan shall be designed to:

- Ensure the security, integrity and confidentiality of the CSUF ASC 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, CSUF ASC Protected Data;
- Comply with all applicable CSUF ASC policies, legal, and regulatory requirements for data protection; and
- 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 CSUF ASC, or who hold CSUF ASC 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 Data be transmitted or stored by Contractor only in an encrypted form approved by the CSUF ASC.

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 laws and regulations, including the European Union Directives, and that it will use best efforts, consistent with Federal Trade Commission guidelines, and any other applicable guidance, to protect CSUF ASC's Protected Information from identity theft, fraud and unauthorized use.

3(b) Contractor agrees that it will protect CSUF ASC Protected Data according to published information security policies 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 laws and regulations, including the European Union Directives, and that it will use best efforts, consistent with Federal Trade Commission guidelines, and any other applicable guidance, to protect CSUF ASC's Protected Information from identity theft, fraud and unauthorized use.

4.0 INCIDENT RESPONSE MANAGEMENT

This section requires the contractor to report an information security breach, and defines required reporting contents and timeline.

4.1 Notification of a Security Incident.

Contractor shall report, in writing, to the CSUF ASC any use, or disclosure, of CSUF ASC Protected Data not authorized by this Agreement and not authorized in writing by the CSUF ASC, including any reasonable belief that an unauthorized individual has accessed CSUF ASC Protected Data. This report shall be made to the CSUF ASC'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 CSUF ASC Protected Data, or any other breach of Protected Data relating to this Agreement. This report shall be made not later than twenty-four (24) hours after discovery.

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 CSUF ASC 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 effects 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 CSUF ASC.

4.3 Notification to Parties

Contractor agrees to fully cooperate with the CSUF ASC with the preparation and transmittal of any notice, which the CSUF ASC 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 COMPLIANCE

5.1 PCI DSS Requirements

This section is to ensure that contractor complies with PCI DSS, required if contractor provides a service that involves storage, processing or transmission of payment card data.

Contractor represents and warrants that it shall implement and maintain certification of Payment Card Industry ("PCI") compliance standards regarding data security, and that it shall undergo independent third party quarterly system scans that audit for all known methods hackers use to access private information, in addition to vulnerabilities that would allow malicious software (i.e., viruses and worms) to gain access to or disrupt the network devices. If during the term of the Agreement, Contractor undergoes, or has reason to believe that it will undergo, an adverse change in its certification or compliance status with the PCI DSS standards and/or other material payment card industry standards, it will promptly notify the CSUF ASC of such circumstances.

Contractor agrees to promptly provide current evidence of PCI DSS standards at CSUF ASC's request. The form and substance of such evidence must be reasonably satisfactory to, and must be certified by, an authority recognized by the payment card industry for that purpose.

Contractor shall maintain and protect, in accordance with all applicable laws and PCI regulations, the security of all cardholder data when performing the contracted Services on behalf of the CSUF ASC.

Contractor will use reasonable care and efforts to detect fraudulent credit card activity in connection with credit card transactions processed for the CSUF ASC.

Contractor shall indemnify and hold CSUF ASC harmless from loss or damages resulting from Contractor's failure to maintain PCI compliance standards in accordance with this section.

Contractor shall not be held responsible for any such loss of data if it is shown that the loss occurred as a result of the sole negligence of the CSUF ASC.

5.2 PA-DSS REQUIREMENTS

This section is to ensure that contractor complies with PA-DSS, and is to be used when contractor provides software applications involving the storage, transmission, and processing of credit card data.

Contractor represents and warrants that the software applications it provides for the purpose of processing payments, particularly credit card payments, are developed in accordance with, and are in compliance with, the standards known as Payment Application Data Security Standards (PA-DSS). As verification of this, the Contractor agrees to provide evidence that any such application it provides is certified as complying with these standards and agrees to continue to maintain that certification. The evidence may be provided in the form of the PA-DSS form, if the contractor self-certified, or a copy of the PA-QSA if the Contractor was certified by an external party. If the contractor is unable to provide a copy of the PA-DSS form or the PA-QSA letter, the contractor must provide the CSUF ASC with proof of bonded insurance listing the CSUF ASC as the beneficiary in the case of a security breach.

If during the term of the Agreement, Contractor undergoes, or has reason to believe that it will undergo, an adverse change in its certification or compliance status with the PA-DSS standards and/or other material payment card industry standards, it will promptly notify the CSUF ASC of such circumstances.

Contractor agrees promptly to provide annually, or at the request of the CSUF ASC, current evidence, in form and substance reasonably satisfactory to the CSUF ASC, of compliance with PA-DSS security standards which has been properly certified by an authority recognized by the payment card industry for that purpose.

Contractor shall indemnify and hold CSUF ASC harmless from loss or damages resulting from Contractor's failure to maintain PA-DDS security standards in accordance with this section.

5.3 NACHA REQUIREMENTS

Contractor agrees to assist the CSUF ASC in documenting compliance with NACHA-The Electronic Payment Association provisions.

5.4 Health Insurance Portability and Accountability Act (HIPAA) Requirements

This section is required if Contractor provides goods or services which involves patient health information under HIPAA. Please note that a Business Associate Agreement may be required under this provision.

Contractor shall agree to use and disclose Protected Health Information in compliance with the security standards for the protection of electronic protected health information as per (45 C.F.R. Parts 160 and 164).

6.0 PERSONNEL SECURITY REQUIREMENTS

This section is required to ensure that contractor personnel, affiliates and subcontractors are required to maintain security and privacy of the CSUF ASC information assets.

Any work to be performed in connection with this Agreement by Contractor, its Affiliates or Subcontractors must be performed in the United States, unless the prior written consent of the CSUF ASC is received. Further, CSUF ASC Protected Data may not be transmitted or stored outside the United States without the prior written consent of the CSUF ASC.

Contractor shall require all Representatives, Affiliates and Subcontractors with access to CSUF ASC Protected Data, as a condition of their engagement, to participate in annual security awareness training.

Contractor shall comply, and shall cause its Representatives, Affiliates and Subcontractors to comply, with all personnel, facility, safety and security rules and regulations and other instructions of the CSUF ASC when performing work at a CSU facility, and shall conduct its work at the CSUF ASC facilities in such a manner as to avoid endangering the safety, or interfering with the convenience of, CSUF ASC representatives or customers.

Contractor shall not knowingly permit a Representative, Affiliate, or Subcontractor to have access to the records, data or premises of the CSUF ASC when such Representative, Affiliate or Subcontractor:

(a) has been convicted of a crime;

(b) has engaged in a dishonest act or a breach of trust; or

(b) uses illegal drugs.

Contractor agrees that under no circumstances shall any of Contractor's Representatives, Affiliates or Subcontractors, whether full-time or part-time, connect to any CSUF ASC system or access any CSUF ASC data, for purposes of downloading, extracting, storing or transmitting information through personally owned, rented or borrowed equipment including, but not limited to mobile devices (e.g., laptops, PDAs, cell phones, etc.,)

Contractor represents that it maintains comprehensive hiring policies and procedures which include, among other things, a background check for criminal convictions, and pre-employment drug testing, all to the extent permitted by law. Contractor shall conduct thorough background checks and obtain references for all its Representatives, Affiliates, and Subcontractors who have access to CSUF ASC's protected information.

Any exceptions are at variance with the CSUF ASC policy and must be approved in advance according to CSUF ASC policy guidelines.

7.0 THE CSUF ASC's RIGHT TO CONDUCT AND/OR REVIEW RISK ASSESSMENTS

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

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

This section is to ensure that the contractor returns or adequately disposes of CSUF ASC protected data.

Upon the termination or expiration of this Agreement, or at any time upon the request of the CSUF ASC, Contractor and its subcontractors shall return all CSUF ASC 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 CSUF ASC shall have the right to require Contractor to verify, to CSUF ASC's satisfaction, that all CSUF ASC Protected Data has been returned, deleted or erased. Contractor agrees to fully cooperate with the CSUF ASC's requests for verification.