

# Procurement Policy for Vendors Handling Sensitive Information

**Procurement Policy Title:** CSUB Procurement Department Guidelines Regarding Protection of Sensitive Information Pertaining to Data Processing Activities Conducted by Vendors and Third Parties:

## **Scope:**

This policy pertains to all procurement and contract requests that may result in any contractor subsequently having access to University information via data that is either stored, processed, transmitted, or transferred and or maintained by CSUB or any CSUB Auxiliary organization.

## **Purpose:**

- a. To establish an approach to ensure the security and protection of sensitive information in the University's custody.
- b. The support CSUB's ITIS function to prevent and protect any threats and hazards to the security or integrity of sensitive University information.
- c. To assist in prevention and protection against any unauthorized access to, or use of, sensitive University information, including confidential and personal information.
- d. To help ensure University-wide compliance to applicable laws, regulations, policies and practices.

## **Procurement Department's Role:**

The CSUB Procurement Department will use a process of controls to assist in ensuring that procurement of products that allow access to vendors and other third-parties is done in a prudent and secure manner. These controls shall be as follows:

- a. If it has been determined that a product and/or service being requested for purchase by a University department may present a possible security risk, then the first step by the Procurement Buyer will be to review the product specifications with the AVP of ITSS and the Campus Information Security Officer.
- b. If a review by the AVP of ITSS and the Campus Information Security Officer confirms a possible security risk would result in the purchase of the product, then steps "c" and "d" shall be followed as outlined below:
- c. An addendum, "Questionnaire for Vendors Who Process or Handle CSUB Confidential Data," shall be forwarded to, and completed by the vendor. Subsequently, it shall be signed and returned prior to the purchase of any product that has been deemed to present a possible information risk. (See attached addendum)
- d. An addendum, "Confidentiality and Non-Disclosure Agreement," shall be signed forwarded to, and signed by the vendor, and the University, prior to the purchase of any product that has been deemed to present a possible information

security risk. (See attached addendum)

**Service Provider Requirements:**

The CSUB Procurement Department may engage vendors, third parties, and/or other CSUB entities to provide services on the University's behalf. Also, these service providers may be engaged in the collection, storage or disposal of University information. Therefore, the University shall not enter into a contractual agreement with any provider who cannot maintain appropriate safeguards for its information, especially confidential information.

**Compliance and Consequences of Non-Compliance:**

The unauthorized modification, deletion, or disclosure of confidential and/or personal information included in data files and data systems can compromise the integrity of programs, violate individual privacy rights, and is therefore expressly forbidden. Any vendor and/or contractor that accidentally or intentionally discloses confidential information will be handled accordingly.

Vendors and/or contractors found to be in non-compliance will be required to take specific steps to become compliant within a specified time. To this end, the CSUB Procurement Department shall work directly with the Campus's Information Security Officer to accomplish this goal. If this cannot be accomplished, the contract with the vendor shall be terminated. Vendors that refuse to provide adequate safeguards shall be subsequently deemed as "non-preferred" vendors.

Michael Chavez  
CSUB-Director of Procurement  
661-654-3183  
Fax: 661-654-3144