California State University Northridge

POLICIES & PROCEDURES

Application Service Providers Security Requirements

Policy 500-14
Revision Date: 11/07/2011

INTRODUCTION:

The University can choose to contract with software and services vendors. These arrangements can require the University to send protected data from its systems to those of the vendor. The University must take steps to ensure that these arrangements do not weaken its information security or place its data at risk of unauthorized disclosure. This document describes the information security requirements for vendors who obtain protected data from the University.

DEFINITIONS:

Application Service Providers (ASP's):

An application service provider is any vendor that provides the University with software that will contain University data but is managed and operated in the vendor's data center and is not controlled or secured by the University's Division of Information Technology. This includes third party software and services vendors.

Audit Trail:

The audit trail shall identify all accesses to the source file, success or failure of the access, the completion status of the access (e.g., failed or successful authentication, or user terminated), and the record and field modified.

Protected Data:

Protected data are any information that the University has deemed to be confidential or sensitive in nature and therefore require additional safeguards in its handling and use. This includes information protected by law such as social security number or credit card numbers. Also included is information that the University has decided to treat as protected because its unauthorized disclosure could cause a loss of privacy, damage to reputation, or economic harm. A list of protected data can be found on the IT website.

Information Assets:

Information assets include anything used to process or store information, including (but not limited to) records, files, networks, and databases; and information technology facilities, equipment (including personal computer systems), and software (owned or leased).

University:

This term is used interchangeably to refer to California State University, Northridge (CSUN) and its auxiliary units.

University Official:

This is any person employed by the campus or an auxiliary unit performing administrative or professional duties.

POLICY PURPOSE:

This document establishes the information security requirements that Application Service Providers (ASPs) must follow when providing software or services to the University that involve the transfer or storage of University protected data

on hardware and software maintained by the vendor outside the CSU or CSUN data center. Compliance with this policy is the responsibility of every University official.

POLICY STATEMENT:

The University Application Service Provider policy specifies the minimum standards that a vendor must meet to ensure that it is handling protected data in a manner that complies with relevant laws, Executive Orders, campus policies, and established best practices. This policy applies to all ASPs hosting CSUN protected data for new contracts, existing contracts as they come up for renewal, and contracts when they are amended to include protected data.

Requirements of ASP Sponsoring Organization (College/Department):

Any University department entering into an agreement to use software operated by an ASP or to provide protected data to a vendor who will store it on its own system (outside CSUN) must ensure that the vendor chosen complies with this policy. Departments must obtain the review and approval of the CSUN Information Security Officer (ISO) that the selected vendor is in compliance with the policy before it is permissible for the Purchasing & Contract Administration Department to negotiate an agreement with the ASP. The department wishing to enter into the ASP arrangement must also secure the written approval of the CSUN division that has overall responsibility for the protected data (if they are not one and the same).

The Information Security Officer (ISO) is responsible for working with CSUN departments to inform vendors of the requirements of this policy and for reviewing the evidence of compliance supplied by the vendor.

Requirements of the Application Service Provider (Vendor):

Vendors can comply with this policy in one of two ways. Either they can offer proof that a third party has attested to the soundness of their security practices through a SSAE16 audit or they can demonstrate that they follow the practices outlined in this policy. These methods of compliance are explained in sections 2.1 and 2.2. Depending on the nature of the project, the ISO may request that additional security measures be implemented in addition to the measures stated in this document.

ASPs that do not meet these requirements may not be used for CSUN projects that transfer or store protected data.

SSE16:

A SSAE16 audit expresses an opinion on the fairness of the presentation of the controls, the design of the controls in terms of their ability to meet defined control objectives, and the operational effectiveness of those controls over a defined period, usually a year. A SSAE16 is typically written by a third-party accounting or audit firm and presented to the ASP’s customers to comply with their own audit functions.

Alternatives to a SSAE16:

1. Payment Card Industry (PCI) Security Standard for Credit Card Processing Only:

    a. The Payment Card Industry, including MasterCard and Visa, require banks, online merchants and Member Service Providers (MSP's) to protect cardholder information by adhering to a set of security standards. The PCI security standard includes MasterCard's Site Data Protection (SDP) program and Visa's Cardholder Information Security Program (CISP).

    b. PCI certification is required for all ASPs that handle credit card data.

CSUN Review of Control:

1. The ASP must provide documentation of the controls for the physical and logical security of the hosted application's infrastructure including network equipment, operating systems, applications, etc. and the maintenance and currency of those controls.
2. The ASP must provide documentation of those users or groups from its organization that will have access to CSUN data, including documentation of the process for obtaining that access and any password controls.
3. The ASP must provide a documented Incident Response Plan, clearly illustrating the steps it takes when a security issue is identified.
4. The ASP must provide a documented Business Continuity Plan.
5. Access to CSUN data must be encrypted using strong encryption either the channel that transmits the data (SSL website or VPN) or the data itself must be stored on an encrypted device.
6. If it provides a custom-built application, the ASP should provide documentation of its security Quality Assurance testing process for the application for example, testing of authentication, authorization, and accounting functions, as well as any other activity designed to validate the security architecture.
7. The vendor must provide a copy of their PCI certificate where cardholder data is transacted, used or stored.

APPLICABILITY AND AREAS OF RESPONSIBILITY:

1. The Information Security Officer (ISO) is responsible for reviewing this policy and updating it on a periodic basis.
2. University officials are responsible for obtaining permission to host CSUN data on the ASP from the application owners, working with the ISO to review the security practices of the ASP, and working with Purchasing & Contract Administration to ensure the ASP agreement is governed by terms and conditions acceptable to the University.
3. The ISO is responsible for contacting the ASP if there is a security issue and disabling the application if deemed necessary.

RESOURCES AND REFERENCE MATERIALS:

Policy 500-8040 Managing Third Parties

Policy 500-8070 Information Systems Acquisition, Development and Maintenance

FURTHER INFORMATION:

Vice President for Information Technology and CIO

APPROVED BY THE PRESIDENT