What is SafeConnect?

A tool that helps ensure that computers connected to the University's Wireless Network meet minimum security standards. Using SafeConnect will help ensure that your personal or University issued device and our network based resources are protected from the effects of malicious software.
What does SafeConnect do?

• Answers Yes/No Questions regarding security software Installation and configuration.
  – Antivirus software Installed and Running?
  – Antivirus Definitions up to date?
  – Operating System Updates set to at least notify?

• SafeConnect does not monitor your activity beyond these basic yes/no questions.
Will I Be Affected?

- Currently required for all students
- University Staff, including Auxiliary Staff will be implemented rollout beings in November
- University Faculty will be implemented in the Spring
Will My Device be Affected?

- Only devices connected to the Wireless Network or “Open” Jacks in public areas are affected.
- Devices running Windows and Mac OSX.
- Ipods, Iphones, Androids, Linux based systems are not affected at this time.
What Will I See?

SafeConnect: Anti-Virus Installation

**Requirement:** SafeConnect requires that PC users have anti-virus software installed and running.

*Your system does not appear to have a SafeConnect recognized anti-virus program installed.*

**Solution:** Visit the following link for a complete list of SafeConnect recognized anti-virus software and instructions for downloading a free anti-virus program.

**WARNING:** If you choose not to install an approved anti-virus software product, your network access will eventually become limited to SafeConnect related resources such as our main SafeConnect informational page, the Software Download page, and other pages where you can download SafeConnect recognized anti-virus solutions.
Where Can I Get More Information?

• Go to www.csus.edu/safeconnect
  – Information on how to prepare in advance
  – List of SafeConnect recognized antivirus software
  – Instructions on how to configure your Operating System to check for updates.
  – Where to get help if you are having issues with SafeConnect
Change in Paper Acquisition & Distribution for the University

- Moving to consistent university approach to paper management
  - “greener” 30% recycled paper
  - Truckload purchases at lower rate
  - $18-25K university savings per year

- Paper stored centrally & delivered weekly
- Photocopy paper will now be separate, per copy cost will be lower as a result
Payment Card Industry (PCI) Compliance on Credit Card Transactions

Information Security Office
(916) 278-1999
iso@csus.edu
Overview

Payment Card Industry Data Security Standard
PCI DSS

Reference: www.pcisecuritystandards.org

Standard

Applies to:
- Merchants (Those who take credit cards for payment)
- Service Providers (Third-party vendor, gateways)
- Systems (Hardware, software)

That:
- Stores cardholder data
- *Transmits* cardholder data
- Processes cardholder data

Applies to:
- Electronic Transactions
- Paper Transactions
Why?

• Policy Requirement
  – ADM-0117
    • Establishes the requirement for the university and its auxiliaries to comply with PCI DSS

• Supplemental Policy
  – 8000.200 Information Security – Introduction and Scope
  – 8035.300 Information Security Awareness and Training
  – 8045.100 Security of Servers and Network Attached Devices
  – 8045.200 Protection Against Malicious Software
  – 8050.0 Configuration Management
CREDIT CARD ACCEPTANCE

On November 1999, the Gramm-Leach-Bliley Act was signed into law. This legislation established the requirement for protecting a customer’s non-public information obtained during the course of business, including credit card information. As a result, the Payment Card Industry (PCI) Data Security Standard was developed by the major credit card companies. Businesses accepting credit cards must comply with this standard or risk losing the right to process credit card payments and be audited and/or fined. As California State University, Sacramento and its auxiliaries do accept credit cards for payment, the university and its auxiliaries must comply with the PCI Data Security Standard.

Any department at Sacramento State wanting to accept credit cards for payment of goods or services must obtain approval prior to doing so and must agree to meet the requirements of the PCI Data Security Standard. This policy governs the process by which university departments request approval to accept credit card payments deposited with the University.

Responsibilities

The University Chief Financial Officer and his/her designee, the University Bursar, are responsible for the process and enforcement of this policy.

University auxiliaries accepting credit cards for payments are responsible for complying with the PCI Data Security Standard.

Scope

This policy applies to any university department or auxiliary wanting to accept credit cards for goods or services provided. University departments may request authorization to accept credit cards via the Procedures hyperlink below. Auxiliary organizations of the University may establish their own procedures, so long as they remain in compliance with the PCI Data Security Standard.

Procedures

Process to Request Authorization to Accept Credit Cards for Payment

If payments are to be deposited with an auxiliary, contact that auxiliary for authorization to accept credit card payments.

Approved by Alexander Gonzalez, President
October 2, 2008
Why! Lost Credit Card Data

• Charged to your department!

• Failure to comply with all PCI regulation could result in loss of the ability to accept credit cards, forced service outages in case of a breach, and steep fines. Fines can be as high as $5,000 per card per day in case of a breach.

• Fines levied by card associations to make notifications to all card holders and replace cards.
• Costs of notifying customers of incident.
• Forensic Investigation Costs.
  — Required by card associations
  — Must used approved firm (QSA)
  — Cost approximately $50,000 (recent CSUSD breach - $15,000)
• Cost associated with discontinuing accepting cards.
• Cost of an annual on-site security audit.
  — Once a breach has occurred, elevated to a Level 1 merchant.
  — Cost approximately $15,000 - $20,000.
What Does This Mean?

6 Sections of PCI Compliance

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy
More Information?

Information Security Office:
http://www.csus.edu/irt/is/pci/presentations/index.html

Payment Card Industry:
http://www.pcisecuritystandards.org