California State University
Information Security Management

Felecia Vlahos
Information Security Officer, San Diego State University
Cheryl Washington
Interim Senior Director, System-wide Information Security Management
Agenda

• CSU Information Security Program
• CSU Information Security Policy Project
• CSU Information Security Awareness Project
• CSU Red Flags Program
• Information Security Advisory Committee (ISAC) – PCI Project
• Questions
Introduction:
CSU Information Security Program

An organized effort across all areas of the University to provide appropriate levels of *confidentiality, integrity, availability*, and *accountability* for *information assets* regardless of format or representation.
DEFINITION: *Information Assets*

Information systems, data, and network resources to include automated files and databases.
CSU Information Security Program Goals

- Support the CSU mission

- Create a secure environment & protect information assets - develop and promote administrative, physical and technical safeguards

- Integrate security into the culture of the CSU

- Collaborate with academic and operational units to ensure confidentiality, integrity, and availability of CSU information assets

- Promote Security Awareness

- Develop an information security risk management program

- Ensuring compliance with applicable federal, state, local and international regulatory/legal requirements related to security and privacy

- Develop programs that are *flexible and adaptable*
System-wide Security Program Benefits

- **Supports Compliance Requirements**
  - demands for personal privacy and data protection continue to increase
- **Demonstrates Leadership Commitment**
  - a key to any successful program
- **Promotes Broad Discussion and Awareness of Information Security**
  - increased awareness – consistently the most effective means for reducing security incidents and data exposure
- **Promotes Consistency**
  - common framework and expectations
- **Establishes a Benchmark**
  - eliminates guessing about what needs to be done
- **Provides Evidence of Due Diligence**
  - important in cases of litigation
The CSU’s Perspective on Security

All members of the CSU community are responsible for protecting information assets owned, leased or entrusted to the CSU.
Information Security Program – Touches Everyone

Administration and Staff
- A sustainable program is established and a bar is set
- Implementation freedom preserved
- Efficiencies gained from eliminating guesswork

Students
- Privacy acknowledged
- Protections provided
- Rules of the Road identified
- Consistency in expectations

Faculty
- Academic Freedom acknowledged
- Protection of research enhanced
- Not set in stone; will continue to evolve
  - Consistency in expectations

Visitors
- Still has access to information
  - Few noticeable impacts
- Privacy more clearly addressed

Auxiliaries & Business Associates
- Part of the integrated approach
- Responsibilities identified
Systemwide Information Security Policy and Standards Project
Policy Project Goals

• Develop system-wide information security policies and standards

• Instill more secure working habits for individuals and entities that deal with CSU information assets

• Position the CSU to be in compliance with privacy and security laws and regulations

• Expand use of risk assessments

• Document CSU information security and privacy protection practices

• Develop an information security governance structure
Project Milestones

September 2007 – Project Begins
Review Cycle 1 – Winter 2008
Review Cycle 2 – Spring 2008
Review Cycle 3 – Fall 2008

Target Completion Date – Summer/Fall 2009
<table>
<thead>
<tr>
<th>Topics Addressed by Policy and Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Management</td>
</tr>
<tr>
<td>Establishing an Information Security Program</td>
</tr>
<tr>
<td>Organizing Information Security</td>
</tr>
<tr>
<td>Information Security Risk Management</td>
</tr>
<tr>
<td>Responsible Use</td>
</tr>
<tr>
<td>Personnel Security</td>
</tr>
<tr>
<td>Privacy</td>
</tr>
<tr>
<td>Security Awareness and Training</td>
</tr>
<tr>
<td>Managing Third Party Service Providers</td>
</tr>
<tr>
<td>Information Technology Security</td>
</tr>
<tr>
<td>Configuration Management and Change Control</td>
</tr>
<tr>
<td>Access Control</td>
</tr>
<tr>
<td>Asset Management</td>
</tr>
<tr>
<td>Information Systems Acquisition, Development and Maintenance</td>
</tr>
<tr>
<td>Physical Security</td>
</tr>
<tr>
<td>Incident Management</td>
</tr>
<tr>
<td>Business Continuity and Disaster Recovery</td>
</tr>
<tr>
<td>Legal and Regulatory Compliance</td>
</tr>
</tbody>
</table>
## Key Policy Concepts

<table>
<thead>
<tr>
<th><strong>Risk Management</strong></th>
<th>Campuses must conduct periodic risk assessments when security requirements change or when significant changes occur in the campus environment.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Awareness Training</strong></td>
<td>Campuses must ensure that system administrators and managers are provided with sufficient ongoing training to stay current with the best practices and technology.</td>
</tr>
<tr>
<td><strong>Information Technology Security</strong></td>
<td>Need procedures in place to effectively detect, prevent, and report malicious software.</td>
</tr>
<tr>
<td></td>
<td>Networks (wired and wireless) need to be designed and segmented based on risk, data, and access.</td>
</tr>
<tr>
<td></td>
<td>Campuses must prevent unauthorized remote access to critical information systems or protected data.</td>
</tr>
</tbody>
</table>
# Key Policy Concepts (more…)

| **Managing Third Party Service Providers** | Before third parties are granted access, a basic risk assessment must be performed.  

Contract terms and conditions must include appropriate information security safeguards. |
| **Configuration & Change Management** | Must maintain a program designed to ensure that operating systems and applications are routinely updated to correct flaws and close vulnerabilities.  

Must review changes to critical information systems, protected data, and network resources. |
| **Access Control** | Managers and data stewards define and approve access.  

A documented process is used to approve additions, changes, and terminations of access rights.  

User privileges must be regularly reviewed. |
## Key Policy Concepts (more…)

| **Asset Management** | All information assets must be classified according to the CSU’s data classification standard.  
| | Media and hardware must be securely sanitized or disposed of when no longer needed. |
| **Incident Management** | Each campus must have a security incident response team (SIRT) and an incident response plan.  
| | Contracts should compel third parties to report security incidents involving campus information. |
| **Business Continuity & Disaster Recovery** | Continuation essential functions and operations following a catastrophic event.  
| | Must be in compliance with the CSU Executive Order 1014. |
Policy Management and Updates

• This policy will be updated to reflect changes in the CSU's academic, administrative, or technical environments, or applicable state, federal, or international laws and regulations.

• The CSU's Senior Director for Information Security Management oversee an annual review of this policy.

Regular opportunity for updates, modifications, and adjustments!
Systemwide Information Security Awareness Training Program
Promoting Security Awareness

Numerous security incidents at institutions of higher learning across the nation, including the CSU, illustrate that the human factor is both a weak link in the security continuum and an important factor in the success of an information security program.

The California State University (CSU) recognizes that an information security awareness program is an important component in the overall strategy to protect the CSU’s information assets.

The CSU’s information security awareness program will inform individuals, who come into contact with CSU assets, of the risks associated with their activities and of their responsibilities to comply with CSU policies and procedures.
High Level Topics for 2008/09

Introduction to Information Security
CSU Policy & User Guidelines
Responsibilities of Employees
Viruses, Malware, and Spyware
Account and Password Security
Information retention and destruction
E-mail Security
Security of Mobile Devices
Security of Third parties
Physical Security
Practicing Safe web surfing
Social Engineering
CSU Security Awareness Course

The hosted web-based environment will be managed and administered by the contractor, WorkPlace Answers.

The intended audience includes:

• CSU faculty & staff
• Auxiliary employees
• Other members of the staff (e.g., volunteers, student employees)
• Third-party service providers (e.g., vendors & contractors) hired by the CSU
Course Specifications

The course is designed around a university setting appropriately reflecting the CSU identity.

The average length of the system wide course is approximately 30-40 minutes.

The course meets all applicable Section 508 Standards, Subpart B 1194.21 & 1194.22.

At the end of the course, the trainee are presented with the CSU Access and Compliance form. **The trainee will be required to read and digitally sign the form acknowledging they understand their responsibilities in adhering to CSU information security policies and standards.**

The hosted online environment provides account management and reporting services.
Account Management

The training environment includes the capability to track the progress of the trainees. Campuses will have the ability to identify individuals who:

• Need to complete the course
• Have attempted but have not completed the course
• Have completed the course

The web-based environment will send automated e-mail reminders to trainees who need to be trained or have started but have not completed the security awareness-training course.
Reporting

Sample Reports include:

- Course title broken down by year, campus, and department that can distributed easily to each campus administrator.

- A listing by campus, broken down by department and trainee of percent course completion.

- An account reconciliation report listing the number of trainee/user profiles created.

All reports can be exportable to Excel and CVS formats for importing into local campus tracking systems.

Each campus will be given access to their reports.
Systemwide Red Flags Program
Introduction – Red Flag program

• In 2003, the U.S. Congress enacted the Fair and Accurate Credit Transaction Act of 2003 (FACT Act) which required the Federal Trade Commission (FTC) to issue regulations requiring “creditors” to adopt policies and procedures to prevent identify theft.

• In 2007, the Federal Trade Commission (FTC) issued a regulation known as the Red Flag Rule. The rule requires “financial institutions” and “creditors” holding “covered accounts” to develop and implement a written identity theft prevention program designed to identify, detect and respond to “Red Flags.”

• Under the Red Flag Rules, every financial institution and creditor that holds any consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, is required to establish a documented Identity Theft Prevention program that provides for the identification, detection, and response to patterns, practices, or specific activities – known as “red flags” – that could indicate identity theft. Examples of red flag activities include unusual account activity, address discrepancies, fraud alerts on a constituent’s consumer report provided by a Credit Reporting Agency, or the attempted use of suspicious account applications.

• The CSU Office of General Counsel has determined the Red Flag Rules likely apply to the CSU.
Definitions

**Account** means a continuing relationship established by a person with a campus to obtain a product or service for personal, family, household or business purposes. Account includes:

- An extension of credit, such as the purchase of property or services involving a deferred payment; and
- A deposit account

A **creditor** is a person or entity that regularly extends, renews, or continues credit and any person or entity that regularly arranges for the extension, renewal, or continuation of credit. Examples of activities that indicate a college or university is a “creditor” are:

- Participate in the Federal Perkins Loan program;
- Participate as a school lender in the Federal Family Education Loan Program;
- Offer institutional loans to students, faculty or staff; or
- Offer a plan for payment of tuition or fees throughout the semester, rather than requiring full payment at the beginning of the semester.

A **covered account** is a consumer account designed to permit multiple payments or transactions. These are accounts where payments are deferred and made by a borrower periodically over time such as a tuition or fee installment payment plan.

**Identity Theft** is the act of fraud committed using the identifying information of another person.

A **red flag** is a pattern, practice or specific activity that indicates the possible existence of identity theft.
Program Requirements

Each campus that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

The Program must include reasonable policies and procedures to:

- **Identify** covered accounts;
- **Identify** relevant Red Flags for the covered accounts that the campus offers or maintains, and incorporate those Red Flags into its Program;
- **Detect** Red Flags that have been incorporated into the Program of the campus;
- **Respond** appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
CSU Compliance Efforts

- The systemwide information security management office will develop a systemwide Red Flag Program which will be submitted to the Board of Trustees for approval.

- The systemwide information security office will provide campuses with implementation guidelines to help campuses develop their Red Flag Programs.

- In designing its Program, a campus may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the campus from identity theft.
Campus Program Administration

Each campus that is required to implement a Program must provide for the continued administration of the Program and comply with the following:

• Program oversight responsibilities include:
  • Assign specific responsibilities for the Program’s implementation;
  • Review reports prepared by staff regarding compliance with the campus Program; and
  • Approve material changes to the Program as necessary to address changing identity theft risks.

• Train staff, as necessary, to effectively implement the Program; and

• Exercise appropriate and effective oversight of service provider arrangements.

• Ensure the Program (including the Red Flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the campus from identity theft.
Information Security Advisory Committee (ISAC) Initiatives 2008/09
ISAC Goals -

Focus on CSU-Wide efforts

Develop specific implementation strategies and models for CSU-Wide policies and standards

Create models that can be adapted for use on many campuses
Project: Payment Card Industry (PCI) Compliance

• This year an ISAC task force will address
  • Sharing and collaboration of campus PCI standards and programs
  • Vendor and software recommendations for payment processing and PCI assessment outsourcing
  • PCI-specific awareness and training for campuses
  • Standards and language for procurement of PCI software and services.
• This task force will develop a framework for PCI compliance guideline for the CSU campuses.
Questions?