

Information Security

Activities and Updates

Teresa Macklin

Information Security Officer

Major Activities

- Information Security Audits
 - 10 campuses last year
 - Both practices and vulnerabilities being tested
- CSU-Wide Info Security Policies & Standards
 - Final comments collected from campus
 - Expected distribution by Exec Order Spr 09
 - Affects campus business practices

Policy & Standards Development

The CSU is implementing a set of CSU-wide policies and standards

- Baseline policy and standard for a broad set of information security elements
- Scope: All campus plus auxiliary organizations



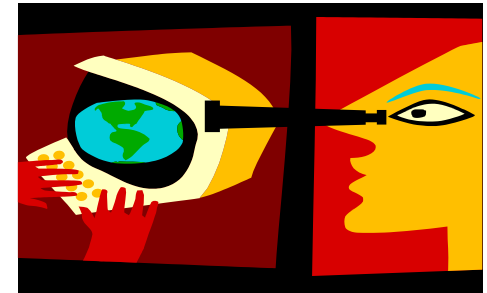
Policy & Standards Scope

- Strict identification, handling practices and tracking of “protected” data.
- More process around accessing an employee’s files and email when they leave campus employment
- Employees will have to receive security awareness training before being granted a user account.
- Structured reviews of user access lists for department shares and similar.
- More use of encryption to store and transmit protected data

Security Awareness

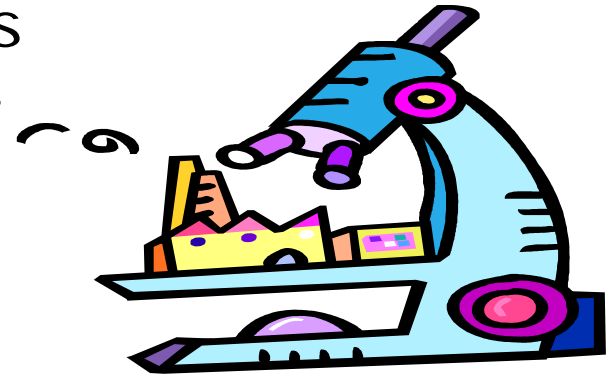
CSU-Wide program

- Online training similar to sexual harassment training
- Customized by campus
- Provides baseline security awareness
- Participation is a requirement
- Scope: Employees
- Schedule: Spring 09



Information Security Audit

- CSU Auditors scheduled 10 audits in 2008, likely the remaining campuses in 2009
- Initial audit document request is for 90 document areas
- Requires participation from IITS, HR, Materials Management, Procurement, Risk Management
- Payment Card Industry standards
 - Requires frequent assessment
 - Affects any use of payment cards via campus network or using campus equipment



Changes To Campus Practices

- Classification of the data your organization uses.
- Periodic review of department access lists and practices by ISO
- IT security assessments required for some organizations
- Many former “practices” documented as procedure
- ...

Example details

- Data Classification (Standard 15)
 - Depts will be required to identify applications and systems which access or store protected data.
 - Some data may not be sent unless encrypted
 - Annual reviews of security permissions & practices.
 - Approval required to create “shadow” systems.
- Mobile Devices (Standards 12.2 & 12.3)
 - No protected data store on mobile devices unless encrypted/protected. (Laptops, data phones, memory sticks)
- Info Security Awareness (Standard 10)
 - Required and tracked for every employee
- Procurement/Contracts (Standards 6, 11)
 - Risk management process prior to procuring new systems
 - Third party contract changes
- Personnel (Standard 8)
 - Exit process must include securing data and access.

Your Action Items

- Respond to specific document requests by ISO
- Develop new internal processes to meet new requirements when policy/standards are published
- Engage in development process for campus implementation
- Establish responsibility for annual reports and internal security audits (with ISO)