

 The California State University
WORKING FOR THE CALIFORNIA DREAM

**Selected pages from
 The CSU System-wide Policy Project
 Communications Materials**

12 November, 2008 –
 Academic Senate Executive
 Committee

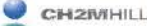
© 2008 CH2MHILL, Inc.
 Data contained on this sheet is proprietary use or
 disclosure restricted. Page 1



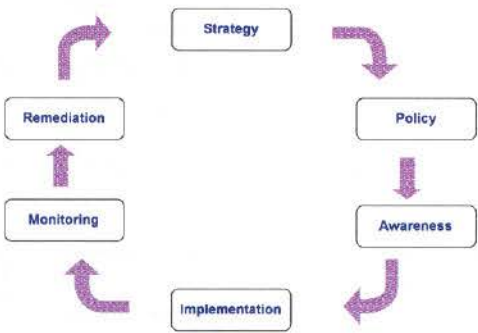
What is an Information Security Program?

An organized effort across all domains (physical, logical, procedural) to provide appropriate levels of confidentiality, integrity, availability, and accountability for information regardless of format or representation.

© 2008 CH2MHILL, Inc.
 Data contained on this sheet is proprietary use or
 disclosure restricted. Page 2



Information Security Program Cycle




```

    graph TD
      Strategy --> Policy
      Policy --> Awareness
      Awareness --> Implementation
      Implementation --> Monitoring
      Monitoring --> Remediation
      Remediation --> Strategy
  
```

Stepping Through the InfoSec Program: ISACA

© 2008 CH2MHILL, Inc.
 Data contained on this sheet is proprietary use or
 disclosure restricted. Page 2



The Elements

Strategy

- Objectives – what needs to be protected and why
- Roles and Responsibilities
- Structure – centralized or decentralized


Policy

- Policy – high level statements
- Standards – specific guidance
- Procedures – step by step instructions
- Guidelines – best practice recommendations

Awareness

- Orientations
- Training
- Reminders
- Forums, Working Groups, Wikis

© 2008 CH2MHILL, Inc.
 Data contained on this sheet is proprietary use or
 disclosure restricted. Page 3



The Elements (cont)

Implementation

- **Administrative Controls** – procedures and processes
- **Technical Controls** – firewalls, permissions, intrusion detection, etc.
- **Physical Controls** – barriers limiting contact with protected resources

Monitoring

- **Asset Management**
- **Change Control**
- **Network Monitoring**
- **Self Assessments**

Remediation

- **Incident Response**
- **Risk Management**
- **Self Assessments**
- **Compensating Controls**

© 2009 CH2MHILL, Inc.
Data subject to the third party privacy and
disclosure policies of Page 7



Information Security Program – Touches Everyone

Visitors

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

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

CSU The California State University
WORKING FOR CALIFORNIA

Administration and Staff

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

Auxiliaries

- Part of the integrated approach
- Responsibilities identified

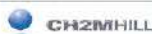
© 2009 CH2MHILL, Inc.
Data subject to the third party privacy and
disclosure policies of Page 7



Proposed Changes To Campus Practices

- All IT-related audit submissions approved by ISO
- Periodic review of department access lists and practices by ISO
- IT security assessments required for some organizations
- Many former "practices" documented as procedure
- IT security governance structure strengthened

© 2009 CH2MHILL, Inc.
Data subject to the third party privacy and
disclosure policies of Page 7



Student Affairs Impact - Examples

- **Data Classification (Standard 15)**
 - ▶ Student Affairs 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.

© 2009 CH2MHILL, Inc.
Data subject to the third party privacy and
disclosure policies of Page 8



Project Background

Timeline

- ▶ September 2007 – Project Begins
- ▶ October 2008 – Draft Policy and Standards Produced
- ▶ Fall 2008 – Spring 2009 Initiate Executive Order Coordination

From the RFP

- ▶ The project proposal is to develop viable system-wide information security policies and standards for the CSU System.
- ▶ This information security policy project will
 - ▶ provide means of furthering information security education.
 - ▶ identify secure working habits for individuals and entities that deal with CSU information assets.
 - ▶ position the University to be in compliance with privacy and security regulations.

Deliverables

- ▶ System-Wide Security Policies
- ▶ System-Wide Security Standards
- ▶ Communication Materials
- ▶ Sample Implementation Strategies

© 2008 CH2M HILL, Inc.
Data contained on this sheet is proprietary and its disclosure is prohibited. Page 11



Policy Objectives

- The CSU is committed to:
 - ▶ the ideals of academic freedom and freedom of expression.
 - ▶ protecting the confidentiality, integrity, and availability of information assets entrusted to the University.

A delicate balancing act.



Policy: A policy is a broad statement of principles that presents management's position for a defined subject.

© 2008 CH2M HILL, Inc.
Data contained on this sheet is proprietary and its disclosure is prohibited. Page 12



Standards and Samples

Standard: A standard provides more specific guidance on a particular topic. These have been written as standalone documents so that they can be more easily incorporated into legal agreements where third parties are providing services.

Sample (Remote Access)

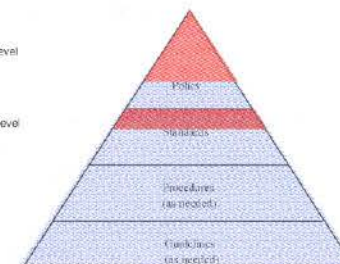
- **Policy** – Campuses must develop procedures that prevent unauthorized remote access to critical information systems or protected data, while ensuring that authorized users have appropriate remote access.
- **Standard** – All remote access to non-public campus information systems, data, and network resources must be authenticated and authorized.

© 2008 CH2M HILL, Inc.
Data contained on this sheet is proprietary and its disclosure is prohibited. Page 11



Security Program Components

- Produced at the System Level
- Produced at the Campus Level



© 2008 CH2M HILL, Inc.
Data contained on this sheet is proprietary and its disclosure is prohibited. Page 12



Topics Addressed by Policy and Standards

- Information Security Roles and Responsibilities
- Risk Management
- Responsible Use
- Personnel Security
- Privacy
- Security Awareness and Training
- Third Party Services Security
- Information Technology Security
- Configuration Management and Change Control
- Access Control
- Asset Management
- Management of Information Systems
- Information Security Incident Management
- Physical Security
- Business Continuity and Disaster Recovery
- Legal and Regulatory Compliance



©2014 CH2M HILL, Inc.
Data contained on this slide is proprietary and/or
otherwise confidential. Page 11



Information Security Roles and Responsibilities

- **Key Policy Concepts** – Everyone (executives, managers, faculty, students, and staff) is responsible for information security including:
 - ▶ the privacy of personally identifiable information (PII).
 - ▶ the integrity of data stored.
 - ▶ the maintenance of applications installed on CSU information systems.
 - ▶ the availability of information.
 - ▶ compliance with applicable local, state, federal, and international laws and regulations, including intellectual property and copyright.
- **Key Standards**
 - ▶ Campus President – establishes campus program
 - ▶ Campus Chief Information Officer
 - ▶ Information Security Officer

©2014 CH2M HILL, Inc.
Data contained on this slide is proprietary and/or
otherwise confidential. Page 11



Possible Campus Rollout Activities

- Respond to specific document requests by ISO
- Develop new internal processes to meet new requirements
- Engage in development process for implementing new policies & standards
- Establish division responsibility for annual reports and internal security audits (with ISO)

©2014 CH2M HILL, Inc.
Data contained on this slide is proprietary and/or
otherwise confidential. Page 11



Sources for Additional Information

- **Campus CIO**
 - ▶ Wayne Veres
 - ▶ veres@csusm.edu
 - ▶ 760-750-4785
- **Campus ISO**
 - ▶ Teresa Macklin
 - ▶ macklin@csusm.edu
 - ▶ 760-750-4787
- **Senior Director for Information Security Management, Chancellor's Office**
 - ▶ Cheryl Washington
 - ▶ cwashington@calstate.edu
 - ▶ 562-951-4190

©2014 CH2M HILL, Inc.
Data contained on this slide is proprietary and/or
otherwise confidential. Page 11



**COAS Budget Reduction
FY 08 to FY 09**

FY 08 Total Need (P+F)	19,388,056	
7.5% proposed reduction	<u>1,454,104</u>	
Projected Budget based on 7.5% reduction	17,933,952	
Student fees allocated to COAS (June)	600,000	
Additional allocation per Haynes/Cutrer (Sept)	<u>135,000</u>	
	18,668,952	<i>(centrally funded salary increases of @ \$500,00 added to this figure for final budget figure of \$19,158,945)</i>
Difference between 08 and 09 (3.7%)	719,104	

Base Budget Review - Department Detail

Fiscal Year 2008/09

Subdivision (College/Unit Name):	Department ID:	Department ID Description:
---	-----------------------	-----------------------------------

A. Salaries and Wages															
<i>PS CF String</i>						<i>Employee Name</i>	<i>Job Classification</i>	<i>Title</i>	<i>FTE</i>	<i>Perm Salary PBB</i>	<i>Perm Benefit Contribution PBB</i>	<i>Fiscal Salary FYB</i>	<i>Fiscal Benefit Contribution FYB</i>	<i>Fiscal Salary Savings FSS</i>	<i>Comments</i>
<i>Acct</i>	<i>Fund</i>	<i>Dept</i>	<i>Pgr</i>	<i>Class</i>	<i>Proj</i>										
Totals									0.0	0	0	0	0	0	

B. Operating Expenses															
<i>PS CF String</i>						<i>Description</i>	<i>FTE</i>	<i>Perm OE&E PBB</i>	<i>Fiscal OE&E FYB</i>	<i>07/08 Actuals</i>	<i>06/07 Actuals</i>	<i>Comments</i>			
<i>Acct</i>	<i>Fund</i>	<i>Dept</i>	<i>Pgr</i>	<i>Class</i>	<i>Proj</i>										
Totals							0.0	0	0	0	0				

C. Funding Sources Available for Offsets to Operational Expenses Listed Above (e.g., Foundation Reimbursements, Chargebacks, Cost Recovery, Transfers In, etc.)															
<i>PS CF String</i>						<i>Funding Source</i>	<i>Fiscal Offset FOF</i>	<i>Purpose</i>	<i>Comments</i>						
<i>Acct</i>	<i>Fund</i>	<i>Dept</i>	<i>Pgr</i>	<i>Class</i>	<i>Proj</i>										
Totals							0								