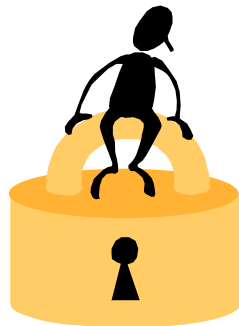


Information Security Annual Report

FY 2006/07



November 2007

TABLE OF CONTENTS

I. INTRODUCTION 1

II. ACTIVITIES FOR THE FISCAL YEAR 2006/07 1

A. INCREASE SECURITY OF THE CAMPUS WIRELESS NETWORK 1

B. USER AUTHENTICATION 1

C. CREATE INVENTORY AND DOCUMENT EXISTING “SHADOW” DATA SYSTEMS..... 2

D. INFORMATION SECURITY FORUMS..... 2

E. INFORMATION DISPOSITION 2

F. CSU INFORMATION SECURITY OFFICERS 3

G. CSU POLICY DEVELOPMENT..... 3

H. AWARENESS TRAINING DEVELOPMENT..... 3

I. CMS PEOPLESOFT STUDENT ADMINISTRATION SYSTEM IMPLEMENTATION 4

J. PARTICIPATE IN THE SYSTEM-WIDE SECURITY PLAN PROJECT 4

K. SOCIAL SECURITY INVENTORY 4

III. GOALS FOR FY 2007/08 5

A. POLICY/STANDARDS DEVELOPMENT 5

B. INFORMATION SECURITY FORUMS..... 5

C. BORDER FIREWALL UPGRADE..... 5

D. SOCIAL SECURITY INVENTORY 5

E. UPDATING INFORMATION SECURITY WEBSITE..... 5

F. AWARENESS TRAINING DEVELOPMENT..... 5

G. INFORMATION DISPOSITION 5

H. FINDING SSNS 5

I. INFORMATION SECURITY STRATEGIC PLAN 6

J. DEVELOPMENT OF STANDARDS FOR TECHNICAL STAFF..... 6

I. Introduction

FY 2006/07 has been an active time for information security. Activities were dominated by the Unisys Assessment which has provided strategic direction guidance. Other activities, such as the development of awareness training and information disposition, required substantial attention with results to be realized in FY 2007/08. Overall, awareness of information security on campus continues to build and the information security program continues to receive support by both management as well as members of the campus community.

Section II of this report summarizes activities that occurred during the past fiscal year (FY 2006/07) to improve the security of University information. Section III briefly describes projects that have been identified to be undertaken in FY 2007/08 that will support continuation of our efforts to secure and protect university data.

II. Activities for the Fiscal Year 2006/07

A. Increase Security of the Campus Wireless Network

For further information contact: Johanna Madjedi

Prior to Fall 2006, wireless users on campus were required to register the Ethernet address of their wireless device. While this method restricted use to registered devices and an associated owner at the time of registration, information about what user was actually using the network was not available. During Fall quarter 2006, the campus implemented username and password authentication for wireless access on campus. Authentication takes place using the same username/password used for access to other campus systems. In addition to access via username/password, the technology implemented allows for guest access and the ability to remove or restrict access in response to any violations or performance issues relating to a particular user.

B. User Authentication

For further information contact: Ryan Matteson or Theresa May

Reference: <http://my.calpoly.edu/>

<http://polydata.calpoly.edu/requests/index.html>

Authentication of users continued to be a focus for security efforts this year. Use of my.calpoly.edu centralized authentication services tripled this year, to over twenty million requests between June 2006 and July 2007. The number of users has also increased in this period to over 57,000 including applicants, students, faculty, and staff. Standardization on this centralized solution continues to reduce the likelihood of compromise and unauthorized access by providing a single logical point of control and audit.

Additional services have been integrated with my.calpoly.edu, including PeopleSoft Student Administration and CashNet for web-based payments. This brings the total number of integrated services to over twenty. An upgrade to the web authentication system was completed in September 2007 to provide for additional capacity and resiliency in this system for future growth.

Annual password expiration was rolled out during winter and spring in order to ensure the effectiveness of the Cal Poly password in protecting resources, and to meet audit requirements. “Forgot my password” functionality was also created to provide more opportunity for users to manage their own passwords. Over sixty thousand password changes occurred last year; a large majority of these changes were completed on a self-service basis, without any assistance required from campus technical or administrative staff. As a result, all user accounts now have updated passwords which meet current strength rules.

C. Create Inventory and Document Existing “Shadow” Data Systems

For further information contact: Theresa May

Storage of sensitive data is a primary consideration related to campus “shadow” data systems, with Social Security Number (SSN) data posing a particular concern. As a result, migrating campus applications away from using SSN as an identifier continued to be a high priority for the campus this year. In order to assist with this migration, the Identity Management team worked with system administrators in identifying how they use the SSN providing an alternative identifier for each campus identity, and assisting with the mapping between SSN and the new identifier. This process helped eliminate the use of SSN throughout campus applications and provide alternate solutions for campus services. Areas and applications that moved away from using SSN data during this year include the Library, Cal Poly Corporation, Housing, and the PolyCard systems.

D. Information Security Forums

For further information contact: Vicki Stover

Reference: http://security.calpoly.edu/what_everyone/security_training.html

The following three information security forums were presented:

Student Data FAQ’s – October 27, 2006 (approximately 30 people)

Identity Theft – March 8, 2007 (74 people)

Due to the popularity of this topic, this forum was repeated in the summer.

Spring Cleaning – May 30, 2007 (approximately 90 people)

The Spring Cleaning Forum presented information regarding the retention of documents due to pending litigation, shredding and storage of materials, and disposition of physical media and hard drives.

E. Information Disposition

For further information contact: Tim Kearns, Mary Shaffer or Vicki Stover

Cal Poly staff (ITS/AFD), along with a small group from other CSU campuses and the Chancellor’s Office, have been working on a systemwide information disposition program. A schedule format has been developed as well as the identification of record series (e.g., Personnel/Payroll, Fiscal, Student Records, etc.). The campuses have assisted the Chancellor’s Office staff by developing and reviewing the schedules.

F. CSU Information Security Officers

For further information contact: Vicki Stover

The CSU Information Security Officers group continues to be a valuable resource. The group meets every other month and the agenda includes such topics as: the systemwide security plan; the security policy project; the Unisys Report; ITAC and CMS updates; security awareness planning; and audit information. In addition, ISO's have had access to training and presentations. For example, SANS – Security 401: Security Essentials training was provided to the campus ISO's and there was a presentation by the California Office of Privacy Protection on privacy laws. ISO's also use the ISO list serve to discuss topics and to exchange information.

Cal Poly's ISO completed her tenure as Chair of the Information Security Officer's group in December 2006.

G. CSU Policy Development

For further information contact: Tim Kearns or Vicki Stover

Reference: <http://redding.calstate.edu/es/csp/doclink.cfm?linkid=147&num=0>

The CSU System signed a Master Enabling Agreement with CH2M Hill Inc. for the term 04/19/06 through 04/18/09. The purpose of the agreement is for the contractor to assess, report on, and make recommendations concerning campus information security policies and practices. It is anticipated that the work from the contractor will result in systemwide policies for Information Security.

H. Awareness Training Development

For further information contact: Vicki Stover

Information security awareness training is an important component in the overall strategy to protect information assets. 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 CSU Information Security Officers (ISO) and an external review team (Unisys Corporation) have assessed current security awareness programs and have concluded that it would be more cost effective for the CSU to develop and manage one comprehensive security awareness orientation course than for each campus to develop its own course. A small group of ISO's, including Cal Poly's, have developed a feasibility study and draft RFP.

The feasibility study has been approved and a RFP is in the final stages of development. The systemwide course proposed by this study will contain the following elements:

- * The course will be mandatory for all employees of the CSU and its auxiliary units.
- * All employees will be required to re-take the course annually.
- * The course will be hosted in a learning management system that will enable the delivery and management of course content.
- * Courses will be “branded” with specific campus contact information including a link to campus information security websites and a link to a campus point of contact.
- * The selected vendor will be given the option to work with campuses on developing additional courseware.
- * The course will be 508 compliant.

- * The course will contain assessment tools to help the CSU and campuses measure the effectiveness of the program.

I. CMS PeopleSoft Student Administration System Implementation

For further information contact: Johanna Madjedi

The CMS Student Administration system was implemented in PeopleSoft as scheduled, completing Fall 2006. All students in the system now use an "emplID" to uniquely identify them in the system. This is no longer associated with SSN; hence, the campus is able to dramatically reduce the use of SSN's to support university business processes.

J. Participate in the System-Wide Security Plan Project

For further information contact: Vicki Stover

During the week of October 9, 2006, Unisys performed an Information Security Program Assessment on campus. ISO 17799:2005, Code of Practice for Information Security Program Management was used as the assessment benchmark as well as applicable State and Federal laws. This assessment was contracted and paid by the CSU Chancellor's Office.

The goal of this project was to assess the current security posture of university policies, standards and best practices and to find ways to improve and/or increase the effectiveness of the Cal Poly Security Framework.

Unisys discovered a few areas of security risk. The areas identified for immediate resolution were: security policy, asset management, and compliance. These risks are addressed in the plans for FY 2007/08.

In addition, Unisys indicated that Cal Poly has:

- * strong security leadership
- * established relationships with all organizations with the university allowing for the effective development and enforcement of security controls throughout the campus
- * established an adequate assets management process for hardware and software
- * established adequate physical and environmental security controls
- * has strong Access Management Controls in place.

The Unisys Information Security Report was shared with the Information Security Committee, IRMPPC, and the President's Management Staff.

K. Social Security Inventory

For further information contact: Vicki Stover

The Social Security Inventory continues to be revised. The Information Security Officer maintains the listing and provides it to the members of the Information Security Committee for review.

Color coding of the items (e.g., Red – Use of SSN Required; Green – no longer using SSN; Yellow – planned/in process of no longer using SSN; White – To be reviewed) provides a status of each item listed.

III. Goals for FY 2007/08

Following are brief descriptions of projects that have been identified to be undertaken in FY 2007/08 that will support continuation of our efforts in the area of security.

A. Policy/Standards Development

In response to the Unisys Assessment, development of the following policy/standards are planned: Incident Response, Training and Awareness, Information/Data Classification and Handling, and Credit Cards.

B. Information Security Forums

Information Security Forums are planned for the Fall, Winter, and Spring quarters. The first forum is scheduled for November 1st and will present information on FERPA.

C. Border Firewall Upgrade

As part of the CSU ITRP@ effort, the campus border firewall will be upgraded to a standard CSU implementation. Expected completion date is December 2007. This project will refresh the campus Border Firewall technology and position the campus to respond to any CSU-wide security initiatives that are associated with this environment.

D. Social Security Inventory

The Social Security inventory will continue to be updated until all processes which include SSN are documented as requiring the SSN.

E. Updating Information Security Website

The Information Security website will be updated and will include a section on “What Students Should Know”.

F. Awareness Training Development

It is anticipated that the Awareness Training program will be available to the campus this upcoming year.

G. Information Disposition

A draft Executive Order is being reviewed and a website is under construction. Once the Executive Order is issued the schedules will be released as they become final. It is anticipated that the first schedules released will be Personnel/Payroll, EH&S, Facilities, and Academic Personnel with the Student Schedule not far behind.

H. Finding SSNs

ITS will be evaluating a tool for finding SSNs on systems. AFD will participate in this pilot evaluation.

I. Information Security Strategic Plan

Based on the information provided by the Unisys Assessment, an information security strategic plan will be developed to address outstanding issues.

J. Development of Standards for Technical Staff

The development of standards for technical staff will focus on ensuring that security requirements are documented and that implemented systems meet these requirements. This will include clarification of the roles of technical staff.