



University of California
San Francisco

advancing health worldwide™

650-16 Training for DOM Managers

IT Services

Department of Medicine

Erik Wieland

Director of IT Services

Monday, February 25, 2008

*UCSF Campus Administrative Policy
650-16: Information Security and
Confidentiality*

Information Security Incidents

- **200** student applicants' information compromised when a UCSF employee's laptop was stolen from her car while parked at an airport
- **7,000** patients' files compromised when a UCSF computer infected with two types of malicious software allowed the opportunity for an attacker to gain access
- **50,000** UCSF employees' information breached when a UCSF computer infected with a virus was compromised - attacker tools were installed which allowed multiple opportunities for data compromises

In all of these cases, the departments were responsible for notifications and associated costs

One incident cost a department over **\$875,000 in notification costs**

Additional Costs

In addition to monetary costs, incidents incur

- **Loss of data**
- **Loss of patient confidence**
- **Loss of employee trust**
- **Impaired business function**
- **Damage to UCSF's reputation**
- **Damage to your reputation**

Notification Costs

\$875,000

one department
ultimately paid
for notification

Postage & Letters

Legal cost

Reputation

Lost research hours and time

Lost employee productivity

Incident response

What Is UCSF Doing About It?

- **Implemented UCSF Policy 650-16 – Information Security and Confidentiality**
- **Provides for compliance with federal and state laws and regulations and university policies that govern the security and confidentiality of electronic information**
 - Developed by the Information Security Committee (ISC)
 - Reviewed and approved by the ISC and IT Governance
 - Initial version dated January 2005
 - Revised January 2007

What Else is UCSF Doing?

- **Developing and deploying tools for detection, prevention and remediation**
- **Using new technologies to assist UCSF faculty, staff, and students in complying with 650-16**
- **Performing risk assessments and minimum standards compliance assessments**
- **UCSF Risk Management and Insurance Services is offering “zero deductible” protection for laptop computers**
- **Conducting awareness sessions about UCSF Policy 650-16**

You and your staff have a role to play in protecting UCSF information

650-16 Highlights

- **Defines terms such as “Restricted Data” and “EIR”**
- **Identifies related UC and UCSF policies**
- **Includes three addenda:**
 - **Addendum A: UCSF Roles and Responsibilities for Securing Electronic Information Resources (EIRs)**
 - **Addendum B: UCSF Minimum Security Standards for Electronic Information Resources**
 - **Addendum C: UCSF Incident Investigation**

Application

- **Policy 650-16 applies to all members of the UCSF community including consultants, temporary staff, third parties, etc.**
- **Applies to all systems used for UCSF purposes, including:**
 - **Personal systems** – home systems, personal systems on campus
 - **Mobile devices** – Treos, iPhones, memory sticks, etc.
 - **Third-party systems** – vendor-owned systems
 - **Off-campus systems** – off site storage, UCSF systems at other locations

University of California
San Francisco



Department
of Medicine

IT Services

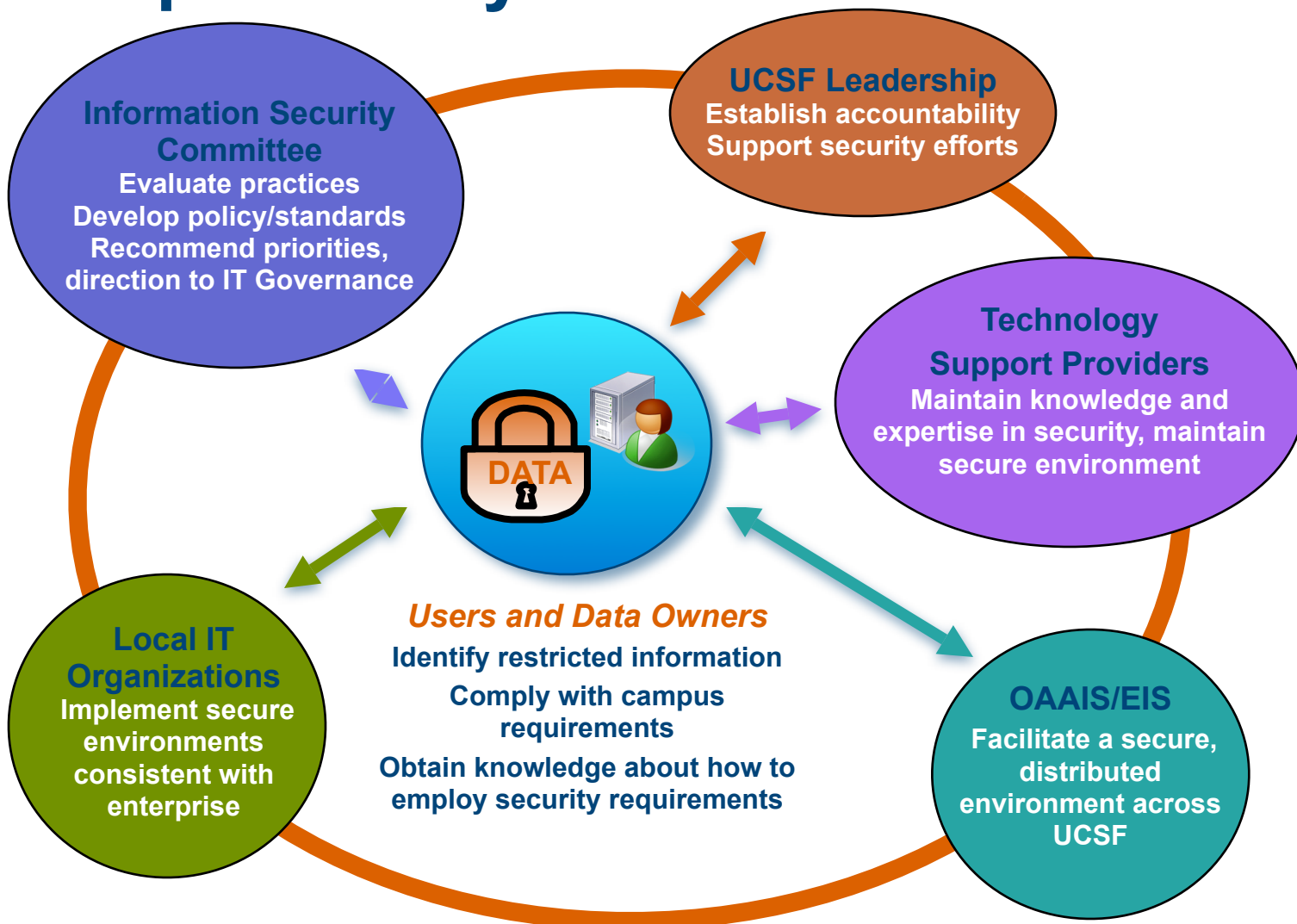
Addendum A

ROLES & RESPONSIBILITIES

Defined Roles and Responsibilities

- **UCSF Leadership**
- **Individuals**
- **Information Security Committee**
- **Unit/Department officials**
- **Office of Academic and Administrative Information Systems (OAAIS)**
- **Other Central IT organizations**
- **Technology Support Providers**

Information Security is a Shared Responsibility



Your Role and Responsibilities

- **Support the policy, and the Department's implementation, including**
 - Following data access policies
 - Abiding by connectivity standards, including security software
 - Knowing where your protected data is, and documenting it
 - Supporting security audits, and handling security incidents
 - Implementing remediation strategies, as defined by Enterprise Information Security (EIS), DOM IT Services, and your local IT team
- **Cover the costs associated with compliance**

When a Security Incident Occurs

- Your unit **must** participate in the incident response process
- You as a manager are primarily responsible for:
 - Working with EIS, DOM IT, and other entities to resolve the incident
 - Coordinating with campus legal and external relations specialists
 - Notifying affected individuals as required by law
 - Notifying Employee & Labor Relations if the incident involves an employee
 - Covering the costs of the incident response process
 - Having proper incentives in place to ensure the timely reporting of security incidents



University of California
San Francisco

Department
of Medicine

IT Services

Recent UCSF Security Incidents

Incident	EIS Role	Department Role
<ul style="list-style-type: none"> ▪ Server with UCSF payroll information was compromised ▪ 46,000 affected 	<ul style="list-style-type: none"> ▪ Analyzed breach ▪ Provided guidance for notifications ▪ Provided guidance to prevent reoccurrence 	<ul style="list-style-type: none"> ▪ Identified exposed information ▪ Implemented changes to prevent recurrence ▪ Responsible for notification
<ul style="list-style-type: none"> ▪ Server containing research data was stolen ▪ >3,000 affected 	<ul style="list-style-type: none"> ▪ Initiated investigation ▪ Analyzed recovered data ▪ Provided guidance for notifications ▪ Provided guidance to prevent reoccurrence 	<ul style="list-style-type: none"> ▪ Restored data from backups ▪ Analyzed and identified information ▪ Worked with EIS and other UCSF entities to resolve incident ▪ Implemented changes ▪ Responsible for notification

University of California
San Francisco



Department
of Medicine

IT Services

Addendum B

MINIMUM SECURITY STANDARDS

Minimum Security Standards

Effective January 1, 2008

- ✓ **Anti-virus software installed and active**
- ✓ **Encryption of ePHI email**
- ✓ **Restrict and protect information on mobile devices**
- ✓ **Host-based firewalls**
- ✓ **Strong passwords**
- ✓ **Physical security of devices**
- ✓ **Software patches kept up to date**
- ✓ **Unnecessary services disabled**

Your Role and Responsibilities

- **Encourage others, and provide resources, to meet the minimum standards**
- **Minimum standards require that departments and managers**
 - Plan to accommodate the **financial impact**
 - **Create a timeline** for implementation
 - Perform a gap analysis, and determine if hardware/software upgrades are needed

Compliance Resources

- **EIS offers *free* tools for detection, prevention, and remediation**
 - antivirus software, personal firewalls, anti-spyware software, etc.
- **Checklists for minimum security**
 - Manager, technical support provider, and user versions
- **EIS and DOM IT provide assistance with risk assessments**
- **EIS Security Awareness presentations**
- **OAAIS Information Security website**
- **DOM IT Services KnowledgeBase**

University of California
San Francisco



Department
of Medicine

IT Services

Addendum C

INCIDENT RESPONSE

Definition and Purpose

- **Incident: an event that violates or is suspected of violating UCSF Electronic Information Resource access and usage policies, such as:**
 - Malicious code (virus, spyware, malware) attacks
 - Passwords attacks
 - Port scanning
 - Lost/stolen mobile devices with restricted information
- **Addendum C: Incident Response**
 - Guidelines and procedures for effective information security incident investigations
 - Goal is to mitigate damage and loss due to an information security incident

Defined Roles and Responsibilities

- **Authorized users**
- **Affected departments**
- **Committee on Human Research (CHR)**
- **Controller**
- **Electronic Information Resources custodian and proprietor**
- **Enterprise Information Security**
- **Human Resources**
- **UC Police Department**
- **UC Privacy Office**
- **Risk Management**

Your Role and Responsibilities

- Your unit **must** participate in the incident response process
- You as a manager are primarily responsible for
 - Working with EIS, DOM IT, and other entities to resolve the incident
 - Coordinating with campus legal and external relations specialists
 - Notifying affected individuals as required by law
 - Notifying Employee & Labor Relations if the incident involves an employee
 - Covering the costs of the incident response process
 - Putting proper incentives in place to ensure the timely reporting of security incidents

Effective Incident Response requires a partnership with EIS and DOM IT Services

How EIS Assists

- **EIS**
 - Assists departments in incident resolution
 - Addresses incident questions from a Campus perspective
 - Provides guidance to prevent incident reoccurrences
 - Provides guidance to address any findings
 - Provides guidance in notification of individuals

Incidents will continue to happen

EIS will work with you to minimize the impact of incidents

Examples of UCSF Incidents

Roles and Responsibilities

Law	Requirement	Individuals	EIS	Departments
SB1386	Protect SSNs, financial information	<ul style="list-style-type: none"> Identify and protect restricted information Identify exposed information 	<ul style="list-style-type: none"> Provides guidance Validates notifications Analyzes incidents 	<ul style="list-style-type: none"> Responsible for notification Ensures protection of restricted information Works with EIS and UCSF to notify affected individuals
e-Discovery	Identify, preserve and protect electronic information related to Federal civil litigation	<ul style="list-style-type: none"> Identify relevant information Make available identified information Work with EIS and Campus to resolve e-Discovery issues 	<ul style="list-style-type: none"> Technical bridge between Risk Management, Legal and end users 	<ul style="list-style-type: none"> Work with Risk Management, Legal and EIS Notify Risk Management of e-Discovery notices

Summary

- **Recap 650-16 and addendums**
 - Addendum A: Roles & Responsibilities
 - Addendum B: Minimum Standards
 - Addendum C: Incident Investigation
- **Effective date: January 2008**
- **Where to find the policy**
 - <http://policies.ucsf.edu/650/65016.htm>

Resources and Guidance

- **Checklists for minimum security**
- **Security Awareness presentations**
- **OAAIS Information Security website** <http://security.ucsf.edu>
- **DOM IT Services KnowledgeBase** <http://domsupport.ucsf.edu/help>
- **Policy Links**
 - Whistleblower <http://whistleblower.ucsf.edu/>
 - IS-3 <http://www.ucop.edu/ucophome/policies/bfb/is3.pdf>
 - 650-16 <http://policies.ucsf.edu/650/65016.htm>