

Information Security Work Group

- UC academic, business and IT leaders
- Convened at the request of President Dynes
- **Objective:** recommend strategies to improve information security and reduce # and severity of security breaches

Information Security Work Group: Leadership

- Define roles / responsibilities / accountability:
 - System wide
 - Campus
 - Unit
 - Individual
- “Insurance” fund to offset cost of breach reporting?

Information Security Work Group: **Communications**

- UC-wide, general audience information security PR campaign
 - UCOP Strategic Communications
- Templates for communication to specific audiences
 - “Security at UC” website for repository

Information Security Work Group: **Education / Training**

- Web-based training module for general UC audience throughout UC
 - UC IT Policy and Security group will review campus offerings / recommend approach

Information Security Work Group: **Security incident handling**

- Log management guidelines
- Forensics tools and services
- UC-wide security peer evaluation / ad hoc security SWAT team
- UC guidelines for incident handling
 - IT Leadership Council, IT Policy /Security Group, IT Internal Audit

Information Security Work Group: **Policy requirements / updates**

- Minimum network connectivity standards
- Standards for allowable use of restricted data
- Guidelines for data encryption
 - IT Leadership Council, IT Policy and Security Officers

Information Security Work Group: Campus security programs

- Designated responsibility
- Develop campus security programs and compliance mechanisms
 - Risk assessment – restricted data
 - Mitigation measures
 - IT Leadership Council, IT Policy and Security Officers, Controllers

Information Security Work Group: Encryption

- Business processes & tools for encryption of restricted data in storage
 - Clinical Services, IT Leadership Council, IT Policy and Security Officers

UCOP Information Security Policy

Phase I: Security of Network Resources

- Servers must be registered with IR&C
- All devices connected to the network must meet specific requirements
- Established standards for Windows and Mac computers
- Effective July 2005

UCOP Information Security Policy

Phase II: Protection of Information Assets

- Departments must establish their own information security programs
 - conduct risk assessments
 - identify and classify electronic resources
 - identify vulnerabilities and threats
 - identify controls/procedures to address risk

UCOP Information Security Policy

Phase II: Protection of Information Assets

- Departments must establish security plan
 - identify individual responsible for security
 - identify controls
 - ensure that vendor-hosted systems and contracts are in compliance with IS-3
 - procedures for reporting suspicious events
 - ensure security training and education for all employees

UCOP Information Security Policy

Phase II: Protection of Information Assets

- Information Security Plan
 - clearly and simply written
 - communicate to staff through standard means
 - communicate to new hires
 - review annually or when workflow changes