

## Privacy, Security & Copyright

---

- **Background and Update**
- **Security Awareness**
- **(Proposed) Minimum Standards for network-connected devices**

## UC Stance on Privacy & Security

---

- Promote open exchange of information**
- Value individual privacy**
- Do *not* “police” systems or networks, looking for violations**
- Do act promptly when a violation comes to light**
- Manage systems and “the network” to ensure functionality and reliability.**

## UC Electronic Communications Policy

---

- **Privacy, confidentiality, and security**
- **Allowable Use includes use “for incidental personal purposes”**
- **Key points under current revision:**
  - **“Nonconsensual access**
  - **“Unavoidable Inspection”**
  - **Update definitions of Public and University administrative records**
  - **Encryption advisory and guidelines as in IS-3**
  - **Retention and disposition as in RMP-2**

## Policies, Laws & Regulations

---

- **DMCA – Digital Millennium Copyright Act**
  - **Provides for limits to the liability of online service providers who are unaware of violations**
  - **Each campus has a designated agent to receive and handle notices of infringement**
  - **Different rules for cases related to faculty or graduate students performing teaching or research than for students, faculty, and staff in general.**

## DMCA Stats for UCI

---

AcadYear	Fall	Winter	Spring	Summer
1999-2000	-	2	2	0
2000-2001	1	4	3	9
2001-2002	3	11	12	13
2002-2003	20	36	10	10+1
2003-2004	23+5	25+1	15+1	12

("X+Y"=X real + Y duplicate/spurious)

**Jan-Oct 2004: 54 allegations:**

**27 in Residential Housing (24 Movies + 3 software)**

**27 elsewhere: 44 Movies + 7 software + 2 Audio + 1 other**

NACS Faculty Advisory -- 29 Nov 2004

franklin@uci.edu - 5

## UC BFB IS-3, Electronic Information Security

---

### IS-3 provides EIS guidelines

- **Local campus implementation coordination**
- **Key points in current revision:**
  - Expand scope to include “conduct of activities in support of the University’s mission”
  - Incident response and planning
  - “Logical” Security: Encryption, Access control (Authentication & Authorization)
  - “Physical” security including mobile devices

NACS Faculty Advisory -- 29 Nov 2004

franklin@uci.edu - 6

## Policies, Laws & Regulations

---

### HIPAA = Health Insurance Portability & Accountability Act

- **Protected Health Information (PHI)**
  - Past, present or future physical or mental health or condition
  - Provision of or payment for health care to the individual
- **Privacy regulations apply to PHI in any form or media: electronic, paper, or oral.**
- **Security regulations apply to electronic PHI**

NACS Faculty Advisory -- 29 Nov 2004

franklin@uci.edu - 7

## Policies, Laws & Regulations

---

### (California) SB 1386

### Personal Information in Computerized Data

(California Civil Code 1798.29 & 1798.82-1798.84)

- **“Personal Information” = Name and any of the following:**
  - Social security number
  - Driver's license number or California Identification Card number.
  - Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

NACS Faculty Advisory -- 29 Nov 2004

franklin@uci.edu - 8

## Why care about (EIR) Security

---

- Legal responsibilities
- Real risks/threats and consequences
- Institutional & Personal (e.g., identity theft)
- Reputation & Trust
- Lost Work
- Lost Time
- Denial of Service
- Cost of Remediation

## Personal Identity “Incidents” 2004

---

<u>People</u>	<u>Date</u>	<u>University</u>
178,000	April	San Diego State
380,000	May	UC San Diego
145,000	June	UCLA
600,000(-1.4M)	October	Berkeley

Even “small” incidents can be “big trouble”

### Major risks:

- Mobile devices:  
Laptops, PDA’s, iPods, “USB drives,”...
- Dormant/Dead accounts
- Unpatched systems

## EIR Security Examples

---

### Obvious examples

- Portable devices:  
Laptops, PDA’s, ...
- Passwords
- Research and development data
- Human resources personnel files
- Student information

### Less obvious examples

- Professor’s contact list
- Email messages
- Personal telephone numbers
- Home address
- Birth date
- Ethnicity information
- Gender information

## Risk Assessment and Mitigation

---

- Technical measures/staff key, but “can only do so much.”
- Much of security depends on “end user”
- Balance technical and social
- Areas of continued & growing risk:
  - Sensitive information where it doesn’t have to be
  - Insecure communication and passwords
  - Mobile devices
  - Old/unpatched software
- Balance cost and convenience

## Security Awareness

---

1. **Use/store confidential information very carefully/sparingly**
2. **Good password practices**
3. **Secure transmission: VPN, https, ssh, ...**
4. **Backup on professionally managed system**
5. **Encrypt on mobile devices and store definitive copy elsewhere**
6. **Keep critical software up to date: patches and virus protection**
7. **Be very cautious with email and web**

## 2. Guidelines for “Good” Passwords

---

- **Hard to guess, but memorable (for you).**
- **Six to 12 characters in length.**
- **At least 1 of each of the following:**
  - Upper case letters; Lower case letters;
  - Digits; Special characters: ,.\_-+#!\*%\$#@()
- **Use digits for letters and syllables:**
  - 1=L,I; 2=to,Z; 3=E; 4=for(e); 5=S; 8=ate
- **Possibly a short phrase (e.g., “2L&2L1ttl3”)**
- **Different passwords for different uses.**
- **Change regularly.**

## 7. Email & Web Security Awareness

---

- **Don’t open unexpected attachments**
  - Cannot trust apparent source to be real source
  - Trusted source may send “dangerous” email
  - Unknown sources are to be trusted even less
- **Don’t send sensitive information via email**
- **HTML email=web page from unknown source**
- **Know source of current page and link target**
- **https for Security: Look for the Lock**

**All these “rules” are better viewed as cautions than as absolutes.**

## What is being done

---

- **IS-3 framework**
  - Policy revision: Change of context/scope
  - Campus-level coordination
  - Identify and limit risk
- **Technical measures**
  - May need administrative backing. For example, Minimum standards (requirements) for network-connected devices; scanning & monitoring
- **“Social” measures**
  - Security Awareness, Reaching Everyone**

## **(Proposed) Minimum Standards**

---

**Software patch updates**

**Anti-virus software**

**Host-based firewall software**

**Passwords**

**No unencrypted authentication**

**No unauthenticated mail relays**

**No unauthenticated proxy servers**

**Physical security**

**No unnecessary services**

## **What is to be done: Next/More Steps**

---

- **Engage academic units in parallel with existing IS3 efforts**
- **Maintain & Expand EIR inventory**
- **Increased (non-technical) management involvement in Security Awareness, Risk Assessment & Mitigation**
- **Shared recommendations, expanding & broadening that already happening among technical staff.**