

# ITS Town Hall



## ITS Town Hall

### Security Policy Update

8/12/09



Information Technology Services

its.ucsc.edu

### UCSC's Minimum Network Connectivity Requirements Policy



As-of March 4, 2009, UCSC has Minimum Network Connectivity Requirements.

• Access Controls	• Firewalls
• Password requirements	• Remove unnecessary services
• Anti-virus/Anti-spyware	• Session timeouts
• Patching	• Physical security
• Secure transmission of passwords & restricted data	• Authenticated email relays and proxy servers
	• Security audit agents can be required



Information Technology Services

## What the Min Network Connectivity Requirements Mean for Us (ITS)



### Expectations for ITS employees:

- Be familiar with the requirements
- Ensure that devices for which you are responsible comply with the requirements
  - Includes workstation or laptop

Campus security requirements apply to all devices used for University business purposes, regardless of ownership or location.

## STOLEN CORNELL LAPTOP CONTAINS SENSITIVE INFORMATION ON STUDENTS, FACULTY AND STAFF – 6/23/09



... The laptop, which was being **used to help diagnose transmission problems** with the university's central administrative systems and **does not appear to have been encrypted**, contained the **names and Social Security numbers** of **22,546** current and former students and **22,731** current and former faculty and staff members.... Cornell officials have sent an email notification to all affected individuals and will be sending out letters shortly.

## UNLV NOTIFIES STUDENTS OVER POTENTIAL DATA LEAK – 6/1/09



In all, about **20** UNLV students received the notice after a **virus allowing remote access** was discovered on a **computer containing the students' personal information**. According to Victor Barragan, CSUN Senate president and former sciences senator, there is **no evidence that the information was leaked** but the law requires the notification be sent.

## NEW UTAH SCHOOL DISTRICT APOLOGIZES FOR LOST EMPLOYEE DATA – 7/13/09



Canyons School District officials are investigating the **disappearance of a thumb drive** that contained the personal information of **more than 6,000** current and recent employees. The USB flash drive is believed to have contained employee **addresses, phone numbers, dates of birth and Social Security numbers**. A district-level worker was using it to **transfer data** for apparently "legitimate," job-related purposes.

## ITS Policy on Personal Identity Information (PII)



- Don't store unencrypted PII on portable devices or media
- Don't store or access PII on a non-University computer

### Going a step beyond our policy

- Figure out how not to store PII on your local devices at all. Keep it on the servers.

Questions?



**Contact Julie Goldstein at  
*julieg@ucsc* or 9-2779**