



# **Seven Deadly Security Sins**

**Presented by  
Information Technology Services  
and  
Office of the General Counsel**

# Universities vulnerable to ID thieves



UCLA, Georgetown, Ohio, Alaska, Texas among targets  
this year – The Associated Press 12/18/06

# Secure Data – FERPA

- Family Educational Rights and Privacy Act of 1974
  - Protects the confidentiality of student records
    - Records directly related to a student
    - Records maintained by the University or a party acting for the University
    - All media including, but not limited to, electronic data, email, video or audio tapes
  - Student information can be released only -
    - With prior written consent of student
    - With a legitimate educational interest
    - With a court order

# Secure Data - HIPAA

- Health Insurance Portability and Accountability Act of 1996
  - Protects all “individually identifiable health information”
    - Electronic, paper or oral formats
  - Disclosure is permitted only -
    - As the privacy rule permits or requires
    - As authorized in writing by the individual who is the subject of the information

# Secure Data – GLB Act

- Gramm-Leach-Bliley Financial Modernization Act of 1999
  - Protects consumer financial information
  - Requires the design, implementation and maintenance of safeguards to protect customer information
  - Covers all entities who gather such information

# Secure Data – PIA

- Public Information Act gives the public the right to request information from governmental bodies
  - Excepted information
    - Information considered confidential by statute or judicial decisions (FERPA, HIPAA, GLB Act, etc.)
    - Information relating to current litigation
  - Types of information available to the public -
    - Information that is collected, assembled, or maintained by a governmental body in any medium
      - Student directory information (designated in policy D-13, Student Records)
      - Personnel information (employee can request that home address, telephone number, social security number and family information be restricted)

# Secure Data – Social Security Number

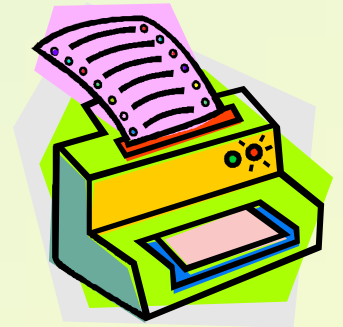
- Privacy Act of 1974, Public Law No. 93-579, 88 Stat. 1897 (Dec. 31, 1974), codified in part at 5 U.S.D § 552a
  - Protects confidential status of social security numbers
  - Texas Statute: Identity Theft Enforcement and Protection Act, Texas Business and Commerce Code, § 48.102

# Secure Data – Other Issues

- Record Management Policy, D-28
  - Follow the University's record retention schedule and dispose of documents properly when indicated
- Data Hold Notice
  - When data is relevant to ongoing litigation, Data Hold Notice will be sent
    - ALL relevant data, including electronic media, must be preserved until further notice

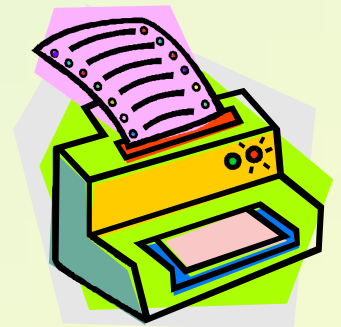
# Sin 7. Carelessness with Print

- Print documents containing sensitive information (e.g. SSN, CID) on publicly accessible printer.



# Sin 7. Carelessness with Print

- Print documents containing sensitive information (e.g. SSN, CID) on publicly accessible printer.
- Leave documents containing sensitive information on your desktop, the conference table, etc.



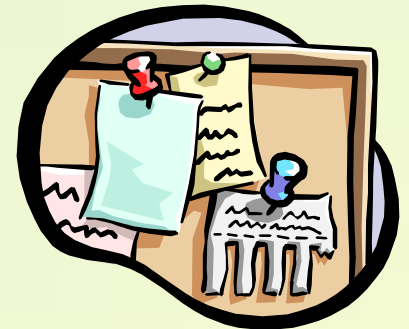
# Sin 7. Carelessness with Print

- Print documents containing sensitive information (e.g. SSN, CID) on publicly accessible printer.
- Leave documents containing sensitive information on your desktop, the conference table, etc.
- Dispose of documents containing sensitive information without shredding them first.



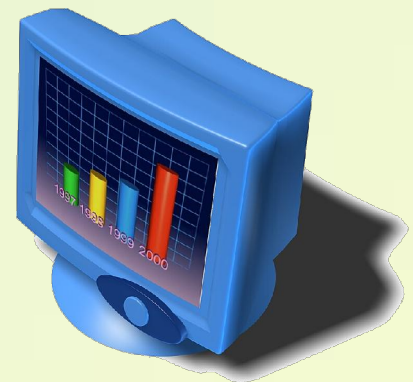
# Sin 6. Intentional Misuse of Print

- Posting documents containing sensitive information for public view (e.g. class rosters, test results).



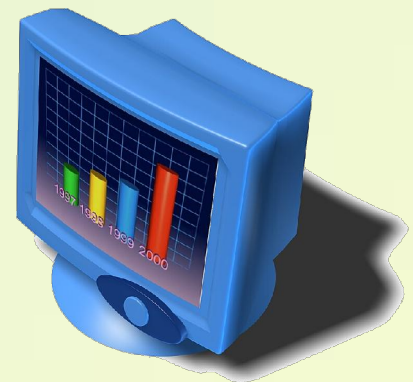
# Sin 5. Carelessness on Workstation

- Display sensitive information on monitor that is the public view.



# Sin 5. Carelessness on Workstation

- Display sensitive information on monitor that is the public view.
- Leave workstation while still logged on, without first locking it.



# Sin 4. Failing to protect your Identify

- Allow other people to use your Logon ID and Password.



# Sin 4. Failing to protect your Identify

- Allow other people to use your Logon ID and Password.
- Use easy-to-guess Passwords.



# Sin 4. Failing to protect your Identify

- Allow other people to use your Logon ID and Password.
- Use easy-to-guess Passwords.
- Write down Passwords and store them in a “convenient” place



# Sin 3. Careless Electronic Distribution

- Posting sensitive information on the Internet (including SFA's public and private websites).



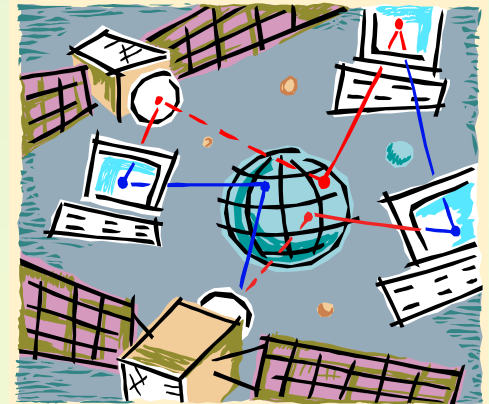
# Sin 3. Careless Electronic Distribution

- Posting sensitive information on the Internet (including SFA's public and private websites).
- Sending sensitive information via e-mail.



## Sin 2. Use of Personal File Sharing

- Installing file sharing software (e.g. Limewire, Morpheus) on your workstation.



# Sin 1. Carelessness with laptops, etc

- Storing sensitive information on a laptop.



# Sin 1. Carelessness with laptops, etc

- Storing sensitive information on a laptop.
- Losing media containing a backup of sensitive information (e.g. thumb drive, floppy, CD)



# Sin 1. Carelessness with laptops, etc

- Storing sensitive information on a laptop.
- Losing media containing a backup of sensitive information (e.g. thumb drive, floppy, CD)
- Throwing away media that fails, rather than destroying it.



# Scenario 1:

You have been assigned the responsibility for disposing of records that have reached their expiration date according to the University's Records Retention Schedule. The documents contain student social security numbers. You should:

1. Place them in a trash bag to be taken to the dumpster.
2. Keep them because you're not sure how to handle disposing of them.
3. Patiently shred each document.

# Scenario 1 Answer:

Number 3: Shred away!



## Scenario 2:

You have been asked to post test grades outside the department door. The students' grades are listed by the last four digits of their social security number. You should:

1. Post the grades as requested.
2. Advise the requestor that you are unable to post the list due to the confidential information.
3. Email the grades to the students instead of posting.

# Scenario 2: Answer

Number 2: Don't post...



## Scenario 3:

An individual enters your office, shows you a badge and asks for information about a student. You should:

1. Give him/her the information quickly because he or she is a peace officer!
2. Refer him/her to the General Counsel's Office.
3. Ask for a signed release and if it is provided, give him/her the information.

# Scenario 3: Answer

Number 2: Call the General Counsel's office!



## Scenario 4:

You need to email a document containing confidential student information. You should:

1. Email the document as an attachment and don't worry about it.
2. Cut and paste the information in the document into your email.
3. Password or encrypt the document and email it as an attachment.

# Scenario 4: Answer

Number 3: Password or encrypt the document.



## Scenario 5:

You decide to download some music to listen to on your computer during your lunch hour. You should:

1. Download from a file sharing web site—no one will ever know.
2. Not download music on your work computer!

# Scenario 5: Answer

Number 2: Don't download!



# Scenario 6:

You have to input student information and are unable to finish the assignment due to other responsibilities, so you consider assigning a student worker the task and giving her access to the Student Information System. You should:

1. Go ahead and do it, because it is acceptable for student workers to have access.
2. Not assign the task to the student worker, because the information contained in the system is confidential and access should be restricted.
3. Check with your supervisor concerning assigning the work to the student worker.

# Scenario 6: Answer

Number 2: Don't assign it to a student worker.



# Scenario 7:

You are assigned to develop a form gathering information from students. You should:

1. Not collect social security information unless absolutely necessary.
2. Collect any information you want.
3. Collect the social security information and keep the students' responses in a locked cabinet.

# Scenario 7: Answer

Number 1: Don't collect it if you don't have to.



# Scenario 8:

You have to be out of the office for vacation and other employees may need to access your computer files. You should:

1. Give them your password and ask them to keep it in a safe place.
2. Provide them with copies of documents they might need, but not share your password.

# Scenario 8: Answer

Number 2: Don't share!



## True or False:

A University employee responsible for technology security was fired for maintaining a P2P file on his/her desktop computer?

**TRUE**

# True or False:

A business office employee sent a campus-wide email with actual screen prints containing student information.

**TRUE**

## True or False:

A student employee set up a website containing social security numbers of student who lived in a particular residence hall.

**TRUE**

# Questions?

