



Modern Data Security in Five Acts

Act I: Modern Data Handling



WELCOME!

- **Gerry McCartney, CIO**



National Cyber Security Awareness Events

- **Act I: Modern Data Handling**
- **Act II: Security on the Go**
- **Act III: Modern “Teleworking” Solutions**
- **Act IV: Beyond the Secret Decoder Rings**
- **Act V: Security Trick or Treat**

<http://www.purdue.edu/securepurdue/training/awarenessMonth.cfm>



The World We Live In ...

- Between January 1 and June 30, 2006, Symantec documented 2,249 new vulnerabilities, up 18% over the second half of 2005. This is the highest number ever recorded for a six-month period.



The World We Live In ...

- The average loss per victim attributed to the crime of identity theft is more than the amount attributed to bank robbery.
- Between January 1 and June 30, 2006, education was the 4th most frequently targeted industry behind Home users, Financial Services, and Government.



Speakers

- Dan Whiteley: Student Services Technology and Assessment
- Hans Sigg: Business Services Computing
- Joanna Grama: ITaP Security & Privacy

- Panelists
 - Brett Coryell: Deputy Chief Information Officer
 - Robert Stanfield: Director, Identity and Access Management Office



DATA HANDLING TRAINING

INTRODUCTION

- **Presented by:**
Hans Sigg
Business Services Computing



Secure Data Handling

Who really cares?



Secure Data Handling

Story Time



Secure Data Handling

Where do we go from here?



DATA HANDLING TRAINING

Data Classification

- **Presented by:**
Dan Whiteley
**Student Services Technology and
Assessment**



- For purposes of handling data appropriately, data is classified by data stewards and information owners into one of the following categories:
 - **Public**
 - **Sensitive**
 - **Restricted**



Confidential

- The term “Confidential”, is often used interchangeably with other security terminology.

“Confidential” is not a data classification like sensitive or restricted. It describes how information should be treated and it can be used to describe information that may be sensitive or restricted. For example, a conversation between an academic advisor and student may be confidential and the student wishes that the advisor not share that information with anyone else.



Public Data

- **Information that may be, or must be open to the public**
- **Examples of student data in this category include:**
 - Summary reporting data as appearing in the data digest.
 - Directory Information: Name, local and home address, local and home telephone listing, electronic mail address, school and curriculum, classification and credit hour load, dates of attendance, degrees, awards and honors received, participation in officially recognized activities, height, weight and position of members on athletic teams



Sensitive Data

- **Information that should be guarded, or could be considered as data that has some privacy concerns**
- Examples of student data in this category include :
 - **PUID**
 - Major Program of Study
 - Prospective Student Contact
 - Admissions applications (both paper and electronic)
 - Admit Decision letters
 - TOEFL, SAT and ACT scores



Restricted Data

- **Information protected by FERPA, HIPAA, GLBA, state statute or data considered by the university to be highly sensitive.**
- **SSN/SID** is included in this category.



FERPA

- <https://www2.itap.purdue.edu/registrar/training/ferpa/content.cfm>
- **Family Education Rights and Privacy Act of 1974**
- Outlines what rights the student has to his/her education records. It also outlines when education records can be disclosed and to whom.
- Example of FERPA protected data are:
 - *Grades, transcripts, degree information, Class schedule, Student's information file (SI file).*



HIPAA

- <http://www.purdue.edu/hipaa>
- **Health Insurance Portability and Accountability Act of 1995**
- Requires that Purdue must preserve the privacy and confidentiality of protected health information
- Examples of protected health information are:
 - *Past, present, or future physical or mental health conditions*
 - *Provision of health care*
 - *Past, present or future payment for health care that identifies an individual (name, address, SSN, DOB)*



GLBA

- http://www.itap.purdue.edu/security/policies/GLB_Safeguards_Rule_Training_General.pdf
- **Gramm Leach Bliley Act**
- Protected information: consumer's information (i.e. loan application information) that is submitted to receive a financial service
- Examples of financial services at Purdue are:
 - *Student loans, Information on delinquent loans, check cashing services*



Indiana State Law

- **Indiana Code 4-1-10: Release of Social Security Number**
- *A University employee who “knowingly, intentionally, or recklessly” discloses an SSN in violation of the non-disclosure rule can be charged with a felony.*



Student Restricted Data

- **Student Restricted Directory Information includes:**
 - RESTR-HOME, home address and telephone listing may not be released
 - RESTR-LOCL, local address and telephone listing may not be released
 - RESTR-ADDR, all address and phone listings may not be released
 - RESTR-PHON, all phone listings may not be released
 - RESTR-SCHOOL, school, field of study, credit hours, or classification may not be released
 - RESTR-DEGS, degrees and honors received may not be released
 - RESTRICTED, no information at all may be released



Student Restricted Data

- Class schedule information
- Clinical dictation for transcribing into voice data format
- Confidential letters of recommendation
- Credit Bureau information
- Credit card information, application fees, check information
- Criminal investigation information
- Deceased students
- Disability information
- Discipline information
- Donor information
- Encumbrance information
- Exam schedule
- Fellowship awards
- Financial Aid information
- Financial information of students and or parents
- Fraudulent records information
- Grades
- GPA



Student Restricted Data

- Insurance information
- Immunization records
- Litigation information via internal staff and 3rd party service providers
- Medical records
- Minority student information
- Patient test results information
- Plan of study
- Psychological reports
- Resume information
- Salary information collected from former students
- Sex change information
- Subpoenas for student records
- Tax record information of students and or parents
- Test scores either internal or from standardized tests such as SAT, ACT
- Transcripts
- Veterans' records
- Witness protection program participants



Examples of Restricted Financial Data

- SSN
- Credit card numbers
- Photographs of individuals
- Transactions, balances for selected accounts (i.e., reserves, endowments, etc.)
- Data covered under GLBA (loan agreements and balances, collection activity)
- Bank account numbers
- Grant proposals
- Selected Ledger Accounts



Examples of Restricted HR Data

- SSN
- Data covered under HIPAA (i.e., Benefit Claims, Benefit Selections)
- Employee appraisals
- Employee counseling
- Employee discipline
- Garnishments/child support



Classification Matrix

- A more complete list of the data classifications is available at the following web site:

**[http://www.itap.purdue.edu/security/procedures/
dataClassif.cfm](http://www.itap.purdue.edu/security/procedures/dataClassif.cfm)**



Personally Identifiable Information (PII)

- PII information includes the following:
 - SSN
 - Date of birth
 - Mother's maiden name
 - Driver's license number
 - Bank account information
 - Credit card information
- When the above information is used in combination with each other, a person's identity could be stolen.
- PII can also be personal characteristics that would make a person's identity easily traceable. For example if you did a query against data and returned information related to gender, ethnicity and residency in a small group, it could be easy to determine who an individual is.



Confidentiality

- A student's confidentiality should be paramount, and if in doubt as to whether you should release any information, please contact the Office of the Registrar, Regulatory and Organizational Assurance area : 4-8219.
- The confidentiality of employee data is also considered as highly sensitive. Questionable use should be referred to the HR data steward.



DATA HANDLING TRAINING

Handling Electronic Data

- **Presented by:**
Hans Sigg
Business Services Computing



Handling Restricted Electronic Data

- Restricted data should not be copied to any removable devices including floppy disks, CD's or flash drives. Fixed hard drives without access controls on individual workstations (PC's) are also not an appropriate location to store restricted data. The most secure place to store this type of data is on a secure server with access controls.
- It is not appropriate to transmit restricted information by any method other than encrypted email or possibly via fax to a secure machine with limited access and advance notification of transmission to the recipient.



Matrix for Restricted Data Stored Electronically

<p>Storage on removable media (i.e. CD's, diskettes, flash drives)</p>	<p>Not permitted. However, in cases where information must be archived or transmitted outside the university, encrypting the information on the media is required.</p>
<p>Printing of Data</p>	<p>Unattended printing permitted only if physical access controls are used to prevent unauthorized viewing.</p>

Continued on next page



Matrix for Restricted Data Stored Electronically

Storage on fixed media (i.e. server) with access controls (password protected)

Encryption not required but recommended as additional level of security

Storage on fixed media (i.e. hard drive) without access controls, but not accessible via the Web

Not recommended, High risk. Preferred method of storage is as listed above.



Matrix for Restricted Data Transmitted Electronically

Fax	Machine must have limited access. It is recommended that the recipient is present during the transmission of data.
By Voice Mail	Do not leave restricted information in voice mail messages. Request the person call you back for the information.

Continued on next page



Matrix for Restricted Data Transmitted Electronically

By Wireless or cellular technology	Do not transmit
Other electronic transmissions (email, ftp, etc.)	Encryption required



Access to Data for Reporting

- University information is stored in several data bases with secure access. Employees should only have the access that is required to perform their assigned duties.
 - DSS Warehouse
 - SAS Share/Echo Data Sets
 - Page Center



Am I Handling Data Properly?

- If you are using reasonable measures to insure that data is secure, then it is being handled properly. This can be further clarified by answering the following questions:
 - What type of data are you utilizing? Is it sensitive, restricted, confidential, or personally identifiable?
 - What does the data handling matrix say to do with it?
 - Who will have access to it?
 - What will that person be doing with it?
- If you still aren't sure, ask your supervisor or Data Steward (listed in the flyer).



Handling Electronic Data

- Where does my responsibility end?
- What happens to the data after I pass it on?
- Question the Answers
- Treat all data as it were your own



DATA HANDLING TRAINING

Handling Printed Data

- **Presented by:**
Dan Whiteley
**Student Services Technology and
Assessment**



Data Handling

- Data handling refers to when you view, update, create, delete or destroy data. It also relates to when you transfer the data from one location to another.
- Based on how data is classified (Public, Sensitive, or Restricted), it may need precautions for handling.



Data Handling

- The quantity and variety of information that is utilized throughout the university is massive. It is not possible to define the appropriate method of handling for each individual piece of data. However, we will provide guidelines and examples which will enable staff to make reasonable decisions regarding the use, distribution, storage and destruction of university information.



Handling Printed Information

- **Public Information:**
 - There are no special requirements for the storage or destruction of documents containing only 'Public' information



Handling Printed Information

- **Sensitive Information:**
 - Sensitive information should be stored out of general sight and physically destroyed beyond recognition once the information is no longer needed.



Handling Printed Information

- **Restricted Information:**
 - It is required that Restricted information be stored in a secure manner. When not in use, these printed materials should be placed in a locked cabinet or other secure environment. Printed documents with Restricted information that is not needed must also be destroyed beyond recognition, with no possibility of recovery.



Data Handling Matrix Example

Handling of Printed information

Action	Public	Sensitive	Restricted
Storage of documents	No special requirements	Store out of sight when not in use	Store in secured location when not in use.
Disposal of documents	No special requirements	Physical destruction beyond ability to recover	Physical destruction beyond ability to recover



Handling Printed Information

- For printed information that must be destroyed beyond recognition or recover, the best alternative is to shred the documents. The University also provides other methods, such as depositing the items in secure recycle bins which are collected and destroyed appropriately by University staff.



Handling of Restricted Printed Data

- Printed materials with Restricted data do not need to be labeled in any special manner, for example by stamping the document as being Restricted. However, staff need to be cautious when duplicating or distributing restricted information. Copies should only be made as specifically required for distribution and these should be marked as 'Confidential'. It is also necessary for staff to understand how the distributed materials will be used and disposed of by the recipient.



Handling of Restricted Printed Data

- When documents are distributed internally (within the University), they should be placed in an envelope marked as “Confidential.”
- When documents are distributed externally, materials should be sent with a confirmation of receipt.



Data Matrix Example

Handling Restricted Printed Data

Labeling	Document envelope should be labeled as 'Confidential' if not hand delivered
Duplication	Receiver of document containing restricted information must not further distribute without permission
Mailing (Internal)	Preferred method of delivery is by hand. Information should be in an envelope marked "Confidential" if not hand delivered
Mailing (External)	Return receipt is required. (Note: partial SSN does not reduce risk.)
Destruction	Beyond recognition



Internal Mailing of Restricted Printed Data

- *Preferred* option: Hand deliver,
- Next best option: Place in an envelope marked ‘Confidential’ and place in the recipient’s individual office mailbox.
- Another option: Place in an envelope marked ‘Confidential’ and place in the recipient’s office mailbox.



Mailing Printed Restricted Data Outside Your Office

- If hand delivery is not an option, place in an envelope marked “Confidential” and place tape across the flap of the envelope



Mailing Printed Restricted Data Off Campus

- When you are sending restricted printed information to an approved recipient that is off campus, the preferred method of delivery is by mail with a return receipt requested.



Faxing Restricted Data

- In some instances it might be impossible for you to hand deliver the information.
- When faxing restricted data, it is necessary to determine if the recipient's fax machine is secure (uses a password for retrieval of information). If it is not, then it will be necessary for you to fax the document when the recipient is standing by the machine so they can pick up the information immediately. They should confirm receipt of the information via a telephone call back to you.



Indiana Social Security Number Disclosure and Security Breach Legislation

- **Presented by:**
Joanna Lyn Grama, J.D.
ITaP Security and Privacy



Outline

- New Indiana Legislation
- Relevant Purdue Policies



Indiana SSN Legislation

- Two new Indiana laws dealing with disclosures of personal information
 1. “Release of Social Security Number” (Ind. Code § 4-1-10)
 2. “Notice of Security Breach” (Ind. Code § 4-1-11)



“Release of SSN”

- Ind. Code § 4-1-10 (effective July 1, 2006)
- Law states that, except where otherwise permitted, “a state agency may not disclose an individual’s Social Security number.”

Ind. Code § 4-1-10-3(b).



“Release of SSN”

- A disclosure is permitted when:
 - The underlying individual gives written consent;
 - Where required by federal or state law;
 - Where required by court order;
 - When administering health benefits plan; and
 - Various other federal law requires (e.g., U.S. Patriot Act).



“Release of SSN”

- Additional Disclosure Exceptions:
 - A state agency may disclose the Social Security Number of an individual to a state, local, or federal agency.
- Ind. Code § 4-1-10-4(1)



“Release of SSN”

- Where a disclosure is impermissibly made, penalties apply to the individual state agency employee making the disclosure.
 - “Knowing, intentional, or reckless” disclosure = Class D felony
 - “Negligent” disclosure = Class A infraction.



“Release of SSN”

- Notification:
 - If a disclosure is impermissibly made, the University must give notice to the affected individuals.
- Ind. Code § 4-1-10-7



“Notice of Security Breach”

- Ind. Code § 4-1-11 (effective July 1, 2006)
- “Any state agency that owns or licenses computerized data that includes *personal information* shall disclose a *breach of the security of the system* following discovery or notification of the breach to any state resident whose *unencrypted personal information* was or is reasonably believed to have been acquired by an unauthorized person.”
Ind. Code § 4-1-11-5(a)



“Notice of Security Breach”

- “Personal Information” is defined as:
 - A person’s first and last name OR first initial and last name, *and at least one* of the following:
 1. Social Security Number
 2. Driver’s license or identification card number
 3. Account number, credit card number, debit card number, security code, access code, or password of an individual’s financial account.



“Notice of Security Breach”

- A “breach of the security of the system” is specifically defined as:
 - “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a state or local agency.”
Ind. Code § 4-1-11-2
 - Encryption is not defined for application of safe harbor provision.



“Notice of Security Breach”

- Notification:
 - If a security breach takes place, the state agency must give notice of the breach to the affected individuals.

Ind. Code § 4-1-11-5



“Notification Requirements”

- Must be made without unreasonable delay.
- Notification must be in writing or by electronic mail (if the individual has provided the state agency with the individual’s email address).

Ind. Code § 4-1-11-8



Purdue SSN Policy

- Purdue's Social Security Number Policy
 - http://www.purdue.edu/policies/pages/information_technology/v_5_1.html



Data Handling Requirements

- Data Classification Requirements
 - <http://www.itap.purdue.edu/security/policies/dataConfident/restrictions.cfm>
- Data Handling Requirements
 - <http://www.itap.purdue.edu/security/procedures/dataHandling.cfm>



Short Video Session

- New Freshmen students: <C:\October Security Events\Pete Technology Act I.wmv>
- The McCumber Cube: Tool for Decision Making: <C:\October Security Events\McCumberCube Act I.wmv>
- <http://www.educause.edu/SecurityVideoContest2007/10955>



National Cyber Security Awareness Events

- **Questions for the Panel?**