Practice

Below are some security best practices

- Always lock your workstation, mobile device or laptop when you are not using them.
- Create strong passwords
- Do not share your password or log in for others
- Do not store restricted university data on any computer.
- Check your hard drive monthly to ensure that you have not saved any sensitive or restricted files. This type of data should always be stored in a secure area on the LAN
- Do not open unexpected email attachments. Verify from the sender that the attachment is legitimate.
- Clear your browser cache monthly
- Never enable the password "auto-save" feature on your browser

Keys to Securing Purdue's Data

October 2011

http://www.purdue.edu/securepurdue/bestPractices/

Know the Laws and Policies that Govern How the Data is Handled

In order to be good stewards of University data, it is important that we understand the laws and policies that govern how our data is handled. Get informed on government laws:

- HIPAA (Health Insurance Portability and Accountability Act of 1996)
- FERPA (Family Educational Rights and Privacy Act of 1974)
- GLBA (Gramm Leach Bliley Act)
- Authentication and Authorization policy (V.1.2)
- Data Security and Access policy (C-31)
- SSN policy (V.5.1)
- Data Governance and Classification Policy (V.1.8)

For more information on these laws and policies or others not listed here, visit

http://www.purdue.edu/Business/Security/Policies_Procedures/

Know How to Handle the Data

There are three ways in which we categorize the handling of our data:

- Handling of Printed Information
- Electronically Stored (Computer-based) Information
- Electronically Transmitted Information

Below is a summary of how to handle restricted data. For the complete guide to handling all university data, go to

http://www.purdue.edu/securepurdue/procedures/dataHandling.cfm

Handling Printed Restricted Data

Labeling	No special requirement. Some documents should be labeled as "Confidential"
Duplication	Receiver of document containing restricted information must not further distribute without permission
Mailing (internal & external)	No classification marking on external envelope, envelope to be sealed in such a way that tampering would be indicated upon receipt.
Destruction	Destroy beyond recognition (shred)
Storage	Store in secure location when not in use

Handling Electronically Stored Restricted Data

Storage on removable media (Example: CDs, diskettes)	Not allowed
Printing of data	Unattended printing permitted only if physical access controls are used to prevent unauthorized viewing
Storage on fixed media (Example: server) with access controls	Encryption not required except for instances of CC and bank account information
Storage on fixed media (Example: hard drive) without access controls, but not accessible via the web	Not recommended

Questions?

A **Data Steward** manages data as a University resource and asset. You may contact the below Data Stewards for questions regarding these data.

- Cheryl Gray (HR) 496-2884
- Kay Parker (Financial) 496-7875
- Dan Whiteley (Student) 494-7416

For a complete listing of all other Data Stewards, go to

- http://www.pedu/securepurdue/policies/dataStewards.cfm

Handling Transmitted Restricted Data

Fax	Unattended printing permitted only if physical access controls are used to prevent unauthorized viewing. Printouts are to be picked up as soon as possible.
By Voice Mail	Do not leave restricted information in voice mail message. Request call back
By Wireless or cellular technology	Do not transmit
Other electronic transmissions (Example: Email, FTP)	Encryption required

Need Training?

Need a review of data handling and security? View the training at http://www.purdue.edu/securepurdue/procedures/dataClassif/Resources.cfm

Log in using your career account and password. If you have problems contact, certify@purdue.edu and put Training Problem in the subject box.

Know How the Data is Classified

The University's data are organized by the area responsible for it. Information regarding specific types of data, its classification (public, sensitive, restricted) and who the Information Owner is can be found at the following link: http://www.purdue.edu/securepurdue/procedures/dataClassif.cfm

Below is a summary of HR, Finance, and Student restricted data

RESTRICTED FINANCIAL DATA
• Social Security Number
• Credit card (CC) numbers
• Transactions and balances of selected accts (i.e. reserves, endowments)
• GLBA (loan agreements/ balances, collection activity)
• Bank account numbers
• Grant proposals
RESTRICTED HR DATA
• Social Security Number
• HIPAA (i.e. Benefit claims)
• Employee counseling
• Employee Background Check
• Employee ADA information
• Employee discipline
• Garnishments/child support
• Bank account information
• Ethnicity
• I9 Documentation
• Employee Selection of Wellness Prog
• Leaves - FMLA, sick leave, LTD/STD
• Payroll deduction selections
RESTRICTED STUDENT DATA
• Social Security Number
• 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

Continued on next page

• Deceased students
• Disability information
• Discipline information
• Donor information
• Encumbrance information
• Exam schedule
• Fellowship awards
• Financial Aid information
• Financial info of students or parents
• Fraudulent records information
• Grades/GPA/Transcripts
• Insurance information
• Litigation information
• Medical records
• Minority student information
• Resume information
• Salary data collected former students
• Subpoenas for student records
• Tax record info of students/parents
• Test scores
• Veterans' records
• Witness protection program

Proper Data Handling

Ask yourself:

- What type of data am I using?
- How is the data classified?
- Who will have access to the data and what will they do with it?
- What do the data handling requirements say?
- Have I followed the appropriate handling requirements for public, sensitive, or restricted data?
- Are there alternative ways to handle the data that make it more secure or less likely to be used or viewed by unauthorized individuals?