

“How Secure Am I” Checklist

You should be familiar with the following items, understand them and how it applies to your job:

- Security policies (i.e. Data Access and Security, SSN and email)
- Security memos (i.e. memo from Jim Almond dated June 25th, 2007)
- Indiana SSN Disclosure and Breach Laws
- Federal laws such as HIPAA, FERPA, GLBA
- Data Classification
- Data Handling
- Best Practices for securing your workstation, using email and the internet

If there were any items listed above that you are unsure of, go to the Business Services Security website at <http://www.purdue.edu/business/Security/> for more information

Data Handling and Security Training

Need a review of Data Handling and Security? View the training at <http://www.itap.purdue.edu/tlt/ecourses/index.cfm>.

Log in using your career account and password. If you don't have access, contact Tammy Murray (tlm@purdue.edu).

DATA SECURITY INVOLVES “U”

Keep It Secure



Business Services
Data Handling and Security
September 2007

<http://www.purdue.edu/Business/Security/>
<http://www.purdue.edu/securepurdue/>



Administration Data Classification & Handling

The University's administrative 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.itap.purdue.edu/security/procedures/dataClassif.cfm>

Information on how to handle the data can be found at:

<http://www.itap.purdue.edu/security/procedures/dataHandling.cfm>

What is Restricted Data

RESTRICTED FINANCIAL DATA	
•	Social Security Number
•	Credit card (CC) numbers
•	Transactions and balances for selected accounts (Example: reserves, endowments)
•	Data covered under GLBA (loan agreements/balances, collection activity)
•	Bank account numbers
•	Grant proposals
RESTRICTED HR DATA	
•	Social Security Number
•	Data covered under HIPAA (i.e. Benefit claims)
•	Employee counseling
•	Employee discipline
•	Garnishments/child support
•	Bank account information
•	Applicant interview results
•	Exit interviews
•	Termination reasons
•	Leaves pertaining to FMLA, sick leave, LTD/STD
•	Payroll deduction selections

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

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)	No special requirements.
Mailing (external)	No special requirements. Confirmation of receipt required as legally mandated
Destruction	Destroy beyond recognition (shred)
Storage	Store in secure location when not in use

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

Who are the Data Stewards?

Administrative data is owned by the University and should be shared appropriately to meet the needs of the University and its customers. A **Data Steward** manages data as a University resource and asset.

- Cheryl Gray (HR) 496-2884
- Hans Sigg (Financial) 494-6320

For a complete listing of all other data stewards, go to <http://www.itap.purdue.edu/ea/stewards/>

Security Best Practices

- ALWAYS lock your workstation, mobile device or laptop when you are not using them.
- Create a strong password and change it every 30 days
- Do not share your password
- Do not log in for others
- Do not download software
- Do not store data on the hard drive
- Do not store restricted university data on your home 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 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

Security Requirements Memo

Dated June 25th, 2007

The memo specifically **states that:**

- Personal or sensitive data shouldn't be stored on your workstation (i.e., hard drive, C:).
- Personal or sensitive data shouldn't be transmitted via e-mail.
- All electronic documents must be stored on the LAN.
- Restricted or sensitive data printed on paper must be stored in a secure location (i.e., locked filing cabinets).
- Your workstation is to be used for business purposes only.

University Security Policies

SSN Policy

Unless the University is legally required to collect an SSN, individuals will not be required to provide their SSN. You can provide your PUID instead.

Acceptable Use Policy

Only access files or data if they belong to you, are publicly available, or the owner of the data has given you permission to access them.

Federal Laws

HIPAA

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 condition.
- Provision of health care.
- Past, present, or future payment for health care that identifies an individual (i.e., name, address, SSN, birth date).

FERPA

Outlines what rights the student has to his/her education records. It also outlines when education records can be disclosed and to whom. Examples of FERPA protected data are:

- Grades, transcripts, and degree information.
- Class schedule.
- Student's information file (including demographic information).

GLBA

Its intent is to protect personally-identifiable information in situations where a consumer has provided information with intent to receive a service. Examples of financial services at Purdue:

- Student loans
- Information on delinquent loans
- Check cashing services