Why is Data Security Important?

1

Ward Against Identity Theft

Identity theft occurs when somebody steals your name and other personal information* for fraudulent purposes. They can use this information to apply for credit cards, drivers licenses, etc. Identity theft can result in an individuals' credit being damaged and could potentially make it difficult for them to get loans or other credit cards. It could also result in numerous hours and money that an individual may spend in clearing their name.

*Social Security numbers, birth date, mother's maiden name, driver's license number, bank account information, and credit card information.

2

Avoid Risking Safety of University Staff

Some staff at the University have chosen to withhold their information (such as home phone and address) from being published in the Purdue directory. They may have chosen this for numerous reasons, but their privacy needs to be respected. Unfortunately, some staff may be in situations where they or their families' personal safety may be in jeopardy if this information fell into the wrong hands.

3

Avoid Federal Penalties and Fines

We are bound by federal guidelines such as HIPAA, FERPA, GLBA etc. These guidelines require us to handle data in a certain way. If we fail to comply with these guidelines, the University could receive penalties and/or fines.

4

Embarrassment to the University

When data is compromised, letters are typically sent out to those who were potentially affected. This may often affect students, staff, donors, etc. Articles may be published in the newspaper and reports may be seen on local or national news. This is very bad publicity for the University.

5

Stolen Financial Resources

Some areas of the University have access to staff bank accounts (i.e., for direct deposit). If this information fell into the wrong hands, the individuals' financial holdings could be at jeopardy.

6

Why Should I Care About How Data is Handled?

We often become desensitized to the data that we handle in our everyday job. However, somewhere at the University, someone is handling your information, whether it be your SSN, your bank account information, etc. Think about how you want your data handled and use those same measures for handling the data of individuals or the University.

7

Security Policies and Memorandums

1

Data Access and Security Policy C-34

- Applies to administrative computing resources regardless of where they reside. Its three major guiding principles are:
  - Access - To assure that employees have access to relevant data they need to conduct University business;
  - Data Security - To prevent unauthorized access to systems, data, facilities, and networks; and
  - Physical Security - To prevent any misuse of, or damage to, computer assets or data.
- Security Policy C-34 specifically states that, “No University employee will knowingly damage or misuse computing resources or data. The employee's need to access data does not equate to casual viewing. It is the employee's obligation, and his/her supervisor's responsibility, to ensure that access to data is only to complete assigned functions.”

2

Security Requirements Memo

Outlines the expectations for Business Services staff regarding the specific handling of data, securing of workstations, utilization of e-mail, etc.

- 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.

**Please read the complete version of the memo before taking the assessment in this section.

3

Information Technology Policies

4

SSN Policy

- All new systems purchased or developed by Purdue will NOT use SSN as identifiers.
- All University forms and documents that collect SSNs will use the appropriate language to indicate whether request is voluntary or mandatory.
- 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.

**Visit the Additional Resources section found at the end of the training for a complete version of the policy

5

E-mail Policy

- Employees are granted e-mail accounts for the purpose of conducting University business.
- E-mails sent by users or which reside on University e-mail facilities may be considered a public record (Indiana Public Records Act).
- Users should exercise caution and any information intended to remain confidential should not be transmitted via e-mail.
- Refrain from improper use (i.e., commercial or private business purposes, organized political activity, to harass or threaten other individuals or to degrade or demean other individuals).

** Visit the Additional Resources section found at the end of the training for a complete version of the policy.

6

IT Resource 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.
- Complies with applicable laws and University policies, regulations, procedures, and rules.
- Prohibits use of IT resources for operating business, political activity, or personal gain.

**Visit the learning guide, IT Resource Acceptable Use Policy, (located on the left panel) for a complete version of the policy.

7

Policies Resulting from State/Federal Guidelines or Mandates

8

Indiana SSN Disclosure

Law 1 Ind. Code § 4-1-10 - "Release of Social Security Number" –Except where otherwise permitted, "a state agency may not disclose an individual's SSN."

A disclosure is only permitted when:

- The person gives their written or electronic consent
- Where required by federal or state law
- Where required by court order
- When administering employee health plan benefits
- Various other federal law requirements (US Patriot Act)
- A state agency discloses the SSN internally or to another state, local, or federal agency
- A state agency discloses the SSN to a contractor who provides goods or services if the SSN is required for the provision of the goods or services (contractual safeguards are required)
- A state agency discloses the SSN to a contractor for the permissible purposes set forth in HIPAA and FERPA

9

Indiana SSN Disclosure Continued

Example: SSN is collected for payment for tax purposes. This process is allowed under the law and is an acceptable business practice. While the law may allow the disclosure of SSN, it may not be an acceptable business practice. In many instances Purdue policy on SSN is more stringent than the Indiana law.

NOTE: When a disclosure is impermissibly made - criminal penalties apply to the employee making the disclosure.

10

Notice of Security Breach

Law 2 Ind. Code § 4-1-11 - "Notice of a Security Breach" - "Any state agency that owns or licenses computerized data that includes personal information shall disclose a breach of the security of the system following a 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 authorized person.

Personal information under the law is defined as a person's first AND last name OR first initial and last name AND at least one of the following:

- SSN
- Driver's license or state ID number
- Account number, credit card number, debit card number, security code, access code password of an account.

The notification that must occur to the affected individuals must be made without reasonable delay and except in certain circumstances, must be made in writing.

11

HIPAA

Health Insurance Portability and Accountability Act of 1996

- 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).
- Staff handling this data need to attend additional training and sign an acknowledgement form. Information regarding the training can be found by visiting the Additional Resources section found at the end of the training. Select the item, HIPAA Training for a link to the actual training.

12

FERPA

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.
- Examples of FERPA protected data are:
  - Grades, transcripts, and degree information.
  - Class schedule.
  - Student's information file (including demographic information).
- Staff handling this data need to attend additional training and sign an acknowledgement form. Information regarding the training can be found by visiting the Additional Resources section found at the end of the training. Select the item 'FERPA Training' for a link to the actual training.

13

GLBA - Gramm Leach Bliley Act

GLBA was set forth by the Federal Trade Commission. 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
- Staff handling this data need to attend additional training. Information regarding the training can be found by visiting the Additional Resources section and selecting 'GLBA Training' for a link to the actual training.

14

Summary

- You should only access data that is needed to complete your assigned functions.
- Use the PUID instead of an SSN wherever possible.
- Users should exercise caution and any information intended to remain confidential should not be transmitted via e-mail.
- An employee can be held personally responsible if an improper disclosure of SSNs is impermissibly made.
- GLBA refers to personally-identifiable information in situations where a consumer has provided information with intent to receive a service.
- FERPA relates to student data that is protected Family Education Rights and Privacy Act of 1974.
- HIPAA refers to protected health information.
- Special care should be taken when handling GLBA, FERPA, HIPAA data. More will be discussed on this in the data handling section.

15

Data Classification

1

Data Classification

For the purpose of handling data appropriately, data is classified by data stewards and information owners into one of the following three categories.

- Public
- Sensitive
- Restricted

2

Public Data

May be or must be open to the public.

Example: chart of accounts, pay scales
An employee's name, department, work phone, and building may also be considered public if it is published in the Purdue directory. The employee has the option to choose whether they want their home address and phone to be public information or restricted.

3

Sensitive Data

Information which may be guarded due to privacy considerations.

Example: employee's salary, account balances

4

Restricted Data

Information protected due to statutes, policies, or regulations. May also include information which has been deemed highly sensitive.

Example: transactions for “restricted” accounts (specific accounts identified by the Comptroller as “sensitive” such as central reserves and endowments) or garnishments.

5

Data Classification vs. Public Record

You might be thinking, “I thought that all Purdue data was public because we are a public institution?”

Do not confuse the Access to Public Records Act with the proper handling of data. Since Purdue is a public institution, we may be required to provide certain information upon request, but this request goes through the Director of Business Managers office and is reviewed prior to providing the information to the requestor. A good example of this is employee’s salaries. This information is available at the library as a matter of public record. However, since this data is classified as “sensitive” we do not provide this data to just any staff member who wants this information.

6

Examples of HR Data Classification

Information Owner	*Information Name*	*Description*	*Public*	*Sensitive*	*Restricted*
Asst Director Benefits	*Benefit Claim*	*Information to support the filing of claims against benefits*			*X*
Asst Director Class/Comp	*Compensation*	*The time spent by an employee for which the University will compensate*		*X*	
Payroll Manager	*Payroll Cycle*	*Defines the time periods against which employees of Purdue are paid*	*X*		

7

Examples of Restricted Financial Data

- SSNs
- Credit card numbers
- Transactions, balances for selected accounts (i.e., reserves, endowments)
- Data covered under GLBA (loan agreements, balances, and collection activity)
- Bank account numbers
- Grant proposals

8

Examples of Restricted HR Data

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

9

Complete Data Classification Listing

Purdue's data classification matrixes can be found in this section prior to the assessment. Please take some time to review how data (that you handle) is classified. Data classification is documented by the area that owns it.

10

Personally Identifiable Information (PII)

PII is data such as:

- SSN
- Any financial information about an individual (account numbers, credit card numbers, pin numbers, etc.)
- Any health information about an individual (including insurance information and health status information).
- Any "non-directory" information about a student.

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 a department had only one female employee and you were displaying data by gender, it would be easy to determine the identity of that individual.

11

Confidential

The term "Confidential" is often used interchangeably with other security terminology.

"Confidential" is not a data classification like sensitive or restricted. It really describes how information should be treated. For example, a conversation between an employee and supervisor may be confidential and the employee wishes that the supervisor not share that information with anyone else.

12

Summary

- For the purpose of determining how to handle data, Purdue has three classifications for data: public, sensitive and restricted.
- Public record is separate from data classification.

13

Data Handling

1

Data Handling

As University employees, we have all been granted access to a wide variety of information in order to perform our duties. Much of this information is considered to be ‘public’, and can be generally shared or distributed. However, our focus is on ‘sensitive’ and ‘restricted’ data that must be held in confidence to avoid its misuse, which could have a negative impact on fellow staff members, faculty, students, or the University. We all have a role in the safeguarding of this information and should be aware of our individual responsibilities. The following three roles have been defined and cover the obligations of all University employees:

- Information Owners
- Data Stewards
- Data Custodians

2

Roles in Data Handling

- **Information Owners** - Provide **policies and guidelines** for the proper use of the information and may delegate the interpretation and implementation of those policies and guidelines to appropriate personnel. In Business Services, this responsibility has been delegated to the heads of departments.
- **Data Stewards** - Responsible for facilitating the **interpretation and implementation** of the data policies and guidelines among their Vice President's delegates. Data Stewards have been designated to monitor access and usage of data related to specific areas within the University (i.e., University Development, HR, Physical Facilities, ITaP, OIR, Card Services, Financial, HFS, SMAS, and Student Services).
- **Data Custodians** - Responsible for **implementing the policies and guidelines** established by the Information Owners. This includes every staff member within the University. Each individual is in the best position to monitor daily data usage and ensure that information is securely handled in the most appropriate manner.

3

Data Handling

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

4

Data Handling

"Handling" information relates 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 upon how data is classified (Public, Sensitive, or Restricted), it may need precautions for handling. For the purposes of handling data, Purdue has grouped our guidelines into three categories:

- Printed Information (paper, microfiche)
- Electronically Stored (computer based)
- Electronically Transmitted (i.e., e-mail, fax)

5

Handling Printed Information

6

Handling Printed Information

The following page provides a *sample* of the matrix that provides general guidelines related to the handling of any form of printed data (paper, microfiche, or microfilm). For a complete version of the matrix, see the data handling matrixes at the end of this section.

7

Data Handling Matrix

(note this is just a sample)

Handling of Printed Information (paper, microfiche, microfilm)			
Action	**Public**	**Sensitive**	**Restricted**
Storage of documents	No special requirement	Store out of sight when not in use	Store in secured location when not in use
Disposal of documents	No special requirement	Physical destruction beyond ability to recover (i.e., shredding). Locked,blue Physical Facility recycle bins are also acceptable.	Physical destruction beyond ability to recover (i.e., shredding). Locked,blue Physical Facility recycle bins are also acceptable.

**Recommendations on handling of restricted data doesn't apply to financial restricted accounts.

8

Handling **Restricted** **Printed** Data

Labeling	No special requirement. However, some HR and Financial documents must be labeled "Confidential". See Additional Resources section at the end of training for a list of these documents. Copies should only be made as specifically required for distribution. It is also necessary for employees to understand how the distributed materials will be used and disposed of by the recipient.
Duplicating	Receiver of document containing restricted information must not further distribute without permission
Mailing	When documents are distributed they should be in a sealed envelope.
Destroying	Destroy beyond recognition (i.e., shredding). The University also provides other methods such as depositing the items in secure recycle bins which are collected and destroyed appropriately by University staff.

9

Examples of Destroying Restricted Printed Data

- Acceptable – put paper in locked recycle bin where it is exposed to few people.
- Best – shred paper.

10

Handling Restricted Electronic Data

Stored and Transmitted

11

Handling Restricted Electronic Data

The next several pages cover how to handle restricted data that is that is either electronically stored or transmitted.

Restricted data should not be copied to any removable devices, including computer floppy disks, CDs or flash drives. Fixed hard drives on individual workstations (PCs) 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 (i.e. LAN) 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.

12

Handling **Restricted Electronically** - **Stored** Data

Storage on removable media (i.e., CD's)	Not allowed
Printing of data	Unattended printing permitted only if physical access controls are used to prevent unauthorized viewing.
Storage on fixed media (i.e., servers with access controls)	Encryption not required except for instances of credit card and bank account information.
Storage on fixed media (i.e., hard drive) without access controls, but not accessible via the Web	Not allowed

13

Examples of **Printing Electronic Restricted** Data

- Acceptable – send to shared printer where small group of people have access to it.
- Best – send to shared printer with a separate bin where there is limited physical access.

14

Handling **Restricted Electronically - Transmitted** Data

Fax	Machine must have limited access.
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 (e-mail, FTP, etc.)	Encryption required.

15

Examples of **Transmitting Restricted** Data

- Acceptable – contact recipient prior to submission and send to private location.
- Best – avoid sending complete credit card numbers. Send last four digits with limited additional information. Send data to private location with prior notification.

16

Complete Data Handling Matrices

A complete listing of all data handling matrices at Purdue can be found by at the end of this section and after the assessment. Please take some time to review this material to ensure you are handling data appropriately.

17

How Do I Know if I am Handling Data Properly?

18

How Do I Know if I am Handling Data Properly?

If an individual employee is using reasonable measures to ensure 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?
- Are there alternatives?
- 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 are still not sure, discuss the matter with your manager or consult the appropriate Data Steward.

19

Data for Reporting

20

Access to Data for Reporting

University information is stored in several databases with secure access. Employees should only have the access that is required to perform their assigned duties.

- **DSS Warehouse – Financial, Employee, and Student**
- **SAS Share Data Sets**
- **PageCenter**
- **OnePurdue (including portal and R/3)**
- **OnePurdue Business Warehouse**

****Specific access is determined by the Data Stewards and closely monitored for unauthorized activity.**

21

Summary

- Everyone at the university is a data custodian and is responsible for securing data through the implementation of data policies and guidelines.
- Data handling guidelines are based on how data is transmitted (printed, electronically stored, electronically transmitted).
- With regards to restricted data, the following measures are best practices:
  - **Paper restricted documents** – shred or place in Blue Physical Faculties recycling bins
  - **Electronically stored restricted data** – store only on secure server (i.e. LAN)
  - **Electronically transmitted restricted data** – in most cases do not transmit. Transmission with encryption is acceptable in some situations.

22

Security Tips

1

Technical Support

The information provided in this session pertains to all Business Services staff. If you are supported by another area other than the Business Services Computing Zone* you should work with your technical support to ensure that these standards can be implemented, except where noted.

*Technical support for Business Services staff in buildings such as Freehafer, Hovde, Young, 501 Hayes and Purdue West

2

Workstation Security

- Lock your workstation when you are away from your desk. To lock your workstation, press Ctrl/Alt/Delete and “Lock Computer”.
- Shut down your workstation each night. **Check with your technical support to see what is required in your area.
- Do not store personal or sensitive data about employees, students, customers, or anyone otherwise affiliated with Purdue on the workstation hard drive, laptops, tablet PCs, CDs, floppy disks, Blackberrys, or other external devices.
- Store FERPA, GLBA, HIPAA data on departmental servers. This will ensure the integrity of the data with proper backup procedures.
- Empty your Recycle Bin daily.
- Do not store Purdue data on your home computer.
- Delete temporary files. This is being done automatically for Business Services PCs.

3

Password Security

- Always use strong passwords and keep them secret. Passwords should not include, proper names, addresses, or phone numbers.
- Do not log in for other people for access to the computer system, e-mail system, or Blackberry device.
- Do not save passwords (mainframe, FTP, website passwords, etc.) to your workstation hard drive, e-mail, or Blackberry. You should be required to enter a password if an application requires a password. It should not auto-populate the password for you.

4

E-mail Security

- Check your e-mail folders: “Sent Items” and “Deleted Items” daily for sensitive data. If items are found, delete them. Empty your deleted items.
- Do not open e-mail attachments that you are not expecting. If someone sends you an attachment and you are not expecting it, contact the sender and ask him/her about it.
- Never store PII on your workstation, your e-mail account, or Blackberry.
- Never comply with requests for personal information from an e-mail or phone call unless you initiated the contact.

5

Internet Security

- Require your web publishers/administrators to ensure that confidential/restricted data is not requested or displayed on unsecure websites.
- Do not download software, screensavers, games, or other programs. These can harbor computer viruses or open a “back door,” giving others access to your computer.
- Delete temporary internet files. **Check with your technical support. This is done automatically for computers supported by the BSC Zone.
- Turn off auto-complete. It stores information such as usernames and passwords. To turn off auto-complete while using the Internet go to Tools, Internet Options, Content Tab.

6

Physical Security

- Sensitive and restricted data should be stored in secured locations (i.e., locked filing drawers and cabinets).
- You need to be aware of what data you may have that is considered sensitive or restricted. Make sure this data is properly secured.

7

Summary

- Data should be stored on a secure server (i.e LAN) instead of your hard drive (c drive).
- Change your password every 30 days and be sure to use a strong password.
- Do not open e-mail attachments that you are not expecting.
- Do not download software, screensavers, games, or other programs.
- Always be sure to physically secure sensitive or restricted data

8