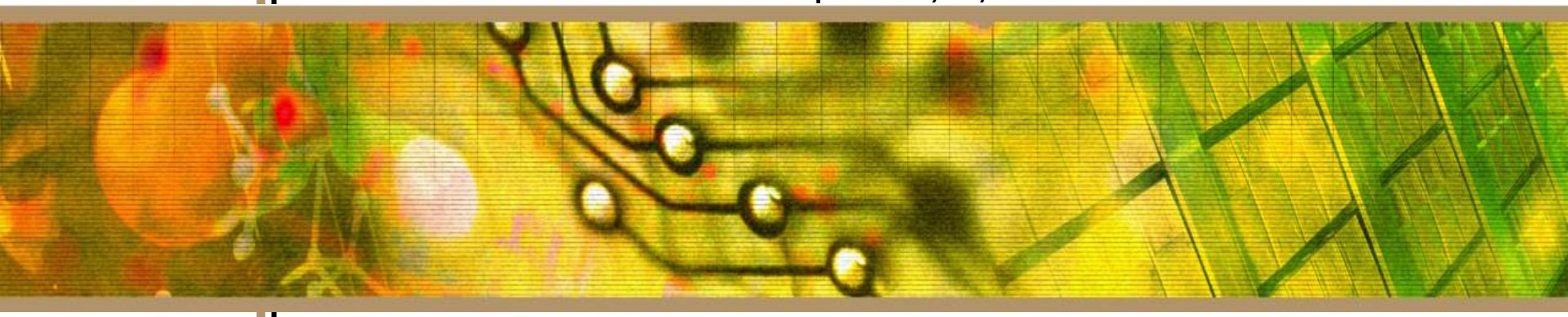
PURDUE
UNIVERSITY

Data Handling at Purdue

Updated 9/23/2019



SECURE PURDUE

PURDUE UNIVERSITY

Topics

Section I

- The Importance of Data Security (slides 4 – 5)
- Laws and Policies (Slides 6 – 18)
  - Federal
  - State
  - Purdue

Section II

- Data Classification (Slides 19 - 26)
- Data Handling (Slides 28 – 40)
- Data Security Tips (Slides 41 – 44)
- Summary (Slides 45 – 48)

Section I

The Importance of Data Security (slides 4 – 5)
Laws and Policies (Slides 7 – 18)

Data Security

Why Is Data Security Important?

- We are bound by federal guidelines such as HIPAA, FERPA, GLBA, etc. These guidelines require us to handle data in a specific manner. If we fail to comply, the university could receive penalties and/or fines.
- Some areas of the university have access to individual bank account information. If this information should fall into the wrong hands, the individual's financial holdings could be put in jeopardy.
- Some individuals at Purdue have chosen to restrict their information from being published. Regardless of why, their privacy needs to be respected. Unfortunately, some may be in situations where they or their families' personal safety may be in jeopardy if this information fell into the wrong hands.
- If stolen, personal information can be used for fraudulent purposes, resulting in numerous hours and money spent clearing an individual's name.
- 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 negative publicity for the university.

Why Should I Care About How Data Is Handled?

Often we become desensitized to the data that we handle in our everyday job. However, somewhere someone is handling your information, whether it be your SSN (Social Security number), your bank account information or other private information. Handle someone else's data how you'd like your data handled.

Laws and Policies

Family Education Rights & Privacy Act of 1974 (FERPA)

- 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 include:
  - Grades, transcripts, and degree information
  - Class schedule
  - Student's information file (including demographic information)
- Faculty and staff handling this data need to complete required certification at: **http://www.purdue.edu/webcert**

Gramm-Leach Bliley Act (GLBA)

GLBA was enacted by the Federal Trade Commission. The intent of GLBA is to protect personally identifiable information (PII) in situations where a consumer has provided information with intent to receive a service.

- Examples of financial services at Purdue include:
  - Student loans
  - Information on delinquent loans
  - Check cashing services
- Faculty and staff handling this data need to complete required certification at: **http://www.purdue.edu/webcert**

Health Insurance Portability and Accountability Act of 1996 (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)
- Additional training could be required by the department in which you work. You will be contacted if you need to complete the required certification at: **http://www.purdue.edu/webcert**

Indiana SSN Disclosure

Law 1 Indiana 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 written or electronic consent
- Where required by federal or state law
- When administering employee health plan benefits
- As required by federal law (U.S. 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

Indiana SSN Disclosure Continued

When a disclosure is impermissibly made, criminal penalties apply to the employee making the disclosure.

Notice of Security Breach

Law 2 Indiana Code § 4-1-11 - "Notice of a Security Breach" – Any state agency that owns or licenses computerized data that include personal information shall disclose a breach of the security of the system following a discovery or notification of a breach to any state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized 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 or password of a financial 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.

Data Classification and Governance

- Every piece of data owned, used, or maintained by the university must have one or more Information Owner(s) identified.
- An Information Owner, in consultation with the relevant Data Steward, must classify the data and records used in his or her administrative unit into the following three risk categories: Public, Sensitive, or Restricted.
- All Purdue University data will be reviewed on a periodic basis and classified according to its use, sensitivity, and importance to the university and in compliance with federal and/or state laws.

Social Security Number (SSN)

- All new systems purchased or developed by Purdue will NOT use SSN as identifiers.
- All university forms and documents that collect SSN data will use the appropriate language to indicate whether the request is voluntary or mandatory.
- Unless the university is legally required to collect an SSN, individuals will not be required to provide it. An individual's Purdue University Identification (PUID) can be provided, instead.

Data Security and Access (C-34)

- Applies to all administrative and academic computing resources. The policy's 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
- This policy 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.

IT Resource Acceptable Use

- 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.

Email

- Employees are granted an email account for the purpose of conducting university business.
- Emails sent by users or which reside on university email 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 email.
- 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).

PURDUE
UNIVERSITY

Purdue University Policies

For a detailed list of Purdue University policies, please visit the following Web URL:

http://www.purdue.edu/policies/

SECURE PURDUE

Section II

Data Classification (Slides 20- 26)
Data Handling (Slides 28 – 40)
Data Security Tips (Slides 42 – 44)
Summary (Slides 46 – 48)

Data Classification Categories

For purposes of handling data appropriately, data at Purdue University is classified by data stewards and information owners into one of the following three categories:

- Public
- Sensitive
- Restricted

Data Classification

Public

Public data may be or must be open to the public.

- Examples of data included in this category include, but are not limited to:
  - Chart of accounts, pay scales
  - The course catalog
  - Directory information
- Individuals have the option to restrict his or her public information.

Data Classification

Sensitive

Sensitive data is information which may be guarded due to privacy considerations.

- Examples of data included in this category include, but are not limited to:
  - Financial account balances
  - Major program of study, admissions applications and decision letters
  - PUID, date of birth

Data Classification

Restricted

Restricted data is information protected due to statutes, policies, or regulations. This may also include information which has been deemed highly sensitive by Purdue University.

- Examples of data included in this category include, but are not limited to:
  - Garnishments; credit card numbers; bank account numbers; grant proposals; employee counseling and discipline; I9 documentation
  - Student academic record information, non-directory information, SSN
  - Self-Identification Information – ethnicity; race; disability status; veteran status

Data Classification vs. Public Record

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

Don’t confuse the Access to Public Records Act with the proper handling of data. As a public institution, Purdue may be required to provide eligible information if a request for data is submitted to the Public Records Officer.

Data Classification

Personally Identifiable Information (PII)

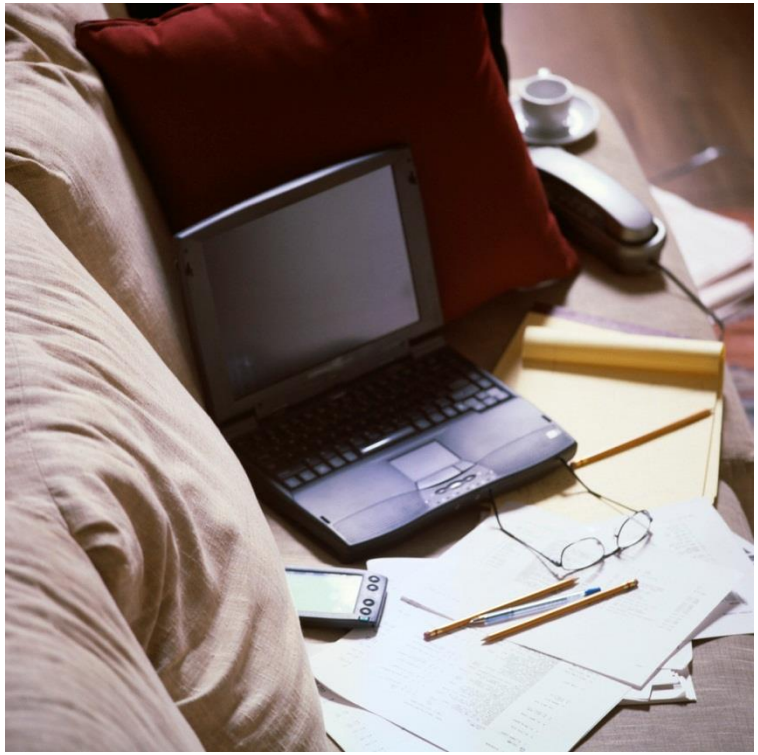
- Certain aspects of PII, such as SSN, are always classified as restricted data. If you are handling PII, you need to be aware of the classification of individual elements of that PII. The more elements of PII that can identify a particular individual, the more care you must use handling that information. Examples of data included in this category include, but are not limited to:
    - Date of birth, mother's maiden name, driver's license number, bank account information, credit card information, PIN numbers, health information, or any non-directory information about a student.
- 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 the individual.

Data Classification

- Self-Identification Information
  - Ethnicity, Race, Disability Status and Veteran Status are Self-Identification data collected from employees with the purpose and understanding that the information will be used to comply with federal and state regulations and will only be reported in summarized levels.
  - Occasional business needs arise in which individual-level data are needed. These requests require approval from the Office of Institutional Equity and should be handled in the same manner as other restricted data.

Confidential Information

The term “Confidential” is often used interchangeably with other security terminology. It is not a data classification like sensitive or restricted. It describes how information should be treated. For example, a conversation between an individual and their supervisor may be confidential if the employee requests the supervisor not share that information with anyone else.



Data Handling

PURDUE UNIVERSITY

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

PURDUE UNIVERSITY

Data Handling

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. A table listing area and information owner can be found at:
  https://www.purdue.edu/securepurdue/data-handling/index.php
- **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., HR, ITaP, HFS, Student Services). A listing of data stewards can be found at:
  https://www.purdue.edu/securepurdue/data-handling/data-stewards.php
- **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.

PURDUE UNIVERSITY

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 guidelines are grouped into three categories:

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

Data Handling (Printed Data)

The next slide provides a *sample* of the master matrix related to the handling of any form of printed data (paper, microfiche, or microfilm).

Go to the URL below for the complete matrix:

https://www.purdue.edu/securepurdue/data-handling/handling-of-printed-information.php

The use of the university confidential recycling program is acceptable for disposal of all classifications of documents/data. Information and requests for services can be found at:

https://www.purdue.edu/physicalfacilities/units/buildings-grounds/grounds/refuse-recycling-request.php

PURDUE UNIVERSITY

Data Handling (Printed Data)

Action	Public	Sensitive	Restricted
Storage	No special requirements	No special requirements	Store in secured location when not in use
Mailing via Campus Mail or via external mail	No special requirements	No special requirements	No classification marking on external envelope, envelope to be sealed in such a way that tampering would be indicated upon receipt.
Labeling	No special requirements	No special requirements	No special requirements. 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.
Duplication	No special requirements	No special requirements	Receiver of document containing restricted information must not further distribute without permission
Disposal	No special requirements	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.

Data Handling (Electronic Data)

- "Handling" information relates to when you view, update, or delete data. For electronic data handling, it also refers to when you transfer the data from one location to another or handle data in an electronic format.
- Like data recorded on paper, Purdue's data classifications apply to electronic data. Purdue has handling requirements for stored and transmitted data. These requirements are based on how the data is classified.
- Examples of electronic data handling:
  - Emailing data from one person to another
  - Faxing data from one person to another
  - Updating or editing database information
  - Storing data on removable media (USB drives, CDs, external hard drives, etc.)
  - Storing data on fixed media (a computer hard drive or networked drive)
  - Deleting information from removable or fixed media
  - Scanning of a document and emailing to yourself

Electronic Data Handling – Restricted Data

- Access to restricted data is determined by the Data Stewards and is closely monitored for unauthorized activity.
- Always use caution when handling personal data about employees, students, customers, or anyone affiliated with Purdue.
- Safeguards for restricted data cover:
  - Storing
  - Printing
  - Transmitting
  - Destroying

Storing Restricted Data

- Restricted data should NOT be copied to any removable media, including USB (or flash) drives, CDs, or external hard drives. Consult with your supervisor and data steward if there is a business need to share/store restricted data using removable media.
- Never store restricted data on your computer's C:\ drive. It is not appropriate to store restricted data on a computer hard drive (a fixed drive on an individual's workstation).
- The best place to store restricted data is on a secure server with access controls (e.g., password protected). This ensures the integrity of the data and makes sure that it is backed-up appropriately.
- When restricted data is archived, it must be encrypted and the storage media must be physically secured (e.g., stored in such a manner that it cannot be accessed by unauthorized persons).
- Do not store restricted data on your home computer or personal removable media device.

Printing Restricted Data

- Printouts must be picked up as soon as possible.
- Unattended printing is allowed only if physical access controls are in place to prevent unauthorized viewing.
- Acceptable: Send to shared printer where a small group of people has access to the printer.
- Best: Send to a shared printer with a separate bin where there is limited physical access to the printer (e.g., a locked room).

Transmitting Restricted Data

- Transmitting means email, instant message, fax, FTP, voicemail, scanning, any way you might communicate data in an electronic format.
- You must transmit restricted data in a way that protects its confidentiality and ensures that unauthorized people do not intercept or view the restricted data.
- Do not email documents, spreadsheets, or other electronic files if they contain restricted information unless you can encrypt the email or use another method to securely transfer the file.
  - Purdue's Filelocker service is a secure transmission method. See https://filelocker.purdue.edu/
- Do not use cellular or wireless technology to transmit restricted data.
- Use caution when faxing restricted data. It can only be faxed to secure machines with limited access and advance notice to the recipient.
- Do not leave restricted data in a voice mail message. Request the recipient return your call.

Data Destruction

- Purdue takes the destruction and disposal of data very seriously. Improper disposal methods can lead to the unintentional disclosure of confidential Purdue, student, employee, or research data.
- More information on data destruction can be found at the *MEDIA DISPOSAL GUIDELINES* Web site: https://www.purdue.edu/securepurdue/data-handling/media-disposal-guidelines.php
- Removable media that ever contained any Purdue data (whether restricted, sensitive, or public) must be physically destroyed when it is no longer used at Purdue.
- Fixed media (hard drives, servers, and other storage devices) that ever contained any Purdue data (whether restricted, sensitive, or public) must be physically destroyed when it is no longer used at Purdue.
- The use of Purdue's *Recycle for the Future* recycling program is acceptable for disposal of all classifications of electronic media and data. Information regarding this program can be found at: https://www.purdue.edu/surplus.

Data Handling - Conclusion

If you are using reasonable measures to ensure that data is secure, then you are handling data properly. Ask yourself these questions when you handle data:

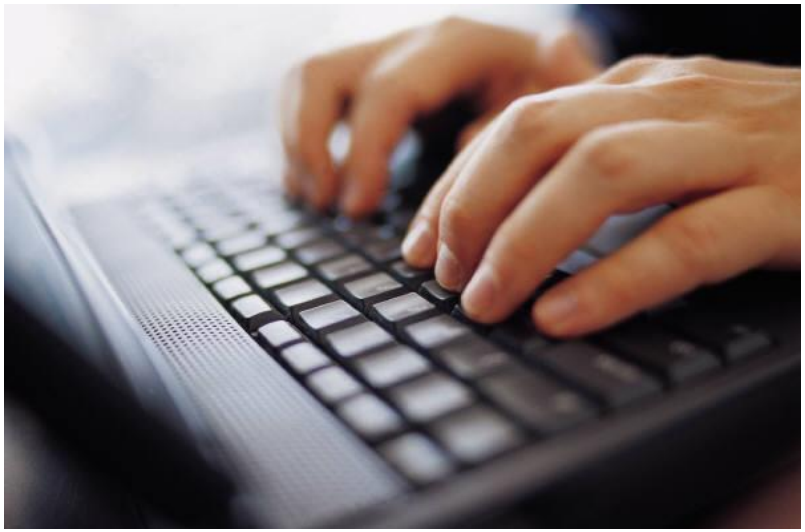
- **What type of data am I using? How is the data classified?**
  - Exercise caution when you are using information that contains personal details, financial information, Social Security numbers, or the Purdue University identification number (PUID).
- **Who will have access to the data and what will 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?**

If you still are not sure that you are handling data appropriately, ask your supervisor or the Data Stewards for advice. They are available to answer your questions and help you properly handle Purdue's data.

Data Security Tips

Data Security Tips

- For additional security practices, check with your departmental IT staff.
- NEVER change any security settings on your computer without first consulting with your departmental IT staff.
- With many areas of the university transitioning to the use of multifunction copier, printer, scan, and fax machines, keep in mind the data in the document you are scanning. If you wouldn't send it in an email, you shouldn't scan it and email from the machine to yourself.



PURDUE UNIVERSITY

Data Security Tips

Top Ten Ways You Can Practice Good Data Security

1. Always use strong passwords and keep them secret. Purdue has password policies and guidelines. You can learn more at: https://www.purdue.edu/policies/information-technology/s16.html
2. Do not login to Purdue IT resources (computer systems, email systems, or mobile devices) for other people.
3. Do not save passwords to your workstation hard drive, email, or cell phone, or other mobile device.
4. Lock your workstation when you are away from your desk or work area during the day, even if you are gone just for a short break. (Use Ctrl/Alt/Delete and select "Lock Computer" for Windows machines.)
5. Log off or turn off your computer each night. Check with your departmental IT staff for the preferred procedure for your area.
6. Ignore unsolicited emails. Never comply with requests via email or phone for personal information or account information unless you initiated the contact.

PURDUE UNIVERSITY

Data Security Tips

Top Ten Tips (Continued)

7. Be suspicious. Do not open or download email or instant messaging attachments unless you are expecting them. If someone sends you an attachment that you are not expecting, contact the sender and ask them about it.
8. Turn off the "auto complete" function in your Web browser as it can store user name and password information. (Ask your departmental IT staff for help doing this.)
9. Do not download software, special fonts, screensavers, games, or other programs. Sometimes these items can hold computer viruses or open up your computer to unauthorized individuals.
10. Read more about information security best practices on the *SecurePurdue* Web site. Best practices are those steps that you can take on your own to help secure the IT resources that you use.

Read more at:

https://www.purdue.edu/securepurdue/it-policies-standards/index.php

Summary

PURDUE UNIVERSITY

Summary

- You should only access data that is needed to complete your assigned job function.
- Use the PUID instead of the SSN wherever and whenever possible.
- An employee can be held personally responsible if an improper disclosure of SSNs is impermissibly made.
- Special care should be taken when handling HIPAA, FERPA and GLBA data.
- For determining how to handle data, Purdue has three classification levels for data: public, sensitive and restricted.
- PII information is not a data classification level.
- Public records is not a data classification level.

PURDUE UNIVERSITY

Summary

- Confidential information is not a data classification level.
- Email could be considered to be public information.
- SSNs are not used as identifiers in systems unless legally required to do so.
- Everyone at the university is a Data Custodian and is responsible for security of data by following data policies.
- Data handling guidelines are based on how data is transmitted (printed, electronically stored, electronically transmitted).
- Information owners provide policies and guidelines for proper use of the information.
- Data Stewards have been designated to monitor access and usage of data related to specific areas within the university.

Additional Information

The Web contains a lot of information and is a good source to assist in answering data handling questions.

Read more at:

- Data Classification and Handling Web site:

  https://www.purdue.edu/securepurdue/data-handling/index.php

- Purdue Information Technology (IT) Policies:

  https://www.purdue.edu/securepurdue/it-policies-standards/index.php

- The *SecurePurdue* Web site,

  https://www.purdue.edu/securepurdue/index.php

- If you still have questions, contact the appropriate data steward:

  https://www.purdue.edu/securepurdue/data-handling/data-stewards.php