Keys to Securing Purdue’s Data

Updated January 2014

Best Practices

- Always lock your workstation, mobile device or laptop when you are not using them.
- Create strong passwords.
- 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.
- Clear your browser.
- Cache monthly.
- Do not share your password or login for others.
- Do not store restricted university data on any computer.
- Do not open unexpected email attachments. Verify from the sender that the attachment is legitimate.
- Never enable the password “auto-save” feature on your browser.

Know Data Handling

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.

Health Insurance Portability and Accountability Act of 1996 (HIPAA): Laws and regulations governing the provision of health benefits, the delivery and payment of health care services and the security and confidentiality of Individually Identifiable and Protected Health Information in written, electronic or oral formats.

Family Educational Rights and Privacy Act of 1974 (FERPA): Federal law designed to protect the privacy of education records. It also provides guidelines for appropriately using and releasing student education records.

Gramm-Leach-Bliley Act (GLBA): Requires financial institutions to develop, implement, and maintain administrative, technical, and physical safeguards to protect the security, integrity, and confidentiality of customer information.

PCI (Payment Card Industry): A world wide security standard, to protect card holder information and the merchants and/or processors who store that sensitive information from fraudulent use.

Authentication & Authorization Policy (V.1.2): Controls that facilitate access to and protect University IT Resources and data. Access to non-public IT Resources will be achieved by unique User Credentials and will require Authentication.

Data Security and Access Policy (C-31): assure employees access to relevant data they need to conduct University business; prevent unauthorized access to systems, data, facilities, and networks; and prevent any misuse of, or damage to, computer assets or data.

For more information on these laws and policies, or others not listed here, visit: http://www.purdue.edu/securepurdue/bestPractices/policiesHierarchy.cfm

Know Data Handling con’t.

Social Security Number Policy (V.5.1): To ensure that the necessary procedures and awareness exist so that University employees and students comply with both the letter and the spirit of FERPA and Indiana Code Title 4 Article 1 Chapter 8 -- State Requests for Social Security Numbers, as amended from time to time.

Data Classification & Governance Policy (V1.8): Provides a framework for the governance and classification of university data in order to ensure the privacy and security of that data.

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?

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

- Handling of Printed Information
- Electronically Stored Information
- Electronically Transmitted Information

For the complete guide to handling all university data, visit:

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

Need Training?

Need a review of data handling and security? Visit http://www.purdue.edu/apps/account/cas/login using your career account and password.

If you have problems, contact certify@purdue.edu and put Training Problem in the subject box.

http://www.purdue.edu/securepurdue/bestPractices/
Know How the Data is Classified

The university's data are organized by the area responsible for it. Below is a summary of HR, Finance, and Student restricted data:

### 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
- 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 from former students via surveys
- Subpoenas for student records
- Tax record info of students/parents
- Test scores
- Veteran's records
- Witness protection program

### Restricted Financial Data
- Social Security Number
- Credit card (CC) numbers
- Transactions and balances of selected accounts (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 Background Check
- Employee ADA information
- Employee discipline
- Garnishments/child support
- Bank account information
- Ethnicity
- I-9 Documentation
- Payroll deduction selections

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](http://www.purdue.edu/securepurdue/procedures/dataClassif.cfm)

---

Know How Restricted Data Should be Handled

#### Restricted Data (Printed)

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

| **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 a voice mail message. Request a call back. |
| **By wireless or cellular technology** | Do not transmit. |
| **Other electronic transmissions (email, FTP)** | Encryption required. |

### Restricted Data (Electronically Transmitted)

| **Storage on removable media (CDs, USB flash drives)** | Not allowed. |
| **Printing of data** | Unattended printing permitted only if physical access controls are used to prevent unauthorized viewing. |
| **Storage on fixed media (server) with access controls** | Encryption not required (exception - HIPAA, FERPA, PCI, GLBA subject to applicable laws) |
| **Storage on fixed media (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 Data Stewards for questions regarding these data at data-stewards@lists.purdue.edu.

For a complete listing of all Data Stewards, visit [http://www.purdue.edu/securepurdue/policies/dataStewards.cfm](http://www.purdue.edu/securepurdue/policies/dataStewards.cfm).